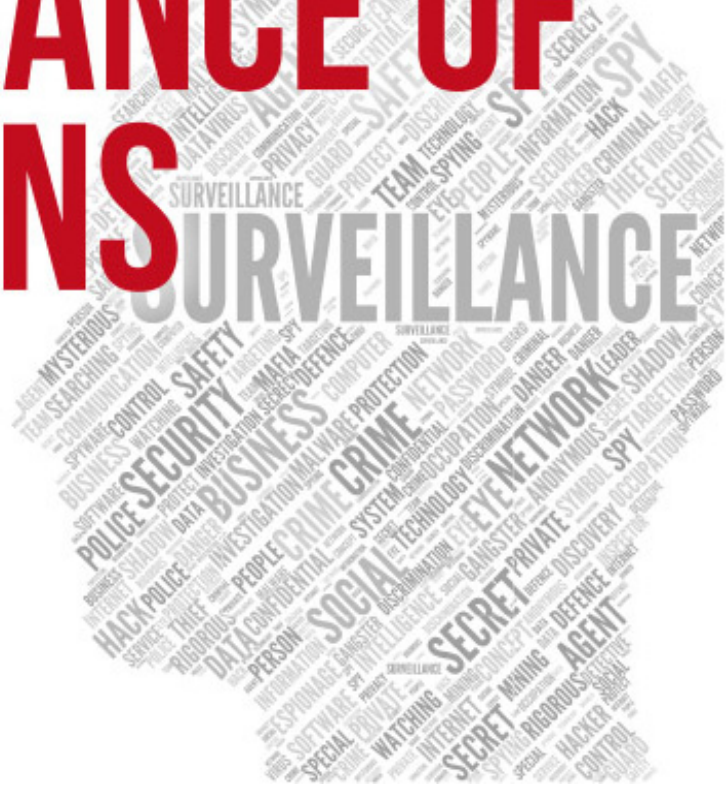
# LIBE COMMITTEE INQUIRY

# ELECTRONIC MASS SURVEILLANCE OF EU CITIZENS




Protecting fundamental rights in a digital age

*Proceedings, Outcome and Background Documents*

2013 – 2014

ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA EUROPSKI PARLAMENT PARLAMENTO EUROPEO
EIROPAS PARLAMENTS EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW
EUROPEES PARLEMENT PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

# Inquiry
# on electronic mass surveillance of EU citizens

## Protecting fundamental rights in a digital age

***Proceedings, Outcome and Background Documents***

2013-2014

# INTRODUCTION

**Claude Moraes MEP, Rapporteur of the Inquiry on electronic mass surveillance of EU citizens**


The Civil Liberties, Justice and Home Affairs Committee (LIBE) Inquiry into the mass surveillance of EU citizens was the first completed, in-depth inquiry to investigate the revelations of previous NSA sub-contractor Edward Snowden and their impact on EU citizens´ fundamental rights. Beyond the testimony of Edward Snowden the European Parliament was conscious that we had already begun the legislative process with the data protection regulation and directive which have given us a unique perspective on privacy issues internationally. For this reason the Inquiry from the outset was able to be more wide-ranging, covering the areas where the EU has direct competence but also touching on some areas where there are concerns for EU citizens.

The European Parliament has established itself as a key player in this debate following 7 months of hearings that have included a broad range of testimony including from Edward Snowden, intelligence and parliamentary scrutiny bodies from around the EU, whistle-blowers, NGOs and journalists including Glenn Greenwald and Alan Rusbridger. We have also had unprecedented access to the US authorities including the head of the NSA, General Keith Alexander, the White House review team and senior US politicians including Congressmen Sensenbrenner and tech industry executives.

For Europe, the Snowden allegations came at a critical time when the EU had already decided to completely overhaul its own outdated data protection, internet and privacy laws. This new information has revealed the previously unknown extent of surveillance of communications of ordinary people by intelligence authorities across the world and has resulted in a lack of trust that Heads of Governments and the EU are not ensuring adequate protections for citizens and respect for the fundamental values enshrined both in the Charter of Fundamental Rights and the European Convention of Human Rights.

The main findings and recommendations of this Inquiry were detailed in a comprehensive report, see below, which is extremely broad in its mandate and covers several issues including a call on both the US and EU Member States to end blanket mass surveillance, condemning the vast blanket collection of personal data of innocent people. The Resolution also concentrates on data transfers between EU and the US, calling for the suspension of both the Safe Harbour principles and the TFTP agreement, the swift adoption of the EU data protection package, the conclusion of the EU US agreement on data protection umbrella agreement, to provide EU citizens with judicial redress for when their personal data is transferred to the US, a call for stronger protection mechanisms for journalists and whistle-

blowers and stronger IT security in the EU. These proposals have been combined to form a Digital Habeas Corpus Bill of Rights for EU citizens, which is a crucial proposal that will be reinforced in the next mandate of this Parliament.

In an age of increased mass surveillance and dwindling trust, the privacy rights of citizens must be a political priority. This Inquiry and the subsequent Resolution adopted by a large majority in the European Parliament, ensures this by providing a road map of measures that must be followed-up in the next mandate. The Snowden revelations have given us the opportunity to both react and build something positive from this unprecedented period. Throughout this process I have found that there has been genuine agreement that something has gone wrong with the way the NSA and certain EU Member States intelligence authorities are operating. It is the EU's turn to say something concrete to citizens about mass surveillance, and what we feel needs to be fixed with a digital bill of rights fit for the digital age.

# European Parliament resolutions

**European Parliament resolution of 12 March 2014 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[1],

– 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[2],

– having regard to the Commission communication on 'Internet Policy and Governance – Europe's role in shaping the future of Internet Governance' (COM(2014)0072);

[1] http://www.un.org/en/documents/udhr/

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

– 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 2013[1],

– 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[2], 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[3], Polish and British[4] courts, as well as before the European Court of Human Rights[5], 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[6], and in particular to Title III thereof,

– having regard to Commission Decision 2000/520/EC 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 on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU (COM(2013)0847), and to the Commission communication of 27 November 2013 on rebuilding trust in EU-US data flows (COM(2013)0846),

---

[1] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

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

[3] 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.

[4] Cases by Privacy International and Liberty in the Investigatory Powers Tribunal.

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

[6] OJ C 197, 12.7.2000, p. 1.

– having regard to its resolution of 5 July 2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce[1], which took the view that the adequacy of the system could not be confirmed, and to the Opinions of the Article 29 Working Party, more particularly Opinion 4/2000 of 16 May 2000[2],

– 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[3] and 2012[4],

– 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[5], 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[6],

– 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)[7] 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[8],

– 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 by a third country, and actions based thereon or resulting therefrom[9],

---

[1] OJ C 121, 24.4.2001, p. 152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
[3] OJ L 204, 4.8.2007, p. 18.
[4] OJ L 215, 11.8.2012, p. 5.
[5] SEC(2013)0630, 27.11.2013.
[6] Opinion of Advocate General Cruz Villalón, 12 December 2013, Case C-293/12.
[7] OJ L 195, 27.7.2010, p. 3.
[8] OJ L 181, 19.7.2003, p. 34.
[9] OJ L 309, 29.11.1996, p. 1.

– 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[1],

– having regard to its resolutions of 5 September 2001[2] and 7 November 2002[3] 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[4],

– 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 impact on EU citizens' privacy[5], whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter

[1] Council document 16987/2013.
[2] OJ C 72 E, 21.3.2002, p. 221.
[3] OJ C 16 E, 22.1.2004, p. 88.
[4] Texts adopted, P7_TA(2013)0203.
[5] Texts adopted, P7_TA(2013)0322.

– 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 the AFET working document on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens;

– having regard to its resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken[1],

– 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[2],

– having regard to its resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe[3],

– 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[4],

– 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 information flows and data, which today dominate everyday life and are part of any person's integrity, need to be as secure from intrusion as private homes;

C. whereas the ties between Europe and the United States of America are based on the spirit and principles of democracy, the rule of law, liberty, justice and solidarity;

[1] Texts adopted, P7_TA(2013)0444.
[2] Texts adopted, P7_TA(2013)0449.
[3] Texts adopted, P7_TA(2013)0535.
[4] OJ C 353 E, 3.12.2013, p. 156.

D. 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;

E. whereas mutual trust and understanding are key factors in the transatlantic dialogue and partnership;

F. 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;

G. 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 and the impact of mass surveillance on citizens and societies;

H. 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;

I. 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;

J. whereas President Obama has recently announced a reform of the NSA and its surveillance programmes;

K. 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;

L. 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***

M. 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[1]; 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;

N. 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[2];

O. 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 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

[1] Klayman et al. v Obama et al., Civil Action No 13-0851, 16 December 2013.
[2] ACLU v. NSA No 06-CV-10204, 17 August 2006.

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;

P. 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[1], 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;

Q. 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;

R. 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*

S. 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;

T. 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

[1] http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong

of democracy; whereas mass surveillance of human beings is incompatible with these cornerstones;

U. 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[1];

V. 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*

W. 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 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;

X. 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);

Y. 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';

Z. whereas the concepts of 'national security', 'internal security', 'internal security of the 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;

AA. 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;

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

AB. 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*

AC. 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***

AD. 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[1], for breach of EU law – which includes any violation of the fundamental rights enshrined in the EU Charter;

AE. 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;

AF. whereas the mass collection of personal data for commercial purposes and in the fight 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*

AG. whereas the US data protection legal framework does not ensure an adequate level of protection for EU citizens;

AH. whereas, in order to enable EU data controllers to transfer personal data to an entity in the US, the Commission, in its Decision 2000/520/EC, 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;

[1] See notably Joined Cases C-6/90 and C-9/90, Francovich and others v. Italy, judgment of 28 May 1991.

AI. 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;

AJ. 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;

AK. whereas Commission Decision 2000/520/EC 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;

AL. whereas Commission Decision 2000/520/EC 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;

AM. 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;

AN. 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;

AO. 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;

AP. 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;

AQ. 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*

AR. 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;

AS. whereas Commission Decisions 2013/65/EU[1] and 2002/2/EC[2] have 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*

AT. 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;

AU. whereas such safeguards may in particular result from appropriate contractual clauses;

AV. 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

[1] OJ L 28, 30.1.2013, p. 12.
[2] OJ L 2, 4.1.2002, p. 13.

contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;

AW. 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;

AX. 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;

AY. 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*

AZ. 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;

BA. 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;

BB. 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;

BC. 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[1];

BD. 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;

BE. 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[2];

BF. 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;

BG. 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*

BH. whereas the EU-US Agreement on mutual legal assistance in criminal matters of 6 June 2003[3] 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')*

[1] 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'.

[2] http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de-contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la

[3] OJ L 181, 19.7.2003, p. 25.

BI. 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;

BJ. 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;

BK. 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;

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

***Data protection reform***

BM. 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[1], which will replace Directive 95/46/EC and establish a uniform law throughout the EU, and a Directive[2] 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;

BN. 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;

BO. 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[3];

[1] COM(2012)0011, 25.1.2012.
[2] COM(2012)0010, 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

***IT security and cloud computing***

BP. whereas Parliament's abovementioned resolution of 10 December 2013 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;

BQ. 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;

BR. 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 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;

BS. 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;

BT. 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';

BU. 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;

BV. 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***

BW. 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;

BX. 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;

BY. 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;

BZ. 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;

CA. 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;

CB. 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[1] 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

[1] No 1 BvR 518/02 of 4 April 2006.

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;

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'[1]; 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 institutions and experts who have contributed to this Inquiry; deplores 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;

18. 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;

19. 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;

***Recommendations***

20. Calls on the US authorities and the EU Member States, where this is not yet the case, to prohibit blanket mass surveillance activities;

21. Calls on the EU Member States, and in particular those participating in the so-called '9-eyes' and '14-eyes' programmes[2], 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

[1] Judgement in Case C-300/11, ZZ v Secretary of State for the Home Department, 4 June 2013.
[2] 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.

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;

22. 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;

23. 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;

24. 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 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;

25. 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;

26. Calls for the termination of mass interception and processing of webcam imagery by any secret service; calls upon the Member States to fully investigate whether, how and to what extent their respective secret services have been involved in the collection and processing of webcam images, and to delete all stored images collected through such mass surveillance programmes;

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 upon the Member States to establish effective mechanisms whereby those responsible for (mass) surveillance programmes that are in violation of the rule of law and the fundamental rights of citizens are held accountable for this abuse of power;

31. 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;

32. 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;

33. 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;

34. 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;

35. 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*

36. 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;

37. 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';

38. 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;

39. Takes the view that the Commission has failed to act to remedy the well-known deficiencies of the current implementation of Safe Harbour;

40. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 2000/520/EC, 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;

41. 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;

42. 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*

43. 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;

44. 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;

45. 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;

46. 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/EU and 2002/2/EU, 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*

47. 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;

48. 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;

49. 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;

50. 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*

51. 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*

52. 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*

53. 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;

54. Reiterates its resolution of 23 October 2013 and asks the Commission for the suspension of the TFTP Agreement;

55. 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')*

56. Considers that a satisfactory solution under the 'Umbrella agreement' is a precondition for the full restoration of trust between the transatlantic partners;

57. 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;

58. 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;

59. 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*

60. 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;

61. 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;

62. 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;

63. 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*

64. 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;

65. Calls on all public bodies in the Union not to use cloud services where non-EU laws might apply;

66. 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;

67. 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;

68. 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;

69. 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;

70. 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;

71. 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;

72. 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)*

73. 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;

74. 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***

75. 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;

76. 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;

77. Calls for the setting up of a Group of Members and experts to examine, in a transparent manner and in collaboration with national parliaments, recommendations 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; considers that the group should examine, in particular, the possibility of minimum European standards or guidelines for 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, criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'[1], as well as principles regarding the limits on the duration and scope of any surveillance ensuring that they are proportionate and limited to its purpose;

78. Calls on this Group to prepare a report for and to assist in the preparation of a conference to be held by Parliament with national oversight bodies, whether parliamentary or independent, by the beginning of 2015;

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 HR/VP to regularly account for the activities of the EU Intelligence Analysis Centre (IntCen), which is part of the European External Action Service, to the responsible bodies of Parliament, including its full compliance with fundamental rights and applicable EU data privacy rules, allowing for improved oversight by Parliament of the external dimension of EU policies; urges the Commission and the HR/VP to present a proposal for a legal basis for the activities of IntCen, should any operations or future competences in the area of intelligence or data collection facilities of its own be envisaged which may have an impact on the EU's internal security strategy;

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

[1] The Global Principles on National Security and the Right to Information, June 2013.

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[1]; 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.;

[1] European Parliament position of 25 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) (Texts adopted, P7_TA(2014)0121).

***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 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; calls on all responsible EU institutions and Member States to invest in EU local and independent technologies, and to develop massively and increase detection 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 June 2015 at the latest with an intermediate report 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 June 2015 at the latest with an intermediate report by December 2014, 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 Commission to present a legal proposal for an EU routing system including the processing of call detail records (CDRs) at EU level that will be a substructure of the existing internet and will not extend beyond EU borders; notes that all routing data and CDRs should be processed in accordance with EU legal frameworks;

109. 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;

110. 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***

111. 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;

112. 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*

113. 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;

114. 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;

115. 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;

116. 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;

117. 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;

118. Considers that clear political signals are needed from our American partners to demonstrate that the US distinguishes between allies and adversaries;

119. 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;

120. 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;

121. 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*

122. 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;

123. 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;

124. 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;

125. 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;

126. 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;

127. 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*

128. Calls on the Commission to present, by January 2015 at the latest, an EU strategy for democratic governance of the internet;

129. 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 Article17 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;

130. 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***

131. Decides to submit to EU citizens, institutions and Member States the above-mentioned recommendations as a Priority Plan for the next legislature; calls on the Commission and the other EU institutions, bodies, offices and agencies referred to in this

resolution, in accordance with Article 265 TFEU, to act upon the recommendations and calls as contained in this resolution;

132. 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;

133. 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 2014-March 2015: 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;

o

o o

134. 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;

135. Instructs its Committee on Civil Liberties, Justice and Home Affairs to address Parliament in plenary on the matter a year after the adoption of this resolution; considers it essential to assess the extent to which the recommendations adopted by Parliament have been followed and to analyse any instances where such recommendations have not been followed

# Explanatory statement

*'The office of the sovereign, be it a monarch or an assembly, consisted 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[1] 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 0ctober 2013 to meet with representatives of both the executive and the legislative branch (academics, lawyers, security experts, business representatives)[2]. 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[3] have been co-authored by the rapporteur, the shadow-rapporteurs[4] from the various political groups and 3 Members from the AFET Committee[5] 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 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

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_en.pdf
[2] See Washington delegation report.
[3] See Annex I.
[4] List of shadow rapporteurs: Axel Voss (EPP), Sophia in't Veld (ALDE), Jan Philipp Albrecht (GREENS/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).
[5] List of AFET Members: José Ignacio Salafranca Sánchez-Neyra (EPP), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).

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[1], Up until now only a few national 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

[1] 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 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'.

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 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 fundaments 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;

## European Parliament 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' privacy (2013/2682(RSP))

*The European Parliament*,

– having regard to Articles 2, 3, 6 and 7 of the Treaty on European Union (TEU) and to Article 16 of the Treaty on the Functioning of the European Union (TFEU),

– having regard to the Charter of Fundamental Rights of the European Union and to the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),

– having regard to Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the additional protocol thereto of 8 November 2001,

– having regard to EU law on the right to privacy and data protection, in particular Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and to the free movement of such data, Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Directive 2002/58/EC on privacy and electronic communications, and Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,

– having regard to the Commission proposals for a regulation and for a directive on the reform of the data protection regime in the EU,

– having regard to the EU-US Mutual Legal Assistance Agreement allowing exchange of data for the prevention and investigation of criminal activities, to the Convention on Cybercrime (CETS No 185), to the EU-US Safe Harbour Agreement (2000/520/EC) and to the current revision of the Safe Harbour scheme,

– having regard to the US Patriot Act and to the Foreign Intelligence Surveillance Act (FISA), including Section 702 of the 2008 FIS Amendment Act (FISAAA),

– having regard to the ongoing negotiations on an EU-US framework agreement on the protection of personal data when transferred and processed for police and judicial cooperation purposes,

– having regard to its previous resolutions on the right to privacy and data protection, in particular that of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (Echelon interception system)[1],

– having regard to the statements by the President of the European Council, Herman van Rompuy, the President of the European Parliament, Martin Schulz, the Vice-President of the Commission / Commissioner for Justice, Fundamental Rights and

[1] OJ C 72 E, 21.3.2002, p. 221.

Citizenship, Viviane Reding, and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, Catherine Ashton,

– having regard to Rule 110(2) and (4) of its Rules of Procedure,

A. whereas the transatlantic partnership between the EU and the US must be based on mutual trust and respect, loyal and mutual cooperation, respect for fundamental rights and the rule of law;

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

C. whereas adherence to these principles is currently in doubt after reports in the international press in June 2013 revealed evidence that, through programmes such as PRISM, the US authorities are accessing and processing on a large scale the personal data of EU citizens using US online service providers;

D. whereas this doubt concerns not only the actions of US authorities, but also those of several EU Member States, which according to the international press have cooperated with PRISM and other such programmes or obtained access to the databases created;

E. whereas, furthermore, several Member States have surveillance programmes of a similar nature to PRISM or are discussing the setting-up of such programmes;

F. whereas particular questions have been raised regarding the compatibility with EU law of the practice of the UK intelligence agency Government Communications Headquarters (GCHQ) directly tapping into undersea transatlantic cables carrying electronic communications, under a programme codenamed Tempora; whereas other Member States reportedly access transnational electronic communications without a regular warrant but on the basis of special courts, share data with other countries (Sweden), and may enhance their surveillance capabilities (the Netherlands, Germany); whereas concerns have been expressed in other Member States in relation to the interception powers of secret services (Poland);

G. whereas there are indications that EU institutions and EU and Member State embassies and representations have been subjected to US surveillance and spying activities;

H. whereas Commissioner Reding has written a letter to the US Attorney General, Eric Holder, raising European concerns and asking for clarification and explanations regarding PRISM and other such programmes involving data collection and searching, and the laws under which such programmes may be authorised; whereas a full response from the US authorities is still pending, despite the discussions which took place at the EU-US Justice Ministerial meeting in Dublin on 14 June 2013;

I. whereas, under the Safe Harbour Agreement, the Member States and the Commission are entrusted with the duty of guaranteeing the security and integrity of personal data; whereas the companies involved in the PRISM case, as reported in the international press, are all parties to the Safe Harbour Agreement; whereas, under Article 3 of that agreement, the Commission has a duty, should the provisions of the agreement not be complied with, to reverse or suspend it;

J. whereas the EU-US Mutual Legal Assistance Agreement, as ratified by the Union and the US Congress, stipulates modalities for gathering and exchanging information, and

for requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another;

K. whereas it would be unfortunate if the efforts to conclude a Transatlantic Trade and Investment Partnership (TTIP), which demonstrates the commitment to further strengthen the partnership between the EU and the US, were to be affected by the recent allegations;

L. whereas on 14 June 2013 Commissioner Malmström announced the setting-up of a transatlantic group of experts;

M. whereas Commissioner Reding has written to the UK authorities to express concern about media reports on the Tempora programme and asking for clarification of its scope and operation; whereas the UK authorities have defended the GCHQ's surveillance activities and affirmed that they operate under strict and lawful guidelines;

N. whereas data protection reform is under way at EU level, through the revision of Directive 95/46/EC and its replacement with the proposed general Data Protection Regulation and the Data Protection Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data;

1. Expresses, while confirming its ongoing support for transatlantic efforts in the fight against terrorism and organised crime, serious concern over PRISM and other such programmes, since, should the information available up to now be confirmed, they may entail a serious violation of the fundamental right of EU citizens and residents to privacy and data protection, as well as of the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, and the freedom to conduct business;

2. Strongly condemns the spying on EU representations as, should the information available up to now be confirmed, it would imply a serious violation of the Vienna Convention on Diplomatic Relations, in addition to its potential impact on transatlantic relations; calls for immediate clarification from the US authorities on the matter;

3. Calls on the US authorities to provide the EU, without undue delay, with full information on PRISM and other such programmes involving data collection, in particular as regards their legal basis, necessity and proportionality and the safeguards implemented to protect the fundamental rights of EU citizens, such as limitation of scope and duration, conditions for access, and independent supervision, as provided for under the Convention on Cybercrime and as requested by Commissioner Reding in her letter of 10 June 2013 to Attorney General Eric Holder; calls on the US authorities to suspend and review any laws and surveillance programmes that violate the fundamental right of EU citizens to privacy and data protection, the sovereignty and jurisdiction of the EU and its Member States, and the Convention on Cybercrime;

4. Calls on the Commission, the Council and the Member States to give consideration to all the instruments at their disposal in discussions and negotiations with the US, at both political and expert level, in order to achieve the above-mentioned objectives, including the possible suspension of the passenger name record (PNR) and terrorist finance tracking programme (TFTP) agreements;

5. Demands that the transatlantic expert group, as announced by Commissioner Malmström and in which Parliament will participate, be granted an appropriate level of security clearance and access to all relevant documents in order to be able to conduct its work properly and within a set deadline; further demands that Parliament be adequately represented in this expert group;

6. Calls on the Commission and the US authorities to resume, without delay, the negotiations on the framework agreement on the protection of personal data when transferred and processed for police and judicial cooperation purposes; calls on the Commission, during these negotiations, to make sure that the agreement meets at least the following criteria:

   (a) granting EU citizens the right to information when their data is processed in the US;

   (b) ensuring that EU citizens' access to the US judicial system is equal to that enjoyed by US citizens;

   (c) granting the right to redress, in particular;

7. Calls on the Commission to ensure that EU data protection standards, and the negotiations on the current EU data protection package, are not undermined as a result of the Transatlantic Trade and Investment Partnership (TTIP) with the US;

8. Calls on the Commission to conduct a full review of the Safe Harbour Agreement in the light of the recent revelations, under Article 3 of that agreement;

9. Expresses serious concern at the revelations relating to the alleged surveillance programmes run by Member States, either with the help of the US National Security Agency or unilaterally; calls on all the Member States to examine the compatibility of such programmes with EU primary and secondary law, in particular Article 16 TFEU on data protection, and with the EU's fundamental rights obligations deriving from the ECHR and the constitutional traditions common to the Member States;

10. Stresses that all companies providing services in the EU must comply with EU law without exception and are liable for any breaches;

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

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

13. Stresses that in democratic and open states based on the rule of law, citizens have a right to know about serious violations of their fundamental rights and to denounce them, including those involving their own government; stresses the need for procedures allowing whistleblowers to unveil serious violations of fundamental rights and the need to provide such people with the necessary protection, including at international level; expresses its continued support for investigative journalism and media freedom;

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

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

16. Instructs its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter in collaboration with national parliaments and the EU-US expert group set up by the Commission and to report back by the end of the year, by:

    (a) gathering all relevant information and evidence from both US and EU sources (fact-finding);

    (b) investigating the alleged surveillance activities of US authorities as well as any carried out by certain Member States (mapping of responsibilities);

    (c) assessing the impact of surveillance programmes as regards: the fundamental rights of EU citizens (in particular the right to respect for private life and communications, freedom of expression, the presumption of innocence and the right to an effective remedy); actual data protection both within the EU and for EU citizens outside the EU, focusing in particular on the effectiveness of EU law in respect of extraterritoriality mechanisms; the safety of the EU in the era of cloud computing; the added value and proportionality of such programmes with regard to the fight against terrorism; the external dimension of the area of freedom, security and justice (assessing the validity of adequacy decisions for EU transfers to third countries, such as those carried out under the Safe Harbour Agreement, international agreements and other legal instruments providing for legal assistance and cooperation) (damage and risk analysis);

    (d) exploring the most appropriate mechanisms for redress in the event of confirmed violations (administrative and judicial redress and compensation schemes);

    (e) putting forward recommendations aimed at preventing further violations, and ensuring credible, high-level protection of EU citizens' personal data via adequate means, in particular the adoption of a fully-fledged data protection package (policy recommendations and law-making);

    (f) issuing recommendations aimed at strengthening IT security in the EU's institutions, bodies and agencies by means of proper internal security rules for communication systems, in order to prevent and remedy unauthorised access and the disclosure or loss of information and personal data (remedying of security breaches);

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

Jan Philipp Albrecht (Greens/EFA), Shadow Rapporteur

Sophie in't Veld (ALDE), Shadow Rapporteur

Cornelia Ernst (GUE/NGL), Shadow Rapporteur

The Rapporteur, Claude Moraes (S&D)

Timothy Kirkhope (ECR), Shadow Rapporteur

Axel Voss (EPP), Shadow Rapporteur


The LIBE Chair, Juan Fernando Lopez Aguilar (S&D), presiding a LIBE Committee Inquiry hearing

**Working document on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights**

EUROPEAN PARLIAMENT 2009 - 2014

*Committee on Civil Liberties, Justice and Home Affairs*

11.12.2013

# WORKING DOCUMENT

on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

## 1. Mass surveillance of EU Citizens

Recent disclosures have revealed the existence of systems of mass surveillance of citizens by the US and certain EU Member States. Prompted by an increasing focus on security, in particular following the 9/11 attacks these activities were enabled by the growth of internet usage, developments in communication technology and a weak oversight of intelligence services.

In only the past 10 or 20 years, citizens' lives have completely changed through the use of internet, email, communication through social media, online shopping, VoIP "phone calls", information technologies and data storage in the cloud. Whilst these are extremely positive developments, particularly in terms of convenience and cost, they entail an increasing amount of electronically held data, much of which contains personal information and private data. In parallel to this, advancements in technology have increased intelligence agencies' capacity to engage in large scale interception and analysis of such data.

These technological developments seemed to have contributed, along with other factors, 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. While intelligence services perform an indispensable function in protecting the democratic society against internal and external threats, they have to operate within the rule of law; otherwise they will lose legitimacy and erode the exact democratic society they are trying to protect. This process of increasing mass surveillance has not been subject to any public debate or democratic decision-making, but decisions have largely been taken in small circles and behind closed doors. It appears that legal frameworks, which were put in place at times when technology was not so far advanced as today, are being used to justify systems of mass surveillance even when this was not the intention behind their initial legal interpretation. Due to the fact that oversight mechanisms in many states have not kept up with the increased capabilities of intelligence services, these systems of mass surveillance have continued to develop.

Such a public debate needs to take place now. We need to discuss the purpose and scale of surveillance and its place in a democratic society. We need to discuss the acceptable measures to fight crime and terrorism and where the lines need to be drawn to preserve the right to private life and protection of personal data in a digitalised world. We need to discuss how our intelligence services are supposed to collaborate without undermining the rule of law. We need to discuss how transatlantic business is conducted and how data flowing between countries and continents is kept safe and the governing laws respected.

The availability of proper information is a vital condition for this debate. The inquiry of the LIBE Committee has aimed to collect and assess such information. This working document is one element of this process. It presents an overview of the surveillance activities and discusses the impact of these on EU citizens' fundamental rights.

## 2. Surveillance Programmes

In recent months revelations were made about numerous different programmes. Several types of alleged surveillance issues can be distinguished as having an impact on the fundamental rights of EU citizens: the mass surveillance of EU citizens by the National Security Agency (NSA), the cooperation of EU Member States authorities in the surveillance programmes operated by the NSA, the surveillance programmes that are conducted by EU Member States themselves as well as surveillance programmes by other

third states. Below some of the programmes of the NSA as well as some EU Member States will be presented.

Mass surveillance of EU citizens by the NSA

Several programmes of the NSA[1] focus on online activities. The **PRISM programme** is alleged to give the NSA direct access to the central servers of nine leading US internet companies allowing them to collect customer material including search history, the content of emails, file transfers and live chats.[2] The US administration confirmed the existence of the PRISM programme. However they stated that it was not an undisclosed collection or data mining programme.[3]

According to reports, the **Xkeyscore programme** allows NSA analysts, without prior authorization, to search through vast databases containing emails, online chats and browsing histories of millions of individuals as well as their metadata[4]. It was described as the NSA's widest reaching system that can cover "nearly everything a typical user does on the internet". In response the NSA confirmed the existence of the programme as part of the NSA's lawful foreign signals intelligence collection system saying it was limited to personnel who required access for assigned tasks[5].

**BULLRUN** is an alleged decryption programme run by the NSA in an effort to break into widely used encryption technologies that would allow the NSA to circumvent online encryption used by millions of people in their online transactions and emails.[6] No response was issued from the NSA in relation to the alleged Bullrun programme. The reports by the Guardian, the New York Times and ProPublica all stated that intelligence officials requested that the story was not published for national security reasons.

According to section 702 of FISA, a service provider might be required to "immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition" of foreign intelligence information. No clarification has been made on whether this provision could compel disclosure of cryptographic keys.[7]

**Boundless Informant** is a powerful data-mining tool deployed by the NSA to record and analyse global electronic information. It details and even maps by country the vast amount of information, mainly metadata, which it collects from computer and telephone networks. According to the reports, "the tool allows users to select a country on a map and view the metadata volume and select details about the collections against that country."[8] In March 2013, 97bn pieces of intelligence were collected from computer networks worldwide.

---

[1] For an overview of the US legal situation see the Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection
http://register.consilium.europa.eu/pdf/en/13/st16/st16987.en13.pdf

[2] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1

[3] http://online.wsj.com/public/resources/documents/prismfactsheet0608.pdf

[4] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[5] http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml

[6] http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[7] The US surveillance programmes and their impact on EU citizens' fundamental rights
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

[8] http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

**MUSCULAR**, as reported by the Washington Post on 31 October[1], is a joint programme operated by the NSA with the GCHQ to intercept, from private links, data traffic flowing between the servers of Yahoo, Google, Microsoft Hotmail and Windows Live Messenger, amongst others. The access point, DS-200B is located outside the US, which renders the programme out of jurisdiction of the FISC court, and relies on an unnamed telecommunications provider to provide a secret access to a cable or switch through which the communications traffic passes. NSA documents about the effort refer directly to "full take," "bulk access" and "high volume" operations on Yahoo, Google and Microsoft networks. It was reported that numerous analysts working on the programme had complained that MUSCULAR produces too much data, much of which with low intelligence value.

In October 2013, media reports in France, Spain and Italy alleged that the NSA was intercepting huge volumes of **telephone calls**. For example, it was alleged that the NSA collected 70.3 million phone records in France from 10 December 2012 to 8 January 2013. In response General Keith Alexander, Chief of the NSA, stated the data was collected jointly by the NSA and the individual Member State intelligence agencies for purposes of defence and support of military operations[2].

Surveillance activities of EU Member States

According to press reports, the UK intelligence agency, **GCHQ**, was alleged to have access to communications collected through the PRISM programme allowing them to circumvent the national legal framework on accessing personal material from an internet company based outside the UK. Reports have also pointed to the joint involvement of GCHQ with the NSA in the MUSCULAR programme. The Intelligence and Security Committee (ISC) of the UK Parliament confirmed the use by the GCHQ of surveillance material obtained from the US PRISM programme but found that the GCHQ had not circumvented UK law by doing so.

GCHQ is alleged to engage in an upstream surveillance activity known as the **Tempora programme** which allows them access to large fibre optic cables that carry huge amounts of internet users' private communications and share it with the NSA. Due to the sheer volume of data collected, the content of the information is said to be deleted after 3 days, and metadata are usually kept for 30 days[3].

GCHQ is alleged to be operating a corresponding decryption programme to BULLRUN known as **Edgehill**. The programmed aims at decoding encrypted traffic used by companies to provide remote access to their systems and to "continue to work on understanding" major communication providers.

Reports on the activities of the **National Defense Radio Establishment (FRA), Sweden** have alleged that they are collecting/receiving data from fibre optic cables crossing Swedish borders from the Nordic and Baltic States and Russia and forwarding the data to the USA[4].

---

[1] http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

[2] http://www.washingtonpost.com/world/national-security/top-intelligence-officials-called-to-testify-on-nsa-surveillance-programs/2013/10/29/e9e9c250-40b7-11e3-a751-f032898f2dbc_story.html

[3] http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[4] Source: M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', Nordic Yearbook of Law and Information Technology, Bergen 2010, pp. 96-134
Source: Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013

They also, allegedly, intercept and routinely monitor the Norwegian phone and internet cables that pass through Sweden as well as intercept mobile phone data and calls of other Nordic countries where the signal is transmitted through Swedish GSM links.

Allegations have emerged in **France that the General Directorate for External Security (DGSE)** intercepts and collects metadata from email, text messages and phone bills by use of a supercomputer capable of collecting, processing and storing data. The data is intercepted and collected by both satellite stations and interception of fibre-optic submarine cables. Also, the database is alleged to be accessed by six other intelligence services including the customs service and the anti-money laundering service[1].

In **Germany**, press reports have alleged that the **Bundesnachrichtendienst (BND)** has set up offices at the DE-CIX (German Commercial Internet Exchange) to divert incoming traffic, copy the data and analyse it later in the BND headquarters[2]. Reports also indicate strong cooperation between the German intelligence services and their US counterparts with reports of millions of metadata collected by the BND were being transferred to the NSA via data collection sites on German territory[3].

## 3. Impact on fundamental rights in the EU

Developments in technology have enabled states to know more about citizens than was ever possible in history. While previously it required considerable efforts and physical proximity to spy on a person, the technology of today allows such action on a scale and depth impossible before.

The systems of mass and indiscriminate surveillance impact significantly on the fundamental rights of citizens. While legal frameworks are in place, questions still remain as to whether the various programmes respect the spirit and were intended by the relevant legal frameworks; including International and European law notably with regards to the question of whether such programmes may be considered proportionate, necessary and appropriate in democratic societies.

The systems of mass surveillance described above have first and foremost an impact on citizens' privacy. By being able to collect data 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. They can know where people are with advanced location programmes[4], with whom they speak and for how long, what they do, what they buy, what they read and even what they most probably think.

Surveillance, therefore, has also an effect on other fundamental rights such as freedom of expression, of opinion, of religion, of association, data protection, right to fair trial, access to an effective remedy etc. Of particular concern, as highlighted during the inquiry, is the impact on the freedom of the press, in particular through the chilling effect created for

[1] Source: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' Le Monde, 4 July 2013.
[2] http://www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html
[3] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html
[4] NSA gathering 5bn cell phone records daily, Snowden documents reveal http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden

journalists providing information needed for an informed debate, through techniques used either to intimidate or to slow down reporting.

While intelligence services are essential in protecting against internal and external threats they have to operate at all times within the rule of law. Even the existence of a threat to national security is not a sufficient reason for an intelligence service to break the law. Illegal activities on the part of an intelligence services not only undermine the same democratic society that the services aim to protect, but also erode the legitimacy and democratic trust and support that the intelligence services need.

A key question which has been discussed during the inquiry is of whether the surveillance programmes violate the law, in particular international law and the European Convention on Human Rights. While obviously only courts are able to answer this question in a definitive manner, there have been strong statements indicating that we are indeed in a scenario where human rights and the rule of law have been violated.

3.1 The protection of privacy under international law

In terms of international law, testimonies were submitted to the Inquiry concluding that the US is in breach of its obligation under Article 17 of the UN International Covenant on Civil and Political rights (ICCPR) to prohibit arbitrary or unlawful interference with anyone's privacy or correspondence as it fails to comply with the permissible limitations test.[1]

In this regard the Inquiry awaits the assessment of the US compliance with Article 17 of the ICCPR by the Human Rights Committee and supports calls for an update to the ICCPR to tackle the transparency and proportionality concerns raised by mass surveillance practices be it by means of a new General Comment introducing a rigorous test for permissible limitations upon privacy rights (including data protection) or a new Additional or Amending Protocol to the ICCPR.

All EU Member States to the ICCPR are also covered as far as their own surveillance activities are concerned whether targeting their own or other Member States' citizens. As to the cooperation of Member States authorities in the surveillance programmes operated by the NSA, the Human Rights Committee states in its General comment, that "State parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant", therefore such cooperation is also unlawful under the ICCPR.

3.2 The protection of privacy under the European Convention on Human Rights (ECHR)

The European Court of Human Rights (ECtHR) has consistently ruled that national security and intelligence agencies are bound to respect the rights and freedoms as laid down in the ECHR. Not only this, but there is a positive obligation on Member States to protect their citizens from surveillance undertaken by third parties, be they states or private entities[2].

[1] See testimony by Professor by Martin Scheinin (EUI), formerly UN Special Rapporteur on human rights and counter-terrorism and Douwe Korff, Professor of International Law, London Metropolitan University, London (UK) in the LIBE Committee on the Electronic Mass Surveillance of EU Citizens on 14/10/2013

[2] *Van Hannover v Germany*, Judgment of 24 June 2004, (2005) 40 EHRR 1, *X & Y v Netherlands ,* Judgment of 26 March 1985, (1985) 8 EHRR 235, see also the Council of Europe's Human Rights Handbook No. 7 on Positive obligations under the European Convention on Human Rights, by Jean-Francois Akandji-Kombe, available at: http://www.coehelp.org/file.php/54/resources/Handbooks/pos_obl_eng.pdf

Given the extent of the mass collection of personal data that are collected through the surveillance programmes, serious concerns have been raised as to whether these activities respect EU citizens' right to private life and privacy of their communications under the ECHR[1]. Whilst the right to privacy is not absolute, this does not infer an automatic suspension on grounds of national security. According to the ECtHR, the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied and thereby may amount in itself to an interference with the exercise of individuals' rights under Article 8, irrespective of any measures actually taken against them[2].

Any interference with this right, by means of surveillance practices, should be prescribed by law, limited, necessary, proportionate and subject to continual assessment. Given that telecommunications technologies have rapidly developed to allow the indiscriminate mass collection of communication data, it is imperative that EU Member States adopt precise legislative frameworks that will ensure effective legal scrutiny to safeguard private information[3].

More particularly, any surveillance must be "in accordance with law". The ECtHR has interpreted this element as accessibility of the relevant provisions and foreseeability of their consequences. The relevant legal rules shall always define categories of offences or persons likely to be subject to surveillance measures[4]. Further, there must be strict limits on the duration of any ordered surveillance[5]. Further, interference shall serve a "legitimate aim in a democratic society", while being "necessary" and "proportionate" in relation to that aim. "Necessary" means corresponding "to a pressing social need"[6] while "proportionate" shall be defined by reference to the legitimate aim pursued. In the same regard, adequate guarantees must be laid down to prevent any misuse of power[7].
Thus, mere usefulness or desirability is not sufficient justification. The ECtHR has also found in several cases that, for instance, rules should provide that the duration of the interception[8] and of the storage of information[9] is limited or, at least, that adequate safeguards are put in place to control the discretion of authorising authorities in this regard[10].
3.3 The protection of personal data

The European data protection framework is founded on a list of core principles including; data must be processed fairly and lawfully, personal data must be obtained for a specific and lawful purpose, personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed and appropriate measures should be taken against unauthorised processing of personal data.

[1] Article 8 of the ECHR
[2] Weber and Saravia, para. 78
[3] Uzun v Germany (2012) 54 EHRR 121 at [61], in Weber v Germany (2008) 46 EHRR SE5 at [93]
[4] *Kennedy v. The United Kingdom,* judgment of 18 May 2010, application no. 26839/05
[5] *Weber and Saravia v. Germany, Liberty and Others v. UK*
[6] *Leander v. Sweden,* judgment 26 March 1987, § 48, Series A no. 116
[7] Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no.176-A, and Eur. Court HR, Huvig v. France judgment of 24 April 1990, Series A no.176-B
[8] Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no.176-A, and Eur. Court HR, Huvig v. France judgment of 24 April 1990, Series A no.176-B
[9] Eur. Court HR, Rotaru v. Romania judgment of 4 May 2000, application no. 28341/95, Eur. Court HR, Amann v. Switzerland judgment of 16 February 2000, application no. 27798/95
[10] Eur. Court HR, Kennedy v. The United Kingdom, judgment of 18 May 2010, application no. 26839/05.

The alleged practices of mass surveillance as described above without any specific, targeted justification are at odds with these founding principles. There is a positive obligation on the EU and its Member States to protect the personal data of their citizens and to ensure that any international transfer of data respects these core principles.

3.4 The right to effective remedy

An effective remedy is a fundamental right under the EU Charter and the ECHR, awarded to all persons, regardless of their nationality, also applicable to cases where data privacy rights have been violated. The ECJ has also established, as a basic principle, that remedies must be available in all cases of breach of EU law. All these EU safeguards are in direct contrast to the legal framework in the US which reciprocally denies European citizens, who are not resident in the US, the right to an effective remedy.

If EU citizens are under surveillance for any lawful reason they must have the right to challenge the information by intelligence authorities. Given the mass international transfer of data of EU citizens to US authorities, the lack of appropriate redress mechanism for European citizens is an issue of extreme concern. As a step towards reciprocity, the US must explore the most appropriate mechanisms to extend at least the legal protection afforded to persons within the US also to EU citizens outside the US, in order to provide an effective legal redress mechanism for EU citizens whose data has been held or accessed by the US authorities.

3.5 The protection against discrimination of EU citizens

Reciprocity is a crucial element of international relations and something that has been fundamentally lacking in the EU-US relationship. Whereas US legal protection concerning communication data applies only to US citizens and residents, in the EU, regardless of their nationality, everyone's personal data and the confidentiality of their communications are protected as fundamental rights.

According to the US legal framework the provisions of the First and Fourth Amendment do not protect EU citizens and it seems that relevance requirements are very low in case of US surveillance activity directed at EU citizens. For instance, under section 702 of the FISA Amendments Act, no probable cause seems to be required in order to target foreign citizens, as targeting and minimisation guidelines do not apply in the case of non-US persons.

European citizens have no right to be informed, nor can they challenge the surveillance activities conducted by US authorities in any way, despite the principle of non-discrimination and equality before the law, as laid down in Article 26 ICCPR.

3.6 Surveillance programmes and their compatibility with the Presumption of Innocence

The practice of untargeted, mass surveillance and the collection of bulk data of EU citizens may at least risk violating the fundamental principle of justice, notably in criminal proceedings, of “presumption of innocence”, which again covers all persons, irrespective of nationality[1].

[1] The presumption of innocence is considered to be a fundamental principle of criminal law and is recognised both in the ECHR and the Charter of Fundamental Rights of the European Union.

The role of mass surveillance leads to a shift in criminal law from its role of sanctioning specific acts on the basis of personal responsibility to reducing risks and identifying possible offenders, which can lead to all citizens, under continuous surveillance, being considered as suspects.

3.7 Freedom of Expression – impact on Journalism and Whistleblowers

There is a consensus on the need for transparency and for an informed debate on the extent of mass surveillance activities, and their impact on privacy. Such a debate is only possible if media freedom is respected. In particular, when supervisory mechanisms fail to prevent or rectify mass surveillance, the role of media and whistleblowers in unveiling eventual illegalities or misuses of power, notably when these infringe upon fundamental citizens' rights, is extremely important.

Throughout the Inquiry, the LIBE Committee has heard several statements by journalists, whistleblowers and the civil society on the need for strong protection of freedom of information and of media freedom in the sensitive area of intelligence activities. Furthermore the Editor of the Guardian, Alan Rusbridger, stated that the reactions from the US and UK authorities to the disclosures by Edward Snowden have had a chilling effect on journalism and he urged the European Parliament to do more to protect the media.

Freedom of expression and information, including media freedom, is protected both under the EU Charter of fundamental rights (Article 11) and the ECHR (Article 10). These were further substantiated by recent reports from the European Parliament[1], EctHR case-law, the Parliamentary Assembly of the Council of Europe (PACE) and various UN texts which all require Member States to protect freedom of expression, interferences being allowed only under restrictive conditions similar to those on privacy, including in the field of surveillance. Journalists must also be protected against intimidation tactics to ensure freedom of the press.

Throughout the Inquiry, it has become evident that whistleblowers play a crucial role in unveiling serious violations of fundamental rights and as a result are extremely vulnerable to retaliation attacks. The ECtHR has upheld whistleblowers' rights under the same conditions governing protection of the freedom of expression, ruling against interferences by the State/their employer[2]. The important role of the whistleblowers and the need for protecting them against dismissals and the related chilling effect has also been confirmed by the Court[3].

Whistleblowers' right to freedom of expression has also been substantiated with several other recent initiatives from the Council of Europe[4], PACE[5], the European Parliament[6] and civil society, including Transparency International[7]advocating for stronger whistleblower

[1] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0203+0+DOC+XML+V0//EN

[2] See for instance, Heinisch v. Germany, App. No. 28274/08, Eur. Ct. H.R. (2001)

[3] Guja v. Moldova, Application no. 14277/04, Judgment of 12 February 2008

[4] http://www.coe.int/t/DGHL/STANDARDSETTING/CDcj/Whistleblowers/CDCJ%20(2012)9E_Final.pdf

[5] http://assembly.coe.int/main.asp?link=/documents/adoptedtext/ta10/eres1729.htm

[6] European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report) (2013/2107(INI))

[7] Transparency International, "Whistleblowing in Europe, Legal protections for whistleblowers in the EU", 2013 http://www.transparency.org/whatwedo/pub/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu

protection. Whilst the European Commission has adopted sectoral provisions on whistleblowing, it is clear that a more comprehensive approach could be envisaged at the EU level.

**Working document on the relation between the surveillance practices in the EU and the us and the EU data protection provisions**

EUROPEAN PARLIAMENT 2009 - 2014

*Committee on Civil Liberties, Justice and Home Affairs*

12.12.2013

# WORKING DOCUMENT

on the relation between the surveillance practices in the EU and the US and the EU data protection provisions

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

Jan Philipp Albrecht (Co-author)

## 1. Mass surveillance practices in the EU and the US

Several Member States and third countries have programmes of mass surveillance of electronic communications by their communications intelligence agencies, as has been established in the context of the revelations unveiled by former NSA contractor Edward Snowden and further elaborated and supported by a large number of journalistic investigations and reports since then.[1] Some of the revelations have been confirmed by the intelligence agencies, but for most part, the respective agencies have declined to comment or have stated that the documents have been misinterpreted. The United States, the UK, Sweden, France and Germany have the means to tap into the internet backbone cables and collect all of the traffic for a certain period of time ("full take", NSA and GCHQ) or part of it (FRA, DGSE, BND), and at least the Netherlands are reportedly working on such a programme. Access to the backbones is either done by lawful interception facilities and standardised interfaces[2] or by tapping into the fibre-optic cables directly and bending or splicing them[3].

According to media reports, at least the US and the UK also have means of gaining access to confidential computer and telecommunications systems by obtaining unauthorised access, including possible access to the communications provider of the EU institutions. It is also alleged that the NSA also has a programme of actively inserting backdoors in widely-used cryptographic tools in order to be able to read most of the intercepted traffic and data.[4]

Access to data stored and processed on computer facilities, including remote computing facilities (cloud computing), is carried out by various intelligence programmes, the most prominent one being the NSA PRISM programme and the underlying legal provisions in the FISA Act and the USA PATRIOT Act. Furthermore, at least US and UK embassies, consulates and military establishments in third countries, including in other Member States, host electromagnetic interception facilities directed at GSM interception, including on heads of state and government.[5]

Raw personal data collected through these programmes is shared in bulk between the intelligence communities of the US, the UK, Canada, Australia and New Zealand under the

---

[1] See the two studies commissioned by DG INPOL, Policy Department C, in the context of the LIBE special inquiry: "The US surveillance programmes and their impact on EU citizens' fundamental rights", PE 474.405, September 2013, and "National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law", PE 493.032, October 2013.

[2] C.f. the secret room 641A at the AT&T switching facility in San Francisco, see Whistle-Blower's Evidence, Uncut, Wired, 22.5.2006, http://www.wired.com/science/discoveries/news/2006/05/70944; the GCHQ Tempora programme, see GCHQ taps fibre-optic cables for secret access to world's communications, The Guardian, 21.6.2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; the German Telecommunications Surveillance Regulation of 2005. The European Telecommunications Standards Institute (ETSI) has a "Lawful Interception Seminar" responsible for defining such standards.

[3] The US Navy has a specialised submarine for doing this on submarine cables, the USS Jimmy Carter.

[4] NSA Cryptanalysis and Exploitation Services: Project Bullrun – classification guide to the NSA's decryption program, published at http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide.

[5] James Ball: NSA monitored calls of 35 world leaders after US official handed over contacts, The Guardian, 25.10.2013, http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

"Five Eyes" agreement.[1] Other intelligence sharing agreements exist to varying degrees between these countries and other Member States.

While in most cases, such mass surveillance is, in a strict reading of the respective laws, only permissible on the communications of foreigners, there are practices to circumvent this limitation including by setting a very low threshold for establishing the probability of the communications subject being foreign (e.g. by an expansive interpretation of the "relevant" threshold in the US FISA act), by declaring the internet as "foreign" by nature (as was recently revealed about the German BND[2]), or by swapping the data collected on each other's citizens.[3] This highlights the intrinsically transnational nature of surveillance activities and the limits to solely national scrutiny bodies.

All these revelations have raised serious concerns on the legality of such measures under EU primary and secondary data protection law, law on cyber-security and cybercrime, obligations under the Council of Europe, and broader provisions in Union law that also address the borders of EU and Member States' competence. The following sections will point out the challenges that mass surveillance practices by the US and several EU Member States pose to EU law and EU data protection in particular.

## 2. EU and European data protection law

Primary law: Member States' legal systems need to comply with the fundamental rights and fundamental legal principles enshrined in Article 6 of the Treaty on the European Union and the Charter of Fundamental Rights of the European Union. Data protection is a binding fundamental right under Article 8 of the Charter of Fundamental Rights, which reflects Article 8 of the European Convention on Human Rights and has a specific legal basis in Article 16 TFEU: "Everyone has the right to the protection of personal data concerning them". Fundamental rights enjoy special protection and higher safeguards than other rights under law.

There is a significant body of jurisprudence from the ECtHr providing the standards for determining the legality and legitimacy of secret surveillance activities by executives and intelligence communities. In particular, ECtHR case law on the right to privacy and data protection in respect to surveillance by secret services has stressed the danger of these measures of undermining or even destroying democracy on the ground of defending it, and affirmed that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate[4]. The ECtHR case law provides that the offences and activities in relation to which national security surveillance may be ordered in a clear and precise manner, the law should clearly indicate which categories of people may be subjected to surveillance and that there must be strict limits on

---

[1] The existence of the Five Eyes agreement, also known as UKUSA Agreement, was already confirmed by the European Parliament special report on the on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), A5-0264/2001, 11.7. 2001. See also: NSA Press release, 24.6.2010: Declassified UKUSA Signals Intelligence Agreement Documents Available, http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml.

[2] Fakt, ARD German TV, 12.11.2013, http://www.mdr.de/fakt/video160094.html, manuscript at http://www.mdr.de/fakt/bnd114-download.pdf.

[3] James Ball: US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, The Guardian, 20.11.2013, http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

[4] Klass and others v Federal Republic of Germany, European Court of Human Rights, 6 September 1978 (Series A, NO 28).

the duration of any surveillance and effective remedies in cases of alleged unlawful interferences with ECHR rights.

Member States have claimed that there is no EU competence as regards intelligence surveillance practices since maintaining law and order and safeguarding national security fall within the remit of their exclusive field of intervention. However, as there are national security exemptions in EU data protection law (see in detail below), it needs to be clarified also from the side of the Parliament what "national security" means and to which extent measures taken with a reference to national security are outside the scope of EU primary and secondary law on data protection.

Data protection law: Directive 1995/46/EC[1] lays down the general rules for data protection in the private and public sector. Framework Decision 2008/977/JHA[2] provides the data protection rules for the law enforcement sector when exchanging data across the internal borders in the Union. Current EU data protection law is based on the principles of purpose limitation, data minimisation, and rights of the data subject, including the right to be informed about and to object to the processing, to get access to one's personal data, and to not be subject to automated decisions that significantly affect the data subject.

Data protection limits for mass surveillance by Member States: According to Article 13 of Directive 1995/46/EC, Member States may adopt legislative measures to restrict these rights only "when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others."

"National security" here relates to the EU Member States, not to a third country. It also is, in practical terms, hard to distinguish from "public security", which does not fall outside of EU competence. There is significant case-law that limits the notion of "national security", and any measure taken by government agencies in this regard must also be proportionate according to general principles of the rule of law. In instances where private enterprises provide personal data to national intelligence agencies for the purposes of national security, this disclosure and the further processing by the national intelligence services could be considered under the "national exemption" of Article 4 TEU. However, such a request made by the national intelligence services must respect Article 2 TEU and be in full compliance with the ECHR and the rule of law.

Data protection limits for mass surveillance by third countries: Third countries' national security does not provide a basis for exemptions under the existing data protection law. Therefore, European personal data is in principle protected against such exemptions when transferred to third countries, such as the Safe Harbour decision of 2000 on transfers of

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

personal data to the United States[1] specifying that any limitations to data subject rights are allowed only "to the extent necessary" to meet national security, public interest, or law enforcement requirements. In case a third country does not provide an adequate level of protection of personal data, there are two ways in Union law to prevent or interrupt the transfer of data from the Union to such countries: a) The Commission can unilaterally lift an existing adequacy rating; b) the national data protection authorities can stop the transfer of personal data. This is also spelt out in the Safe Harbour Agreement in Article 3(1), based on Article 25(3) of Directive 1995/46.[2] The Commission has recently announced 13 recommendations to improve the Safe Harbour Agreement with, among others, the aim of ensuring that the national security exemption in the Safe Harbour decision is used only to an extent that it is strictly necessary and proportionate.[3]

In general, the EU system on transfers of personal data to third countries is based on the principle of the continuity of protection, so as to avoid that the protection granted in the EU is lost, eroded or denied just because the data are transferred to a third country. The rules and mechanism established aim at ensuring this requirement. This was already established in Directive 95/46/EC, and the current proposals for a Regulation and a Directive will make this principle clearer. The Directive will also improve the situation with regard to law enforcement activities as it will achieve a greater convergence of the data protection legal framework applicable to this sector. Transfers to third countries always require respect of the purpose limitation, and personal data shall be only processed in the third country for the specific, specified and legitimate purpose and not further processed in an incompatible manner. This is a prerequisite that applies to any transfer, whether it is based on an adequacy decision of the Commission or on contractual arrangements put in place by the EU controller and the importer. Further processing of data transferred to a third country for intelligence purposes is an incompatible purpose and would necessarily be an exception to the obligations imposed. It therefore should be in line with the system of exceptions of Article 13 of Directive 1995/46/EC.[4] Regarding mass surveillance and activities of intelligence conducted on the basis of processing of bulk categories of personal data, countries where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection will not be safe destinations for transfers.

The data protection reform package: The above-mentioned two laws are currently being revised, with a General Data Protection Regulation replacing the 1995 Directive, and a Data Protection Directive replacing the 2008 Framework Decision. This Committee has on 21 October 2013 voted almost unanimously for the negotiation mandates for the rapporteurs, Jan Philipp Albrecht and Dimitrios Droutsas, with the aim of achieving a first reading agreement with Council before the end of this legislative term.

---

[1] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441.

[2] C.f. Franz C. Mayer: Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen? Teil 1: NSA, www.verfassungsblog.de/de/mit-europarecht-gegen-die-amerikanischen-und-britischen-abhoeraktionen-teil-1-nsa.

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

[4] The EDPS in his presentation to the LIBE Committee hearing of 7 October 2013 took this view.

The LIBE reports build on the rights established in the existing EU laws, specify them to a certain extent, and aim at a better and more coherent enforcement across the Union. The explicit reference to the "national security" exemption in Article 2 on the scope of the regulation has been deleted by LIBE, based on the argument that the scope of the national security exemption is contested. The LIBE report also has introduced a new Article 43a into the data protection regulation to ensure that access requests by public authorities or courts in third countries to personal data stored and processed in the EU can only be granted if they also have a legal basis in EU law and are authorised by the competent European data protection authority.

The e-Privacy Directive, confidentiality of communications, and data retention: Electronic communications privacy is also specifically regulated in Directive 2002/58.[1] Under Article 5, Member States shall "ensure the confidentiality of communications through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1),"Such a restriction of the confidentiality of communications can only be adopted by Member States according to Article 15 (1), when it "constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". Again, such a national security exemption cannot be used as a carte blanche, but has to meet certain tests. Article 15, however, as a general opening clause, has led several Member States to adopt laws for data retention that go further than the Data Retention Directive of 2006[2]. The data retention directive is currently subject to a proceeding of the Court of Justice after constitutional complaints in Ireland and Austria.[3] The e-Privacy Directive also establishes positive obligations on Member States to prevent mass surveillance of communications data by private operators. In its ruling in the case Scarlet v Sabam, the CJEU ruled that a system of general surveillance by an internet service provider of its customers to track their activities on the internet was not in line with the e-Privacy Directive and the EU Charter of Fundamental Rights.[4]

Data protection by Union institutions: Regulation 2001/45[5] concerns the processing of personal data by Union institutions and bodies. For agencies such as Europol or Eurojust, the data protection regime is set out in their specific legal acts. Moreover due to the specific and sensitive nature of the information processed by these agencies they have a higher responsibility, because of the serious adverse effects on individuals' fundamental rights raised from disclosure to third countries. Where the EU or its agencies transfer personal data to third countries, they should take the necessary measures to ensure that data transferred is not further processed for incompatible purposes such as intelligence. Should they become

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), last amended 2009.

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[3] The statement of the attorney-general is expected for 12 December 2013.

[4] Judgement of the Court (Third Chamber) in Case C-70/10, 24 November 2011.

[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

aware that data is or may be used for intelligence purposes or mass surveillance, they should adopt the necessary measures to prevent it, inform the EDPS and if needed suspend the transfer.

Concerns have been raised that the sharing of information with Europol by national law enforcement authorities and potentially by intelligence services, and other international partners, renders indistinguishable the boundaries of what is police cooperation covered by Title V, Chapter 5 TFEU) and what is intelligence at EU level. This leaves little room for properly reviewing the legality and adequacy of the kind of information exchanged and their exact sources against data protection principles, because it is not clear which law is applicable and consequently which principles apply. The allegations of surveillance programmes operating by some EU Member States indicate a progressive merging of police, military and intelligence actors and practices which create legal insecurity and uncertainty in the actions and credibility of EU agencies themselves and reveal an accountability gap which needs to be effectively addressed at European level.

EU-US data protection framework agreement: In May 2010, the European Commission adopted the mandate for negotiations between the EU and the US on a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement"), authorised by the Council on 2rd December 2010.[1] From the beginning the negotiations have been challenging and over a year ago reached a stalemate. The main importance of a framework agreement would be the resolution of the issue of judicial redress for EU citizens when their personal data is transferred to the US. At the moment EU citizens do not enjoy full and reciprocal judicial redress rights as access to US courts are guaranteed only to US persons (citizens and permanent residents). On top of this actual and urgent issue, completing the negotiations would restore trust in transatlantic data transfers. It would be crucial that the Commission objective of a meaningful and comprehensive agreement that ensures legal redress for EU citizens be reached before summer 2014.

Council of Europe Convention 108: The EU is currently acceding the European Convention on Human Rights of the Council of Europe, and all Member States are already party to it. Article 8 ECHR states "Everyone has the right to respect for his private and family life, his home and his correspondence." This is more clearly spelled out in Convention 108 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data from 28 January 1981, which provides in Article 5 that personal data shall be "obtained and processed fairly and lawfully" and stored "for legitimate purposes and not used in a way incompatible with those purposes". Article 9 of Convention 108 allows derogations only if they constitute "a necessary measure in a democratic society" or for "protecting the data subject or the rights and freedoms of others". There is a significant body of case law spelling out what falls under these limits.[2]

## 3. Data Security and Cyberattacks Provisions

Data security provisions: All of the Union's data protection laws have provisions that mandate the data controller to ensure the security of the personal data processed. This

[1] http://europa.eu/rapid/press-release_IP-10-1661_en.htm

[2] Two prominent examples are S and Marper v United Kingdom (2009), which curtailed the retention period in the UK National DNA Database, especially for non-suspects, and Gillan and Quinton v United Kingdom (2010), which ruled that powers granted to the police under the Terrorism Act of 2000 were neither sufficiently circumscribed nor subject to adequate legal safeguards and therefore not 'in accordance with the law'.

includes securing the data against cyber-attacks from the outside and notifications to the supervisory authorities and the data subject in case of data breaches. By logical conclusion, Member States' authorities should be banned from pursuing such attacks and rather obtain lawful access in individual cases based on lawful interception. It is as yet unclear if the reported attacks on Belgacom and other telecommunications providers such as SWIFT have included a breach of personal data, however, given that Belgacom have subsequently admitted that there is a possibility that customers personal data have been accessed[1], precautionary measures should be put in place to notify the customers, which includes the EU institutions, about the reported cyberattacks.

Cyberattacks directive and Budapest Convention: The new Directive on attacks against information systems[2] has entered into force this summer and has replaced the existing Framework Decision. Both are based on the Council of Europe Convention on Cybercrime from 2001, also known as the Budapest Convention.[3] The Budapest Convention mandates its parties to establish as criminal offences, if done without right, the access to a computer system, the interception of non-public data transmissions, as well as interference with computer data and computer systems. While the Budapest Convention has provisions that allow the parties to establish legal provisions for the interception of content data by competent authorities (e.g. in the case of law enforcement measures), these apply only to the territory of the respective country. The (mass) surveillance of communications and the attacks on information systems in the territory of another party to the Convention are not covered and are therefore illegal under the national transpositions of the Budapest Convention and the EU Framework Decision and the new Directive. This is even more relevant, as the United States is a party to the Budapest Convention.

The LIBE Committee has recently expressed its concern about the work carried out within the Council of Europe's Cybercrime Convention Committee with a view to developing an additional protocol on trans-border access to stored computer data, and expressed that it is "alarmed by the fact that should such an additional protocol be endorsed, its implementation could result in unfettered remote access by law enforcement authorities on servers and computer systems 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."[4]

## 4. Conclusions and recommendations

1. Member States' legal systems need to comply with the fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on the European Union and the Charter of Fundamental Rights of the European Union.

2. Data protection is a binding fundamental right under Article 8 of the Charter of Fundamental Rights, which reflects Article 8 of the European Convention on Human Rights and has a specific legal basis in Article 16 TFEU.

[1].http://www.lesoir.be/343247/article/economie/2013-10-18/belgacom-pirate-donnees-privees-ses-clients-sont-concernees

[2] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[3] Council of Europe, Convention 185 on Cybercrime, Budapest, 23.11.2001

[4] Opinion under Rule 50 of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Industry, Research and Energy on unleashing the potential of cloud computing in Europe (2013/2063(INI)), 19.9.2013, PE504.203v02-00.

3. Member States are bound by several EU data protection and cyber-security laws. It should be further investigated if any of the mass surveillance activities are in breach of EU primary or secondary law in this regard. It should also be investigated if Member States' activities are in breach of obligations in the context of Council of Europe conventions and the European Convention on Human Rights.

4. As there are national security exemptions in EU data protection law, it should be clarified also from the side of the Parliament what "national security" means and to which extent measures taken with a reference to national security are outside the scope of EU primary and secondary law on data protection.

5. Third countries' national security does not provide a basis for exemptions under the existing data protection laws. European personal data is in principle protected against such exemptions when transferred to third countries, such as the Safe Harbour decision of 2000 on transfers of personal data to the United States. The revision of the Safe Harbour Agreement should clearly limit the scope of possible exemptions and should exclude mass surveillance activities.

6. The EU data protection reform should be concluded with priority. After the adoption of the LIBE reports and negotiation mandates on 21 October 2013, Council should now adopt its negotiation position as soon as possible, so an agreement can still be reached before the end of this legislative term. It will be of utmost importance to maintain the new Article 43a on protection against data access by third countries.

7. The negotiations between the EU and the US on a framework agreement on data protection in the field of police and judicial cooperation should be concluded swiftly, while solidly resolving the current lack of judicial redress for EU citizens in the US.

8. The proposed Council of Europe's Cybercrime Convention additional protocol on trans-border access to stored computer data could result in unfettered remote access by law enforcement authorities on servers and computer systems located in other jurisdictions, which is unacceptable. Any such protocol should instead refer to MLA agreements and other instruments of judicial cooperation to guarantee data protection and due process.

9. The future Europol regulation should include an article stating that data obtained in violation of fundamental rights in accordance with article 6 TEU and the Charter of Fundamental Rights of the European Union shall not be processed.

10. The allegations of surveillance programmes operated by some EU Member States indicate a progressive merging of police, military and intelligence actors and practices, which create legal insecurity and uncertainty in the actions and credibility of EU agencies themselves and reveal an accountability gap which needs to be effectively addressed at European level.

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

EUROPEAN PARLIAMENT 2009 - 2014

*Committee on Civil Liberties, Justice and Home Affairs*

12.12.2013

# WORKING DOCUMENT

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

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

Axel Voss (Co-author)

## Impact of US Surveillance programmes on transatlantic agreements

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

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

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

## Safe Harbour

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

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

In case of a breach of the Decision 2000/520/EC it implies a twofold system for suspension or termination of the mechanism. According to Article 3 the data protection authorities of the Member States may exercise their existing powers to suspend data flows to an organisation in cases where there is a substantial likelihood that principles are being violated and processing of personal data or the continuing transfer would create an imminent risk of grave harm to data subjects. The Member States must inform the European Commission in such cases. The European Commission is required to evaluate the implementation of the decision on the basis of available information and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC. Consequently the

Commission may state that the implementation or the functioning of Safe Harbour does not work and it may propose measures for instance to suspend or to revoke the decision.

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

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

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

**TFTP Agreement**

The TFTP Agreement between the European Union and the US on the processing and transfer of financial messaging data from the EU to the US for the purpose of the Terrorist

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

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

Finance Tracking Program (hereinafter 'the TFTP Agreement') was concluded on 13th July 2010 and entered into force on 1st August 2010.

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

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

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

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

The US Department of the Treasury also gave assurances in relation to access to SWIFT formatted messages in accordance with other legal tools in place.

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

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

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

Inquiry Committee that there were no indications for a breach of the TFTP Agreement by the NSA.

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

**EU-US PNR Agreement**

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

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

Given the serious concerns raised in the EU about US surveillance programmes, the European Commission issued the joint review of the implementation of the Agreement between the EU and US on the processing and transfer of PNR to the DHS to verify how these agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection experts from the EU and the US, looking at how the Agreement has been implemented.

According to this final report[2] "DHS has declared that it shares PNR with the U.S. Intelligence Community if there is a confirmed case with a clear nexus to terrorism and

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

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

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

**US Surveillance programmes and their impact on future transatlantic agreements**

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

**Recommendations;**

The EU and the US approach to data protection and privacy fundamentally differ from each other. Whereas data protection is a fundamental right in the EU, it is perceived as an element of consumer protection and organised in a sectorial way in the US. Whilst within the EU there is a constant effort to balance data protection and privacy on the one hand and security and law enforcement on the other, the US seems to give only priority to security and law enforcement.

The surveillance activities by the NSA have primarily an impact on the EU citizens' privacy but also on the relations between the US and EU. US surveillance activities, with respect to EU data, might have legal implications on the existing transatlantic agreements and on future transatlantic cooperation. A lack of trust and tensions between the transatlantic partners are consequences resulting from the breach of legal agreements between the US and EU. (Temporary) suspension and renegotiations of existing economic transatlantic agreements might be a possible legal implication resulting from US surveillance activities. As mentioned already, this refers to the above proposal of ending Safe Harbour in order to balance the transatlantic relationship. In relation to this, the European Commission is strongly urged to conclude the on-going negotiations on a data protection agreement for law

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

enforcement purposes (umbrella agreement). This agreement is of utmost importance as and it would act as the basis to facilitate data transfer in the context of police and judicial cooperation and in criminal matters; moreover it would give EU citizens the right to judicial redress in the US whenever their personal data are being processed in the US for law-enforcement or judicial cooperation purposes. This agreement should enforce data protection and privacy rights of EU citizens' whilst restoring trust in transatlantic cooperation in the field of justice and home affairs.

**Working document on democratic oversight of member state intelligence services and of EU intelligence bodies**

EUROPEAN PARLIAMENT 2009 - 2014

*Committee on Civil Liberties, Justice and Home Affairs*

20.12.2013

# WORKING DOCUMENT

on Democratic oversight of Member State intelligence services and of EU intelligence bodies

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

Sophie In't Veld (Co-author)

Cornelia Ernst (Co-author)

**The importance and challenges of efficient oversight of intelligence services**

- The existence of intelligence services in democratic countries requires strong oversight and accountability mechanisms. Intelligence services are given special, intrusive powers and capabilities in order to protect the state, its citizens and democratic order. However, given the extent of these powers, there exists the potential that they could be used to undermine the security of individuals and subvert the democratic process. Therefore, checks and balances are crucial in ensuring that the intelligence services fulfil their responsibilities in accordance with the constitution and the rule of law.

- In other fields, checks and balances are put in place by rules, controls and democratic/public scrutiny mechanisms aiming at minimising the potential for illegal conduct and abuse of power. However, the high level of secrecy that is intrinsic to the intelligence services - in order to avoid endangering on-going operations, revealing modus operandi or putting at risk the lives of agents - impedes full transparency, public scrutiny and normal democratic or judicial examination.

- The resulting lack of accountability in combination with the special powers that intelligence services enjoy bears a high risk of abuse of power, illegality and a culture of impunity, especially taking into consideration the temptation to use the granted special powers for other purposes than the protection of national security (for instance for economic/industrial or diplomatic espionage or for political reasons). Given these dangers, countries are facing the challenge of creating specific oversight mechanisms to hold intelligence services to account for their policies and actions in terms of legality, propriety, effectiveness and efficiency, while ensuring confidentiality.

- The exact form of oversight varies widely among countries. However, it usually consists of: i) *ex ante* oversight as to the legal framework including mandate and powers of the intelligence services, some form of fundamental rights assessment and prior authorization of certain intelligence operations that infringe on individual rights, and ii) *ex post* oversight by parliamentary or expert bodies, independent of the incumbent government, monitoring the behaviour of the intelligence services and ensuring the respect of the rule of law on behalf of the electorate.

- Most of these national oversight mechanisms and bodies were set up or revamped in the 1990s. However, implementation across Europe has been uneven, with some oversight bodies relatively weak in terms of mandate and powers.[1] This situation has been aggravated by parallel developments: rapid technological developments, changing nature of security threats, and international mobility of data, leading to declined relevance and effectiveness of national oversight mechanisms.

**Rapid technological developments**

- Modern information and communication technologies enable intelligence services to collect information on a mass scale. The revolutionary development in data storage and analysis capacities (data mining, profiling, etc.) further encourages the collection of increasingly vast quantities of personal data in order to extract relevant information or patterns out of them (connecting the dots).

[1] See also "Parliamentary oversight of security and intelligences agencies in the EU", study for the European Parliament, 2011.

- These technological developments have enabled a certain shift in the paradigm of intelligence services, away from suspicion based, targeted monitoring towards more generalised massive, and systematic surveillance.

**Changing nature of security threats**

- The nature of security threats has changed drastically with the technological developments, making them more international, heterogeneous and asymmetric. This has increasingly led to (international) intelligence cooperation, also involving the exchange of personal data, and often blurring the line between intelligence and law enforcement cooperation.

**Availability and mobility of data**

- Increase in internet bandwidth and the development of mobile computing devices have led to an exponential growth in the amount of personal data available in digital form (email traffic, web searches, internet phone calls, geo-location, financial transactions, medical files, etc). Increasingly, our identity can be distilled from this "digital footprint" of available online personal and meta-data.

- These personal digital data, transiting through cables or satellites and stored/processed within cloud computing services around the world, can rather easily be intercepted/collected by intelligence services.

- As the world becomes more and more wired and interconnected, these data are increasingly stored and transmitted freely across borders and through transit countries, leading to an unclear situation regarding jurisdiction and diminishing the relevance of national legislation and of national oversight.

**Challenges to national oversight of intelligence bodies**

- The above mentioned trends lead to the following paradox: While legislation and oversight concerning intelligence services is regulated on a national basis, security threats, intelligence information and personal data increasingly transcend national borders. This can result in the flow of information from highly protective environments to less protective jurisdictions, circumventing national legislation. For example, the extraction of certain information by a foreign intelligence service and its return under the head of intelligence sharing to the national intelligence service can be used by the latter to "launder" this information and to circumvent national legislation that safeguards privacy protections it would otherwise enjoy.

- Domestic oversight bodies may have jurisdiction over the sending agency or the receiving one but not both of them, leading to gaps in which information exchanges can take place without adequate review. This problem is further aggravated by the so-called "third party rule" or the principle of "originator control", which has been designed to enable the originator to maintain control on the further dissemination of its sensitive information, but is sometimes also interpreted as applying to the recipient services' oversight. Some intelligence services are reluctant to request the permission of originating services to transmit intelligence to oversight bodies, while reviewers, conscious of the services' reputational concerns, rarely demand that the services make such requests.

- Given the power of the third party rule to shield swathes of information, the expansion and acceleration of international intelligence cooperation presents thus a formidable challenge to accountability processes. This problem will likely be further increased by technological developments that will increase the amount of communications subject to potential interception by foreign intelligence agencies to the point that, if left unregulated, national laws would become moot.

- While both the threats to national security and the responses to these threats have become increasingly globalised, accountability mechanisms have remained territorially bounded. The growing cooperation between national intelligence agencies has not been adequately matched by international collaboration between national oversight bodies. Ultimately, the combination of the weakness of these bodies on the one hand, and the levels of secrecy, sensitivity and multi-territoriality inherent in international cooperation activities on the other, has led to an increasing accountability deficit and made in certain cases intelligence sharing an area of relative impunity To a certain extent, the lack of transparency surrounding international agreements concerning intelligence agency cooperation has aggravated the problems described above.

- National oversight bodies were designed for a different era, and in response to a very different set of abuses and are hamstrung by inadequate legal powers to access all information and fully hold intelligence services to account. These bodies seem thus to be ill equipped to hold intelligence services and their political masters to account in present days of international cooperation, technological developments and mobility of data.[1]

**Solutions**

- One avenue is to increase transparency and thus public scrutiny. While full transparency is not possible in this field, intelligence services tend to have an excessive or even obsessive attitude towards secrecy. Confidentiality should be regarded more as an exception, demanding convincing justification motivated with reference to specific and significant harm that might arise from public disclosure of information, instead of being simply based on the broad and ambiguous concept of "national security". Criteria could be developed on enhanced transparency, building on the general principle of access to information and the so-called “Tshwane Principles”.[2] These criteria would need to be binding on the governments in order to have any effect.

- A second avenue is to strengthen national oversight systems. This should be done in terms of *ex-ante* authorization by an independent investigating magistrate who is well-trained in the judicial assessment of human rights. Furthermore, the *ex-post* oversight of their activities by parliamentary or independent expert bodies should be strengthened by providing them with full access to information (including classified information and information from other services), the power to conduct on-site visits, a robust set of powers of interrogation, sufficient technical expertise, adequate resources and strict independence from the government. In general, these bodies should also be obliged to report to their respective parliaments. This should be complemented by setting binding minimum European standards or guidelines on the oversight of national intelligence services, building on existing best practices and recommendations by international bodies (UN, Council of Europe, etc).

[1] I. Leigh, Accountability and intelligence cooperation.
[2] The Global Principles on National Security and the Right to Information, June 2013.

- A third suggestion is to allow for oversight bodies to keep pace with the activities being overseen. Since intelligence services have to cooperate with each other in order to tackle threats and networks across borders, oversight bodies need to cooperate on an international level as well in order to hold intelligence services accountable. Recognising the need for increased cooperation between national review bodies of intelligence agencies[1], a platform has been established allowing oversight bodies to share common problems and best practices.[2] This call for increased collaboration was further substantiated with the signing of the Declaration of Brussels which recognises the need for more intensive exchange of information between the parliamentary oversight bodies of the EU Member States, Switzerland and Norway.[3] So far, this happened uncoordinated, whereas there is room for more conscious international collaborative oversight. This could take place through joint committees, sharing of information or the creation of supranational bodies. This could be achieved through a body similar to the Article 29 Working Party in the field of data protection.

- A High-Level Group could be set up to propose, in a transparent manner and in collaboration with parliaments, further steps to be taken for increased oversight collaboration in the EU, including the oversight of the EU Intelligence Analysis Centre (IntCen).

- Weak formalised national systems of intelligence accountability could be counterbalanced by more informal accountability through revelations provided by investigative journalists in tandem with activists and whistle-blowers. This requires however not only a better legal protection for them, but also a break on uncontrolled surveillance that can create a chilling effect on these same persons. Also here the "Tshwane principles" as well as the work performed by the Council of Europe could act as an inspiration for further development. It should be noted however, that a proper mechanism for oversight should not be depending on journalists and whistleblowers, and be equipped with powers that enable it to achieve its goals on its own.

- An area of concern in relation to the scope of oversight mechanisms is the evident overlap between the operation of intelligence agencies and the scope of traditional policing. Given that there is a strong framework of accountability and stricter rule of law in the latter, it is imperative that oversight mechanisms ensure that fundamental rights are also protected within the scope of intelligence activities.

**Questions for debate**

- Given the extent of international cooperation by intelligence agencies in the EU it is crucial that the scope of this activity is subject to adequate control allowing oversight bodies to scrutinise international intelligence cooperation. There is a threat that with international cooperation, intelligence agencies in EU Member States may be able to receive communications that they could not otherwise lawfully gather themselves. As stated, the third party rule can serve as a barrier to proper oversight mechanisms if the established oversight committee is deemed as a third party. How can it be ensured that information received from a foreign or international agency is subject to adequate oversight? Would it be possible that oversight bodies were not considered as third parties?

---

[1] http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A.HRC.10.3.pdf

[2] See for example ENNIR - The European Network of National Intelligence Reviewers (www.ennir.be).

[3] http://www.parlement-eu2010.be/pdf/30sep-1okt-declarationE.pdf

- How can national security measures, with a disposition towards the use of obscurity/ambiguity, be embedded in a democratic framework of parliamentary and judicial oversight?

- What should the role and powers of the European Parliament be to exercise parliamentary oversight? Should the European Parliament create a specialized (sub-)committee that is able to receive and scrutinize classified information? How could the EP's "power of the purse" (budget right) be used most effectively to support the possible increased role of scrutiny for the EP?

- If more cooperation and exchange of information takes place among national intelligence services, is it still effective to have exclusively national rules and oversight mechanisms for intelligence services within the EU? How to best organize within Europe collaborative oversight of intelligence services?

- Can national oversight mechanisms, given the technological developments and the mobility of data, ensure that the civil rights of all EU citizens are respected by the different national intelligence services? If not, is there a need for minimum European standards or rules that intelligence services should adhere to regarding information exchange, data protection, transparency and oversight?

**Working Document on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens (AFET Committee)**

EUROPEAN PARLIAMENT 2009 - 2014

*Committee on Foreign Affairs*

20.11.2013

# FINAL WORKING DOCUMENT

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

Committee on Foreign Affairs

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

***Preliminary findings:***

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

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

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

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

   According to Article 4(2) of the EU Treaty, national security remains the sole responsibility of each Member State, however this must be interpreted along with the existing EU competences or legislation including internal security, data protection and the fight against terrorism and other crimes. Given the rising importance of international cooperation among intelligence services, the EU institutions need to develop an appropriate framework to strengthen their ability to defend themselves against spying activities from third countries including the US.

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

As top representatives of US Administration and Members of US Congress admitted, the scale and scope of some of NSA surveillance conducted violates the US Constitution and rights of American citizens, and goes far beyond measures required for counter-terrorism purposes. US authorities also admitted that congressional and judicial oversight of these intelligence operations failed. President Obama instructed two bodies to review the ongoing surveillance programs so as to find a new balance between security and privacy, and strengthen transparency and protections against abuse. Also, a debate in Congress about the scale and scope of surveillance and about appropriate judicial and congressional oversight is ongoing.

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

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

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

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

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

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

6. The Snowden materials also revealed allegations on US spying activities against EU

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

institutions and EU Delegations on US soil. Such activities are inacceptable among allies. These revelations must however create an incentive for the EU institutions to improve their ability to defy spying activities directed against them, including by strengthening the IT security of EU institutions.

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

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

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

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

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

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

***Preliminary recommendations:***

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

2. In light of global challenges facing the EU and the US, the transatlantic partnership needs to be further strengthened, and it is vital that transatlantic cooperation in counter-terrorism continues. However, clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership. Therefore, an EU-US agreement protecting the privacy of citizens and allowing for equal rights in terms of information and judicial redress rights for European and American citizens is needed. The ongoing negotiations on an EU-US umbrella agreement on data transfer for law enforcement purposes are an important opportunity in this regard.

   The EU's task is to actively engage US counterparts so that in the ongoing American political debate on reforming surveillance and reviewing intelligence oversight, the

privacy rights of EU citizens are addressed, equal information rights and privacy protections in US courts are guaranteed and the current discrimination is not perpetuated.

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

Clear political signals are needed from our American partners that the US distinguishes between allies and adversaries.

3. As some EU Member States pursue bilateral communication with US authorities on spying allegations and make anti-spying arrangements, it is important that these Member States make sure to take the interests of the EU as a whole fully into account.

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

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

6. The EU institutions should 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.

7. As it is vital that the cooperation among intelligence services within the transatlantic partnership continues, it is of crucial importance to strengthen the judicial control and the democratic oversight of European intelligence services, both on national and also, in particular when it involves EU instruments or agencies, on EU level.

# 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)[128], 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 |
|---|---|---|
| 5th September 2013 15.00 – 18.30 (BXL) | - Exchange of views with the journalists unveiling the case and having made public the facts | • Jacques FOLLOROU, Le Monde<br>• Jacob APPELBAUM, investigative journalist, software developer and computer security |

[128] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+20130704+ITEMS+DOC+XML+V0//EN&language=EN, sdocta3

| | | |
|---|---|---|
| | | researcher with the Tor Project<br>• Alan RUSBRIDGER, Editor-in-Chief of Guardian News and Media (via videoconference) |
| | - Follow-up of the Temporary Committee on the ECHELON Interception System | • Carlos COELHO (MEP), former Chair of the Temporary Committee on the ECHELON Interception System<br>• Gerhard SCHMID (former MEP and Rapporteur of the ECHELON report 2001)<br>• Duncan CAMPBELL, investigative journalist and author of the STOA report 'Interception Capabilities 2000' |
| 12th September 2013<br>10.00 – 12.00 (STR) | - Feedback of the meeting of the EU-US Transatlantic group of experts on data protection of 19/20 September 2013 - working method and cooperation with the LIBE Committee Inquiry (In camera) | • 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)<br>• Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection)<br>• Reinhard PRIEBE, Director DG HOME, European Commission (co-chair of the EU-US ad hoc working group on data protection) |
| | - Exchange of views with Article 29 Data Protection Working Party | • Jacob KOHNSTAMM, Chairman |
| 24th September 2013 9.00 – 11.30 and 15.00 - 18h30 (BXL) | - Allegations of NSA tapping into the SWIFT data used in the TFTP programme | • Cecilia MALMSTRÖM, Member of the European Commission<br>• Rob WAINWRIGHT, Director of Europol |

| | | |
|---|---|---|
| **With AFET** | | • Blanche PETRE, General Counsel of SWIFT |
| | - Feedback of the meeting of the EU-US Transatlantic group of experts on data protection of 19/20 September 2013 | • 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)<br>• Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection)<br>• Reinhard PRIEBE, Director DG HOME, European Commission (co-chair of the EU-US ad hoc working group on data protection) |
| | - Exchange of views with US Civil Society (part I) | • Jens-Henrik JEPPESEN, Director, European Affairs, Center for Democracy & Technology (CDT)<br>• Greg NOJEIM, Senior Counsel and Director of Project on Freedom, Security & Technology, Center for Democracy & Technology (CDT) (via videoconference) |
| | - Effectiveness of surveillance in fighting crime and terrorism in Europe | • Dr Reinhard KREISSL, Coordinator, Increasing Resilience in Surveillance Societies (IRISS) (via videoconference) |
| | - Presentation of the study on the US surveillance programmes and their impact on EU citizens' privacy | • 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 |
| 30th September 2013 15.00 - 18.30 (Bxl)<br><br>**With AFET** | - Exchange of views with US Civil Society (Part II)<br><br>- Whistleblowers' activities in the field of surveillance and their legal protection | • Marc ROTENBERG, Electronic Privacy Information Centre (EPIC)<br><br>• Catherine CRUMP, American Civil Liberties Union (ACLU)<br><br>Statements by whistleblowers:<br><br>• Thomas DRAKE, ex-NSA Senior Executive<br><br>• J. Kirk WIEBE, ex-NSA Senior analyst<br><br>• Annie MACHON, ex-MI5 Intelligence officer<br><br>Statements by NGOs on legal protection of whistleblowers:<br><br>• Jesselyn RADACK, lawyer and representative of 6 whistleblowers, Government Accountability Project<br><br>• John DEVITT, Transparency International Ireland |
| 3rd October 2013<br><br>16.00 to 18.30 (BXL) | - Allegations of 'hacking' / tapping into the Belgacom systems by intelligence services (UK GCHQ) | • Mr Geert STANDAERT, Vice President Service Delivery Engine, BELGACOM S.A.<br><br>• Mr Dirk LYBAERT, Secretary General, BELGACOM S.A.<br><br>• Mr Frank ROBBEN, Commission de la Protection de la Vie Privée Belgique, co-rapporteur 'dossier Belgacom' |
| 7th October 2013 19.00 – 21.30 (STR) | - Impact of us surveillance programmes on the us safe harbour | • Dr Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (GERMANY) |

| | | |
|---|---|---|
| | | • Christopher CONNOLLY – Galexia<br>• Peter HUSTINX, European Data Protection Supervisor (EDPS) |
| | - impact of us surveillance programmes on other instruments for international transfers (contractual clauses, binding corporate rules) | • Ms Isabelle FALQUE-PIERROTIN, President of CNIL (FRANCE) |
| 14th October 2013 15.00 - 18.30 (BXL) | - Electronic Mass Surveillance of EU Citizens and International, | • 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' |
| | Council of Europe and | • Judge Bostjan ZUPANČIČ, Judge at the ECHR (via videoconference) |
| | EU Law | • Douwe KORFF, Professor of Law, London Metropolitan University |
| | - Court cases on Surveillance Programmes | • Dominique GUIBERT, Vice-Président of the 'Ligue des Droits de l'Homme' (LDH)<br>• Nick PICKLES, Director of Big Brother Watch<br>• Constanze KURZ, Computer Scientist, Project Leader at Forschungszentrum für Kultur und Informatik |
| 7th November 2013 | - The role of EU IntCen in EU Intelligence activity (in Camera) | • Mr Ilkka SALMI, Director of EU Intelligence Analysis Centre |

| | | |
|---|---|---|
| 9.00 – 11.30 and 15.00 - 18h30 (BXL) | | (IntCen) |
| | - National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law | • Dr Sergio CARRERA, Senior Research Fellow and Head of the JHA Section, Centre for European Policy Studies (CEPS), Brussels<br>• Dr Francesco RAGAZZI, Assistant Professor in International Relations, Leiden University |
| | - The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part I)[129]<br>(Venice Commission) | • Mr Iain CAMERON, Member of the European Commission for Democracy through Law - 'Venice Commission'<br>• Mr Ian LEIGH, Professor of Law, Durham University |
| | (UK) | • Mr David BICKFORD, Former Legal Director of the Security and intelligence agencies MI5 and MI6<br>• Mr Gus HOSEIN, Executive Director, Privacy International |
| | - EU-US transatlantic experts group | • Mr Paul NEMITZ, Director - Fundamental Rights and Citizenship, DG JUST, European Commission<br>• Mr Reinhard PRIEBE, Director - Crisis Management and Internal Security, DG Home, European Commission |
| 11th November | - US surveillance programmes and their impact on EU citizens' privacy | • Mr Jim SENSENBRENNER, US House of Representatives, |

[129] Intelligence oversight bodies of the various EU National Parliaments have been invited to testify at the Inquiry

| | | |
|---|---|---|
| 2013<br><br>15h-18.30 (BXL) | (statement by Mr Jim SENSENBRENNER, Member of the US Congress) | (Member of the Committee on the Judiciary and Chairman of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations) |
| | - The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (NL,SW))(Part II) | • Mr Peter ERIKSSON, Chair of the Committee on the Constitution, Swedish Parliament (Riksdag)<br>• Mr A.H. VAN DELDEN, Chair of the Dutch independent Review Committee on the Intelligence and Security Services (CTIVD |
| | - US NSA programmes for electronic mass surveillance and the role of IT Companies (Microsoft, Google, Facebook) | • Ms Dorothee BELZ, Vice-President, Legal and Corporate Affairs Microsoft EMEA (Europe, Middle East and Africa)<br>• Mr Nicklas LUNDBLAD, Director, Public Policy and Government Relations, Google<br>• Mr Richard ALLAN, Director EMEA Public Policy, Facebook |
| 14th November 2013 15.00 – 18.30 (BXL)<br><br>**With AFET** | - IT Security of EU institutions (Part I) (EP, COM (CERT-EU), (eu-LISA) | • Mr Giancarlo VILELLA, Director General, DG ITEC, European Parliament<br>• Mr Ronald PRINS, Director and co-founder of Fox-IT<br>• Mr Freddy DEZEURE, head of task force CERT-EU, DG DIGIT, European Commission<br>• Mr Luca ZAMPAGLIONE, Security Officer, eu-LISA |
| | - The role of Parliamentary oversight | • Mr Armand DE DECKER, Vice-Chair |

| | | |
|---|---|---|
| | of intelligence services at national level in an era of mass surveillance (Part III)(BE, DA) | of the Belgian Senate, Member of the Monitoring Committee of the Intelligence Services Oversight Committee<br>• Mr Guy RAPAILLE, Chair of the Intelligence Services Oversight Committee (Comité R)<br>• Mr Karsten LAURITZEN, Member of the Legal Affairs Committee, Spokesperson for Legal Affairs – Danish Folketing |
| 18th November 2013 19.00 – 21.30 (STR) | - Court cases and other complaints on national surveillance programs (Part II) (Polish NGO) | • Dr Adam BODNAR, Vice-President of the Board, Helsinki Foundation for Human Rights (Poland) |
| 2nd 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) | • Mr Michael TETZSCHNER, member of The Standing Committee on Scrutiny and Constitutional Affairs, Norway (Stortinget) |
| 5th December 2013, 15.00 – 18.30 (BXL) | - IT Security of EU institutions (Part II)<br><br>- The impact of mass surveillance on confidentiality of lawyer-client relations | • Mr Olivier BURGERSDIJK, Head of Strategy, European Cybercrime Centre, EUROPOL<br>• Prof. Udo HELMBRECHT, Executive Director of ENISA<br>• Mr Florian WALTHER, Independent IT-Security consultant<br><br>• Mr Jonathan GOLDSMITH, Secretary General, Council of Bars and Law Societies of Europe (CCBE) |
| 9th December 2013<br><br>(STR) | - Rebuilding Trust on EU-US Data flows<br><br>- Council of Europe Resolution 1954 (2013) on 'National security and access to information' | • Ms Viviane REDING, Vice President of the European Commission<br><br>• 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' |
| 17th-18th December (BXL) | Parliamentary Committee of Inquiry on Espionage of the Brazilian Senate (Videoconference) | • Ms Vanessa GRAZZIOTIN, Chair of the Parliamentary Committee of Inquiry on Espionage<br>• Mr Ricardo DE REZENDE FERRAÇO, Rapporteur of the Parliamentary Committee of Inquiry on Espionage |
| | IT means of protecting privacy | • Mr Bart PRENEEL, Professor in Computer Security and Industrial Cryptography in the University KU Leuven, Belgium<br>• Mr Stephan LECHNER, Director, Institute for the Protection and Security of the Citizen (IPSC), - Joint Research Centre(JRC), European Commission<br>• Dr Christopher SOGHOIAN, Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union<br>• Christian HORCHERT, IT-Security Consultant, Germany |
| | Exchange of views with the journalist having made public the facts (Part II) (Videoconference) | • Mr Glenn GREENWALD, Author and columnist with a focus on national security and civil liberties, formerly of the Guardian |
| 22 January 2014 (BXL) | Exchange of views on the Russian communications interception practices (SORM)(via videoconference) | • Mr Andrei Soldatov, investigative journalist, an editor of Agentura.ru |

# 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[1]
- Mr Robert S. Litt, General Counsel, Office of the Director of National Intelligence[2]
- 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, Yahoo
- Dr Saskia Horsch, Senior Manager Public Policy, Amazon

[1] The Rapporteur met with Mr Alexander together with Chairman Brok and Senator Feinstein in Washington on 29th October 2013.

[2] The LIBE delegation met with Mr Litt in Washington on 29th October 2013.

**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**

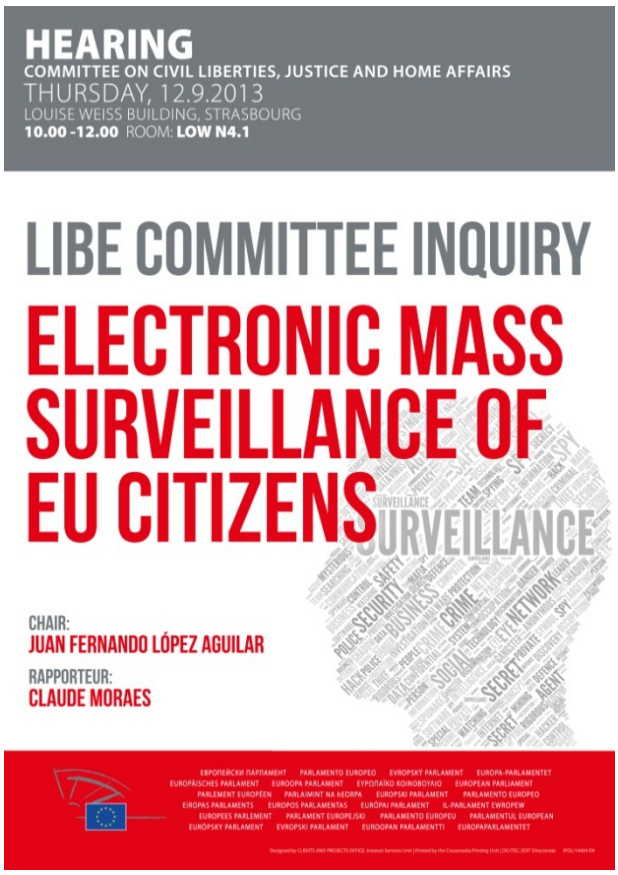
**Netherlands**

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

**Sweden**

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

## Background documents




**LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens**

http://www.europarl.europa.eu/committees/en/libe/events.html?action=1&id=hearings#menuzone

All the documents related to the Inquiry on Electronic Mass Surveillance of EU Citizens, as well as the video recording of the hearings, are accessible on the LIBE (Civil Liberties, Justice and Home Affairs) Committee website by following the link above.

A detailed chronological list of these documents, including a direct link to each one, can be found below.

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 1st Hearing - 05 September 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130905-1500-COMMITTEE-LIBE)

- Draft programme of the LIBE Committee Inquiry on electronic mass surveillance of EU citizens, 15:00 - 18:30 hours
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/1001/1001938/1001938en.pdf
- Duncan CAMPBELL - Interception Capabilities 2014
  http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf
- Dr Gerhard SCHMID - Speaking notes
  http://www.europarl.europa.eu/document/activities/cont/201312/20131203ATT75410/20131203ATT75410EN.pdf
- Background note of the LIBE Secretariat
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_backgrounddivers_/note_backgrounddivers_en.pdf

- Background Note on the EP's temporary committee on the ECHELON interception system http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_echelon_/note_echelon_en.pdf

- Background note on US Legal Instruments for Access and Electronic Surveillance of EU Citizens http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_uslegalinstruments_/note_uslegalinstruments_en.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 2nd Hearing on 12 September 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130912-1000-COMMITTEE-LIBE)

- Draft programme for the LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 12 September 2013, 10.00 - 12.00 hours (LOW N1.3) http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/draft_programme_/draft_programme_en.pdf

- Letter of Vice-President Viviane Reding to Mr Lòpez Aguilar, Chair of LIBE committee of 11 July 2013 on the transatlantic group of experts http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/reding_lopezaguilar_2013071_/reding_lopezaguilar_2013071_en.pdf

- Letter of President Martin Schulz to the Lithuanian Presidency, Ms Dalia Grybauskaite of 11 July 2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/schulz_lt_presidency_20130711_/schulz_lt_presidency_20130711_en.pdf

- Reply Letter of Ms Dalia Grybauskaite, Lithuanian Presidency to President Martin Schulz of 30 July 2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/gribauskaite_schulz_20130730_/gribauskaite_schulz_20130730_en.pdf

- Letter of Jacob Kohnstamm, Chairman of Article 29 Data Protection Working Party to Chair Lòpez Aguilar of 13 August 2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/kohnstamm_lopez_20130813_/kohnstamm_lopez_20130813_en.pdf

- Letter of Jacob Kohnstamm, Chairman of Article 29 Data Protection Working Party to Vice-President Viviane Reding of 13 August 2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/kohnstamm_reding_20130813_/kohnstamm_reding_20130813_en.pdf

- Council document 12183/1/13 REV1 EXT 1 on EU-US Working Group on Data Protection (Declassified) of 9 September 2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/12183_2013_/12183_2013_en.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 3rd Hearing on 24 September 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130924-0900-COMMITTEE-LIBE and http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130924-1500-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 24 September from 9 to 11.30 hours and 15 to 18.30 hours http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/draftagenda_/draftagenda_en.pdf

- Statement to LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citzens by Dr Reinhard Kreissl IRKS Vienna, Coordinator of IRISS http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/kreissl_testimonial_/kreissl_testimonial_en.pdf

- TFTP Agreement http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/1_tftp_agreement_/1_tftp_agreement_en.pdf

- Resolution on TFTP of September 2009 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/2_resolution_tftp_sept_2009_/2_resolution_tftp_sept_2009_en.pdf

- Resolution on TFTP of February 2010 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_resolution_tftp_febr_2010_/3_resolution_tftp_febr_2010_en.pdf

- Resolution on TFTP of May 2010 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/4_resolution_tftp_may_2010_/4_resolution_tftp_may_2010_en.pdf

- Recommandation on TFTP of July 2010 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/5_recommendation_tftp_july_2010_/5_recommendation_tftp_july_2010_en.pdf

- Resolution on TFTP of July 2010 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/6_resolution_tftp_july_2010_/6_resolution_tftp_july_2010_en.pdf

- Letter of Commissioner Mamström to David S. Cohen, Under Secretary - Department of Treasury http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/7_letter-malmstrom_davis_s_cohen_/7_letter-malmstrom_davis_s_cohen_en.pdf

- Briefing note of the Policy Department C: The US surveillance programmes and their impact on EU citizens' fundamental rights http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

- Jens-Henrik JEPPESEN (CDT) written contribution
  http://www.europarl.europa.eu/document/activities/cont/201309/20130925ATT71925/20130925ATT71925EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 4th Hearing on 30 September 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130930-1500-COMMITTEE-LIBE)

- Draft programme of the LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens of 30 September 2013, 15.00 to 18.30 hours
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/draft_agenda20130930_/draft_agenda20130930_en.pdf

- Survey of Federal Whistleblower and Anti-Retaliation Laws by US Congressional Research Service of April 22, 2013
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/crs_whistleblowers_/crs_whistleblowers_en.pdf

- The current state of whistleblower law in Europe: A report by the Government Accountability Project by Thad M. Guyer and Nikolas F. Peterson
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/gap_whistleblowerlawineu_/gap_whistleblowerlawineu_en.pdf

- Binney - Drake - Wiebke PCLOB input
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/pclob_input_/pclob_input_en.pdf

- Thomas DRAKE: short bio
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/drake_bio_/drake_bio_en.pdf

- Kirk WIEBE: short bio
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wiebe_shortbio_/wiebe_shortbio_en.pdf

- Kirk WIEBE: Presentation
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wiebe_presentation_/wiebe_presentation_en.pdf

- Annie MACHON: Biography, Background Material and Recommendations
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/machon_annie_bio_/machon_annie_bio_en.pdf

- Anne MACHON: short bio
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/machon_annie_shortbio_/machon_annie_shortbio_en.pdf

- Jesselyn RADACK: short bio
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/radack_bio_/radack_bio_en.pdf

- GAP Government Accountability Project Whistleblower.org - Briefing points by Jesselyn RADACK
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/radack_briefing_/radack_briefing_en.pdf

- Transparency International report on Money, Politics, Power: Corruption Risks in Europe
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/tireport_moneypoliticspower_/tireport_moneypoliticspower_en.pdf

- Transparency International report on whistleblower protection and the UN convention against corruption
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ti_report_/ti_report_en.pdf

- John DEVITT: Short bio
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/devitt_john_bio_/devitt_john_bio_en.pdf

- Thomas DRAKE - Written Statement
  http://www.europarl.europa.eu/document/activities/cont/201310/20131001ATT72162/20131001ATT72162EN.pdf

- Catherine CRUMP - Written Testimony
  http://www.europarl.europa.eu/document/activities/cont/201310/20131003ATT72272/20131003ATT72272EN.pdf

- Jesselyn RADACK and Edward SNOWDEN Statements
  http://www.europarl.europa.eu/document/activities/cont/201310/20131009ATT72576/20131009ATT72576EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 5th Hearing on 03 October 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131003-1500-COMMITTEE-LIBE)

- Draft programme of the LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens of 03 October 2013, 16.00 to 18.30 hours
  http://www.europarl.europa.eu/document/activities/cont/201309/20130930ATT72076/20130930ATT72076EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 6th Hearing on 07 October 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131007-1900-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 7 October 2013 from 19.00 - 21.30 hours http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/1005/1005206/1005206en.pdf

- Links to websites with documents on international transfers http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/01_links_websites_/01_links_websites_en.pdf

- Commission decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US department of Commerce http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/02_safeharbour_26_7_2000_/02_safeharbour_26_7_2000_en.pdf

- Report on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/03_epreport2000pe_285929_/03_epreport2000pe_285929_en.pdf

- Article 29 Data Protection Working Party: Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles" http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/04_wpopinion_safeharbour_/04_wpopinion_safeharbour_en.pdf

- Commission Staff Working Paper: The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/05_2002-196ecstaff_wp_/05_2002-196ecstaff_wp_en.pdf

- Commission Staff Working Document: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/06_2004-1323ecstaff_report_/06_2004-1323ecstaff_report_en.pdf

- Safe Harbour Decision Implementation Study (only available online for download) http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/07_etude_safe-harbour-2004_/07_etude_safe-harbour-2004_en.pdf

- The US Safe Harbor - Fact or Fiction? (2008) - Galexia Pty Ltd.
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/08_galexia_safe_harbor_/08_galexia_safe_harbor_en.pdf

- Commission decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/10_contra_clauses_2004_915_/10_contra_clauses_2004_915_en.pdf

- Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/11_contr_clauses_2010_87_/11_contr_clauses_2010_87_en.pdf

- Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/12_international_transfers_faq_/12_international_transfers_faq_en.pdf

- Commission decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/09_contr_clauses_2001_497_/09_contr_clauses_2001_497_en.pdf

- Chris CONNOLLY - Presentation on EU/US Safe Harbour
http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf

- Peter HUSTINX - Presentation
http://www.europarl.europa.eu/document/activities/cont/201310/20131009ATT72609/20131009ATT72609EN.pdf

- Dr. Imke SOMMER - Press release
http://www.europarl.europa.eu/document/activities/cont/201310/20131009ATT72578/20131009ATT72578EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 7th Hearing on 14 October 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE)

- Draft programme of the LIBE Committee Inquiry on Electronic Mass Surveillance of EU citizens on Monday, 14 October 2013, Brussels

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/1006/1006304/1006304en.pdf

- International Covenant on Civil and Political Rights: Key elements in the context of the LIBE Committee inquiry
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/statement_professor_scheinin/statement_professor_scheininen.pdf

- The Right to Privacy. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, submitted to the UN Human Rights Council in December 2009
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/right_privacy_un_ga_1209/right_privacy_un_ga_1209en.pdf

- SURVEILLE Deliverable 2.6, Matrix of Surveillance Technologies (pages 1-4)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/surveille_d2-6_matrix_1_4/surveille_d2-6_matrix_1_4en.pdf

- SURVEILLE Deliverable 2.6, Matrix of Surveillance Technologies (pages 8-17)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/surveille_d2-6_matrix_8_17/surveille_d2-6_matrix_8_17en.pdf

- Submission by the EDRi and Fundamental FREE on the surveillance activities of the United States and certain European States' national security and "intelligence" agencies
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/submission_us-europe_edri_final/submission_us-europe_edri_finalen.pdf

- Court cases of 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
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/fidhcourtcase_/fidhcourtcase_en.pdf

- Judgement of the Court (Grand Chamber) of 4 June 2013 in Case C-300/11 (Freedom of movement for persons – Directive 2004/38/EC – Decision refusing a citizen of the European Union admission to a Member State on public security grounds – Article 30(2) of the directive – Obligation to inform the citizen concerned of the grounds of that decision – Disclosure contrary to the interests of State security – Fundamental right to effective judicial protection)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/courjudgement_20130604/courjudgement_20130604en.pdf

- Joint application by Big Brother Watch, Open Rights Group, English pen and Dr. Constanze Kurz, UK under Article 34 to the European Court of Human Rights on national surveillance programs
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/bbw_org_ep_ck_v_uk_/bbw_org_ep_ck_v_uk_en.pdf

- Statement by Professor Martin Scheinin (EUI), formerly UN Special Rapporteur on human rights and counter-terrorism, currently leader of the FP7 consortium SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency)

http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf

- Professor Martin SCHEININ - Statement (ppt)
  http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72924/20131017ATT72924EN.pdf

- Presentation by Douwe Korff, Professor of International Law, London Metropolitan University, London (UK)
  http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72932/20131017ATT72932EN.pdf

- Note by Professor Douwe Korff on EU and International law on trans-national surveillance
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf

- Speaking notes of Constanze Kurz, Computer Scientist, Project Leader at Forschungszentrum für Kultur und Informatik
  http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72935/20131017ATT72935EN.pdf

- Speaker Notes: Nick Pickles, Director, Big Brother Watch
  http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72937/20131017ATT72937EN.pdf

- Dominique GUIBERT - Presentation
  http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72940/20131017ATT72940EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 8th Hearing on 07 November 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131107-0900-COMMITTEE-LIBE and http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131107-1500-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 7 November from 9.00 to 12.15 hours and 15.00 to 18.30 hours
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/0_oj_/0_oj_en.pdf

- Study of the Policy Department: National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/2_poldeptc_study_/2_poldeptc_study_en.pdf

- Report on the democratic oversight of the security services (adopted by the Venice Commission, 1-2 June 2007)

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_cdl-ad(2007)016_/3_cdl-ad(2007)016_en.pdf

- Letter to the LIBE Committee from Privacy International
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_privacy_int_/3_privacy_int_en.pdf

- Presentation of the Policy Department C on: National Programmes for Mass Surveillance in EU Member States and Compatibility with EU law made by Dr. Sergio CARRERA and Dr. Francesco RAGAZZI
  http://www.europarl.europa.eu/document/activities/cont/201311/20131105ATT73945/20131105ATT73945EN.ppt

- David BICKFORD CB (Judicial Scrutiny of Intelligence Agencies) - Presentation
  http://www.europarl.europa.eu/document/activities/cont/201311/20131105ATT73943/20131105ATT73943EN.pdf

- Professor Iain CAMERON - Speaking notes (Venice Commission)
  http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74429/20131114ATT74429EN.pdf

- Statement by Professor Ian LEIGH and Mr Aidan WILLS
  http://www.europarl.europa.eu/document/activities/cont/201401/20140120ATT77923/20140120ATT77923EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 9th Hearing on 11 November 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131111-1500-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 11 November from 15.00 to 18.30 hours
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/oj_11-11_/oj_11-11_en.pdf

- USA Freedom Act
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/usafreedomact_/usafreedomact_en.pdf

- Letter from Google Belgium to the Chairman of the LIBE Committee
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/google_letter_/google_letter_en.pdf

- Apple report on Government information request
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/apple_letter_/apple_letter_en.pdf

- Richard ALLAN - Statement (Facebook)
  http://www.europarl.europa.eu/document/activities/cont/201311/20131111ATT74240/20131111ATT74240EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 10th Hearing on 14 November 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131114-1500-COMMITTEE-LIBE)

– Draft agenda of the LIBE Inquiry meeting of 14 November from 15.00 to 18.30 hours http://www.europarl.europa.eu/document/activities/cont/201311/20131111ATT74236/20131111ATT74236EN.pdf

– Luca ZAMPAGLIONE - Presentation (eu-LISA) http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74418/20131114ATT74418EN.pdf

– Guy RAPAILLE - Stetement (Comité R) - NL-FR http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74420/20131114ATT74420FR.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 11th Hearing on 18 November 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131118-1930-COMMITTEE-LIBE)

– Draft agenda of the LIBE Inquiry meeting of 18 November from 19.30 to 21.45 hours http://www.europarl.europa.eu/document/activities/cont/201311/20131115ATT74512/20131115ATT74512EN.pdf

– Adam BODNAR - Speaking notes (Helsinki Foundation) http://www.europarl.europa.eu/document/activities/cont/201311/20131115ATT74519/20131115ATT74519EN.pdf

– Adam BODNAR and Katarzyna SZYMIELEWICZ - Article The Guardian http://www.europarl.europa.eu/document/activities/cont/201311/20131115ATT74521/20131115ATT74521EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 12th Hearing on 02 December 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131202-1500-COMMITTEE-LIBE)

– Draft agenda of the LIBE Inquiry meeting of 02 December from 15.00 to 17.00 hours http://www.europarl.europa.eu/document/activities/cont/201312/20131202ATT75299/20131202ATT75299EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 13th Hearing on 05 December 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131205-1500-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 5 December from 15:00 - 18:30 hours
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/oj_inquiry_/oj_inquiry_en.pdf

- Working Document 1 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights (Moraes)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf

- Working Document 3 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights (Moraes-Albrecht)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd3_moraes_1011370/wd3_moraes_1011370en.pdf

- Working Document 4 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights (Moraes-Voss)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd4_1011371/wd4_1011371en.pdf

- Working Document 5 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights (Moraes-In 'T Veld-Ernst)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd5_moraes_1009342/wd5_moraes_1009342en.pdf

- Final Working Document on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens (AFET Committee)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/afet_wd_/afet_wd_en.pdf

- CCBE Statement on mass electronic surveillance by government bodies (including of European lawyers' data)
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ccbe_statement_/ccbe_statement_en.pdf

- Report by D.A.O. EDWARD, Q.C. on the Professional secret, confidentiality and legal professional privilege in the nine Member States of the European Community
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ccbe_edward_report_/ccbe_edward_report_en.pdf

- Update on the report by D.A.O. EDWARD, Q.C. on the Professional secret, confidentiality and legal professional privilege in Europe
  http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ccbeedward_report_update_/ccbeedward_report_update_en.pdf

- Jonathan GOLDSMITH - Presentation (CCBE)
  http://www.europarl.europa.eu/document/activities/cont/201312/20131204ATT75508/20131204ATT75508EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 14th Hearing on 09 December 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131209-1845-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 9 December from 19:30 - 21:30 hours http://www.europarl.europa.eu/document/activities/cont/201312/20131204ATT75506/20131204ATT75506EN.pdf

- Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/i_rebuild_trust_/i_rebuild_trust_en.pdf

- Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/i_safeharbour_/i_safeharbour_en.pdf

- Resolution 1954(2013) (provisional version) National security and access to information http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ii_resolution_/ii_resolution_en.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 15th Hearing on 17-18 December 2013** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131217-1500-COMMITTEE-LIBE and http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131218-0900-COMMITTEE-LIBE)

- Draft agenda of the LIBE Inquiry meeting of 17-18 December from 16:30 - 18:30 and 09:00 - 12:30 hours http://www.europarl.europa.eu/document/activities/cont/201312/20131213ATT76114/20131213ATT76114EN.pdf

* **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - Meeting on 22 January 2014** (watch it on EPTV: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20140122-0900-COMMITTEE-LIBE)

- Exchange of views on the Russian communications interception practices (SORM) - Powerpoint presentation of Andrei Soldatov, investigative journalist http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/soldatov_presentation_/soldatov_presentation_en.pdf

- CV of Andrei Soldatov http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/cv_soldatov_/cv_soldatov_en.pdf

## Procedure documents

Procedure file - **2013/2188(INI):**
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2013/2188(INI)

- LIBE Committee draft 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:
  http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-526.085+02+DOC+PDF+V0//EN&language=EN

- Amendments tabled in Committee:
  http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE527.988 and
  http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE527.993

- LIBE Committee 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, as tabled for Plenary:
  http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN