VS- NUR FÜR DEN DIENSTGEBRAUCH

Bundeskanzleramt

Bundeskanzleramt, 11012 Berlin

Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

MAT A BK-1/4s

zu A-Drs.: 2

Philipp Wolff
Beauftragter des Bundeskanzleramtes
1. Untersuchungsausschuss
der 18. Wahlperiode

HAUSANSCHRIFT Willy-Brandt-Straße 1, 10557 Berlin
POSTANSCHRIFT 11012 Berlin

TEL +49 30 18 400-2628
FAX +49 30 18 400-1802
E-MAIL philipp.wolff@bk.bund.de
pgua@bk.bund.de

An den
Deutschen Bundestag
Sekretariat des
1. Untersuchungsausschusses
der 18. Wahlperiode
Platz der Republik 1
11011 Berlin

Deutscher Bundestag
1. Untersuchungsausschuss
29. Aug. 2014

Berlin, 25. August 2014

BETREFF 1. Untersuchungsausschuss der 18. Wahlperiode

HIER 4. Teillieferung zu den Beweisbeschlüssen BK-1 und BK-2

AZ 6 PGUA – 113 00 – Un1/14 VS-NfD

BEZUG Beweisbeschluss BK-1 vom 10. April 2014
Beweisbeschluss BK-2 vom 10. April 2014
Beweisbeschluss BND-1 vom 10. April 2014

ANLAGE 27 Ordner (offen und VS-NfD)

Sehr geehrte Damen und Herren,

in Teilerfüllung der im Bezug genannten Beweisbeschlüsse übersende ich Ihnen die folgenden 29 Ordner (2 Ordner direkt an die Geheimschutzstelle):

- Ordner Nr. 71, 72, 73, 74, 80, 81, 82, 83, 84, 85, 87, 89, 90, 93, 94, 95 und 98 zu Beweisbeschluss BK-1,
- Ordner Nr. 75, 77, 78, 79, 96, 97 und 99 zu Beweisbeschlüssen BK-1 und BK-2,
- Ordner Nr. 76, 86 und 88 zu Beweisbeschluss BND-1
- sowie über die Geheimschutzstelle des Deutschen Bundestages zu den Beweisbeschlüssen BK-1 und BK-2:
  - VS-Ordner 91 und 92
  - VS-Ordner zu den Ordnern 75, 77, 78, 79, 90 und 93

...

1. Auf die Ausführungen in meinen letzten Schreiben, insbesondere zur gemeinsamen Teilerfüllung der Beweisbeschlüsse BK-1 und BK-2, zum Aufbau der Ordner, zur Einstufung von Unterlagen, die durch Dritte der Öffentlichkeit zugänglich gemacht wurden und zur Erklärung über gelöschte oder vernichtete Unterlagen, darf ich verweisen.

2. Alle VS-Ordner wurden wunschgemäß unmittelbar an die Geheimschutzstelle des Deutschen Bundestages übersandt. An dem Übersendungsschreiben wurden Sie in Kopie beteiligt.

Bei den eingestuften Ordnern handelt es sich überwiegend um Zuarbeiten zu verschiedenen Antwortentwürfen sowie um interne vertrauliche Kommunikation zwischen hochrangigen Regierungsvertretern. Eine Offenlegung dieser Dokumente wäre für die Interessen der Bundesrepublik Deutschland schädlich oder könnte ihnen schweren Schaden zufügen.

3. Im Hinblick auf die Handhabung von Unterlagen gem. Verfahrensbeschluss 5, Ziff. III, die nach der VSA als „STRENG GEHEIM" eingestuft sind, wurden derartige Unterlagen soweit sinnvoll in einen gesonderten VS-Ordner einsortiert.

Die vorliegende Übersendung enthält zudem Dokumente, die als „GEHEIM SCHUTZWORT" oder „GEHEIM ANRECHT" eingestuft sind. Derartige Unterlagen werden nur einem gesondert ermächtigten kleinen Personenkreis zugänglich gemacht und sind daher als „höher als ‚GEHEIM' eingestufte Unterlagen" im Sinne des o.g. Verfahrensbeschlusses anzusehen. Im Hinblick auf die Handhabung im Deutschen Bundestag wurden diese Unterlagen daher ebenfalls im „STRENG GEHEIM"-Ordner einsortiert. Es wird darum gebeten, diese Unterlagen nur zur Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages bereitzustellen.

4. Soweit im Bundeskanzleramt von VS-Dokumenten Überstücke gefertigt wurden (dies betrifft insbesondere Mappen für Teilnehmer der Sitzungen der PKGr und der G10-Kommission, die nach der Sitzung zurückgegeben, bislang aber noch nicht vernichtet wurden), werden die Überstücke aus Gründen der Über-

sichtlichkeit nicht vorgelegt, sofern sie keine Anmerkungen oder sonstigen individuellen Unterschiede zum Vorlageexemplar aufweisen.

5. Soweit Dokumente insb. zu den in den Beweisbeschlüssen BK-2 bzw. BND-2 angesprochenen Fragen übersandt werden, geht das Bundeskanzleramt davon aus, dass Themenkomplexe, die bereits in Untersuchungsausschüssen früherer Wahlperioden aufgearbeitet wurden, nicht erneut dem Parlament vorgelegt werden sollen. Sollte der 1. Untersuchungsausschuss der 18. Wahlperiode ein anderes Verfahren wünschen, so wird um entsprechenden Hinweis gebeten.

6. Das Bundeskanzleramt arbeitet weiterhin mit hoher Priorität an der Zusammenstellung der Dokumente zu den Beweisbeschlüssen, deren Erfüllung dem Bundeskanzleramt obliegt. Weitere Teillieferungen werden dem Ausschuss schnellstmöglich zugeleitet.

Mit freundlichen Grüßen
Im Auftrag

(Wolff)

Ressort

Bundeskanzleramt

Berlin, den

11.07.2014

Ordner

77

Aktenvorlage
an den
1. Untersuchungsausschuss
des Deutschen Bundestages in der 18. WP

gemäß Beweisbeschluss:	vom:
BK-1, BK-2	10.04.2014

Aktenzeichen bei aktenführender Stelle:

603 – 15100 – Bu10NA2, Band 14a

VS-Einstufung:

VS-NUR FÜR DEN DIENSTGEBRAUCH

Inhalt:

[schlagwortartig Kurzbezeichnung d. Akteninhalts]

Snowden-Enthüllungen
Sachverhaltsaufklärung
EU, LIBE-Ausschuss

Bemerkungen:

VS - Nur für den Dienstgebrauch

Inhaltsverzeichnis

Ressort

Bundeskanzleramt

Berlin, den

11.07.2014

Ordner

77

Inhaltsübersicht
zu den vom 1. Untersuchungsausschuss der 18. Wahlperiode beigezogenen Akten
hier: Beweisbeschlüsse BK-1, BK-2

des:

Referates	603

Aktenzeichen bei aktenführender Stelle:

603-15100-Bu10NA2, Band 14a

VS-Einstufung:

VS-NUR FÜR DEN DIENSTGEBRAUCH

Blatt	Zeitraum	Inhalt/Gegenstand	Bemerkungen
1-317		**Sachverhaltsaufklärung**	
1-317		**EU, LIBE-Ausschuss**	
1-2	03.07.2013	Mail BKAmt 603 an AL6 Weiterleitung Mail BKAmt 132 zum AStV am 04.07.2013	
3-4	04.07.2013	Drahtbericht Brüssel Euro Nr. 3428 an AA und BKAmt 252/2013 VS-Vertraulich, 3. Exemplar Materielle Sicherheit der EU-Institutionen AA VS-RegNr. 10156/13 vsv in 603-Bu10NA2	Dok. siehe VS-Ordner BK-Kopie 2
5	o.D.	Statement by the Chair of COREPER	

		Proposed compromise text for COREPER agreement on EU-US
6		Mail BKAmt 603 an AL6
		Weiterleitung Mail 501
7-9	05.07.2013	Interne Mail BKAmt 603
		Weiterleitung Mail 132
		DEU Vertreter für Auftaktveranstaltung COREPER
10	05.07.2013	Interne Mail BKAmt 603
		Weiterleitung Mail 501
		Hinweis, dass KOM durch Dir. Priebe und Dir. Nemitz vertreten ist
11-14	05.07.2013	Mail BKAmt 603 an AL6
		Sachstand zu mögl. Teilnahme BND oder BMI an COREPER-Auftaktveranstaltung
15-16	05.07.2013	Mail BKAmt 603 an Pressesprecherin ChBK
		Sprachregelung zur Kooperation des BND mit Partnern mit der Bitte um Freigabe
17		Anlage: Sprachregelung
18-20	10.07.2013	Mail BKAmt 603 an AL6
		Weiterleitung Mail 132: Weisungsentwurf zu TOP EU-US-High level expert group on security and data protection
21-24		Anlage: Text der Weisung
25-27	12.07.2013	Mail BKAmt 603 an BMI
		Änderung am Weisungsentwurf
28-34		Anlage: Weisungsentwurf
35-86	23.12.2013	Draft Report des Committe on Civil Liberties, Justice and Home Affairs des EP
87-91	09.01.2014	Draft Agenda zum LIBE-Treffen
92-93	10.01.2014	Mail BND an BKAmt 603
		Richtigstellung zur Aussage im LIBE-Berichtsentwurf, wonach Pr BND keine Antwort auf Einladung gegeben habe
94	20.11.2013	Anlage: Brief Pr BND an LIBE-Vorsitzenden
95-97	13.01.2013	Draft Agenda zum LIBE-Treffen extraordinary meeting
98	14.01.2014	Mail BKAmt 603 an BND
		Bitte um Bewertung des LIBE-Berichts

99	14.01.2014	Mail BKAmt 603 an BMI Bitte um Bewertung des LIBE-Berichts
100-101	14.01.2014	Weiterleitung Mail des BMI Hinweis auf dortige Befassung mit LIBE-Bericht
102	14.01.2014	Mail BL ChBK an Verteiler im Hause Weiterleitung Mail des MdEP Voss zum Überwachungsprogramm der NSA
103-104	15.01.2014	Mail BKAmt 603 an BND Bitte um Anregungen für Änderungsvorschläge
105-107	16.01.2014	Mail BND an BKAmt 603 Stellungnahme zum LIBE-Bericht
108-110	17.01.2014	Mail BKAmt 603 an BND Bitte um Übermittlung des Einladungsschreibens des LIBE-Ausschussvorsitzenden an Pr BND vom 14.10.2013
111	17.01.2014	Mail BND an BKAmt 603 Übersendungsmail zum erbetenen Einladungsschreiben an Pr BND
112		Anlage: Einladungsschreiben
113-114	17.01.2014	Schreiben BKAmt 603 an BND, VS-NfD Bitte um Befassung des BKAmtes im Vorfeld von Äußerungen gegenüber nationalen und internationalen Organen und Gremien sowie gegenüber Presse Vfg.
115	17.01.2014	Schreiben BKAmt 603 an BND, VS-NfD Bitte um Befassung des BKAmtes im Vorfeld von Äußerungen gegenüber nationalen und internationalen Organen und Gremien sowie gegenüber Presse 1. Ausfertigung
116		Faxbeleg
117-120	17.01.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an St Fritsche Stellungnahme und Einschätzung des BND zur LIBE-Berichtsentwurf

		Vfg.
121-124	17.01.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an St Fritsche Stellungnahme und Einschätzung des BND zur LIBE-Berichtsentwurf 1. Ausfertigung
125	20.01.2014	Mail BKAmt 603 an BND Ergänzender Hinweis auf Schriftform von Mitteilungen an BKAmt (siehe Pos. 115)
126-130	20.01.2014	Mail BND an BKAmt 603 Hinweis auf notwendige Klarstellungen im LIBE-Berichtsentwurf
131-134	21.01.2014	Interne Mail BKAmt 603 Weiterleitung Mail PSt BMI an MdEP Voss
135-185	23.12.2013	Anlage: Draft Report LIBE
186-246	21.02.2014	LIBE-Report Plenary Sitting
247	21.01.2014	Mail BKAmt 132 an 603 Mitzeichnung der Vorlage 603 zum LIBE-Bericht mit Änderungen
248	21.01.2014	Mail BKAmt 601 an 603 Mitzeichnung der Vorlage 603
249-252	21.01.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an BL ChBK Stellungnahme zum LIBE-Berichtsentwurf und Einbringung von Änderungsvorschlägen 1. Ausfertigung
253-256	21.01.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an BL ChBK Stellungnahme zum LIBE-Berichtsentwurf und Einbringung von Änderungsvorschlägen Vfg.
257-260	24.01.2014	Amendments 1-265 des LIBE-Committees
261-264	25.02.2014	Interne Mail BKAmt 603 Weiterleitung Mail BL ChBK (Mail Büro MdEP Voss an BL ChBK)
265-267	28.01.2014	Interne Mail BKAmt 603 Bitte um Weiterleitung des Antwortschreibens Pr BND an Ausschussvorsitzenden an BL ChBK

268-270	28.01.2014	Mail BKAmt 603 an BL ChBK Übersendung Antwortbrief Pr BND an LIBE-Ausschussvorsitzenden
271	20.11.2013	Anlage: Antwortschreiben des BND
272-277	30.01.2014	Draft Agenda LIBE-Treffen
278-281	31.01.2014	Interne Mail BKAmt 603 Weiterleitung aktueller Sachstand hinsichtlich LIBE-Endberichts
282	06.02.2014	Schreiben LIBE-Ausschussvorsitzender an Pr BND
283-284	11.02.2014	Mail BKAmt 603 an AL6 Weiterleitung des Schreibens an Pr BND gem. Pos. 283
285	11.02.2014	Mail BKAmt AL6 an 603 Bitte um Entwurf einer Vorlage
286-289	13.02.2014	Mail BKAmt 503 an 603 Hinweis zu Vorlage bzw. zu weiterem Vorgehen
290-291		Anlage: Vorlage 603 an BL ChBK zum Schreiben des LIBE-Vorsitzenden an Pr BND und Bitte um Beteiligung am Vorgang durch BT-Verwaltung
292	13.02.2014	Artikel Die Welt „Europaparlament rechnet mit NSA und BND ab“
293	13.02.2014	Mail BKAmt 121 an 603 Anregung, FF zur Antwort gegenüber BT-Verwaltung im BKAmt zu belassen
294-296	14.02.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an BL ChBK zum Schreiben des LIBE-Vorsitzenden an Pr BND und Bitte um Beteiligung am Vorgang durch BT-Verwaltung Vfg.
297-298	14.02.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an BL ChBK zum Schreiben des LIBE-Vorsitzenden an Pr BND und Bitte um Beteiligung am Vorgang durch BT-Verwaltung 1. Ausfertigung

299-300	21.02.2014	Interne Mail BKAmt 603 Weiterleitung einer Mail von BKAmt 603 an Europabüro-Koordination Bundestag
301	20.11.2013	Anlage: Brief Pr BND an LIBE-Ausschussvorsitzenden
302	27.02.2014	Mail BKAmt 603 an BMI Übersendung Vorabfassung des LIBE-Berichts mit der Bitte um Prüfung hinsichtl. Änderungsbedarf
303	27.02.2014	Mail BKAmt 603 an BND Übersendung Vorabfassung des LIBE-Berichts mit der Bitte um Prüfung hinsichtl. Änderungsbedarf
304-306	03.03.2014	Mail BND an BKAmt 603 Übersendung der Bewertung zum LIBE-Bericht
307	03.03.3014	Mail BMI an BKAmt 603 Übersendung des Entwurfs einer Stellungnahme des BMI
308-310		Anlage: Stellungnahme des BMI
311	03.03.3014	Mail BKAmt 603 an 601, 132, 413 Bitte um Prüfung des LIBE-Berichtsentwurfs
312-314	03.03.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an BL ChBK Stellungnahme zum konsolidierten Bericht des LIBE-Ausschusses Vfg.
315-317	03.03.2014	603-15100-Bu10/14 NA 2 VS-NfD Vorlage 603 an BL ChBK Stellungnahme zum konsolidierten Bericht des LIBE-Ausschusses 1. Ausfertigung

Anlage zum Inhaltsverzeichnis

Ressort

Bundeskanzleramt

Berlin, den

11.07.2014

Ordner

603-15100-Bu10NA2, Band 14a 77

VS-Einstufung:

VS-NUR FÜR DEN DIENSTGEBRAUCH

Blatt	Begründung
92-93	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM), Telefonnummern deutscher Nachrichtendienste (TEL)
98	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
103	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
105-106	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
108-110	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
111	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
113	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
115-116	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM), Telefonnummern deutscher Nachrichtendienste (TEL)
125	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
126-129	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM), Telefonnummern deutscher Nachrichtendienste (TEL)
284	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)
303	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM)

304-305	Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste (NAM), Telefonnummern deutscher Nachrichtendienste (TEL)

Anlage 2 zum Inhaltsverzeichnis

In den nachfolgenden Dokumenten wurden teilweise Informationen entnommen oder unkenntlich gemacht. Die individuelle Entscheidung, die aufgrund einer Einzelfallabwägung jeweils zur Entnahme oder Schwärzung führte, wird wie folgt begründet (die Abkürzungen in der Anlage zum Inhaltsverzeichnis verweisen auf die nachfolgenden den Überschriften vorangestellten Kennungen):

NAM: Namen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste

Die Vor- und Nachnamen von Mitarbeiterinnen und Mitarbeitern deutscher Nachrichtendienste sowie personengebundene E-Mail-Adressen wurden zum Schutz von Leib und Leben sowie der Arbeitsfähigkeit der Dienste unkenntlich gemacht. Durch eine Offenlegung gegenüber einer nicht kontrollierbaren Öffentlichkeit wäre der Schutz dieser Mitarbeiter nicht mehr gewährleistet und der Personalbestand wäre möglicherweise für fremde Mächte potenziell identifizier- und aufklärbar. Hierdurch wäre im Ergebnis die Arbeitsfähigkeit und mithin das Staatswohl der Bundesrepublik Deutschland gefährdet.

Nach Abwägung der konkreten Umstände, namentlich dem Informationsinteresse des parlamentarischen Untersuchungsausschusses einerseits und den oben genannten Gefährdungen für die betroffenen Mitarbeiterinnen und Mitarbeiter sowie der Nachrichtendienste und dem Staatswohl andererseits sind die Namen zu schwärzen. Dem Informationsinteresse des Untersuchungsausschusses wurde dabei in der Form Rechnung getragen, dass die Initialen der Betroffenen aus dem Geschäftsbereich des Bundeskanzleramtes ungeschwärzt belassen werden, um jedenfalls eine allgemeine Zuordnung zu ermöglichen. Zudem wird das Bundeskanzleramt bei ergänzenden Nachfragen des Untersuchungsausschusses in jedem Einzelfall prüfen, ob eine weitergehende Offenlegung aufgrund eines konkreten zum gegenwärtigen Zeitpunkt für das Bundeskanzleramt noch nicht absehbaren Informationsinteresses des Ausschusses doch möglich ist. Schließlich wurden die Namen von Personen, die – soweit hier bekannt – aufgrund ihrer Funktion im jeweiligen Nachrichtendienst bereits als Mitarbeiter eines deutschen Nachrichtendienstes in der Öffentlichkeit bekannt sind, ebenfalls ungeschwärzt belassen.

...

TEL: Telefonnummern deutscher Nachrichtendienste

Telefon- und Faxnummern bzw. Teile davon (insb. die Nebenstellenkennungen) deutscher Nachrichtendienste wurden zum Schutz der Kommunikationsverbindungen unkenntlich gemacht. Die Offenlegung einer Vielzahl von Telefonnummern und insbesondere von Nebenstellenkennungen gegenüber einer nicht abschließend einschätzbaren Öffentlichkeit erhöht die Gefahr einer fernmeldetechnischen Aufklärung dieser Anschlüsse und damit erheblicher Teile des Telefonverkehrs der Dienste. Hierdurch wäre die Kommunikation der Dienste mit anderen Sicherheitsbehörden und mit ihren Bedarfsträgern nach Art und Inhalt für fremde Mächte aufklärbar und somit die Funktionsfähigkeit, mithin das Staatswohl der Bundesrepublik Deutschland, beeinträchtigt.

Bei der Abwägung zwischen dem Informationsinteresse des Untersuchungsausschusses einerseits und den oben genannten Gefährdungsaspekten andererseits ist zu berücksichtigen, dass die Aufklärung des Sachverhalts – nach gegenwärtiger Einschätzung – voraussichtlich nicht der Bekanntgabe einzelner Telefonnummern oder Nebenstellenkennungen bedarf. Eine Zuordnung der Schriftstücke anhand der Namen bzw. Initialen bleibt dabei grundsätzlich möglich. Im Ergebnis sind die Telefonnummern daher unkenntlich gemacht worden.

MAT A BK-1-4s.pdf, Blatt 15

000001

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Mittwoch, 3. Juli 2013 14:12
An: AL-6; Schäper, Hans-Jörg; ref601; ref603
Betreff: WG: EIlt sehr: 2459. AStV (Teil 2) am 04.07.2013 - Nachforderung von Weisungen; TOP 30 (Prism)

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Rensmann, Michael
Gesendet: Mittwoch, 3. Juli 2013 14:08
An: Konow, Christian; Nell, Christian; Gothe, Stephan
Cc: Bartodziej, Peter; Hornung, Ulrike
Betreff: AW: EIlt sehr: 2459. AStV (Teil 2) am 04.07.2013 - Nachforderung von Weisungen; TOP 30 (Prism)

Liebe Kollegen,

ich habe BMI vorsorglich darauf hingewiesen, dass ggf. noch Änderungswünsche über AA zu erwarten sind.

Unabhängig davon wird BMI die Weisung noch einmal dahingehend konkretisieren, dass jedenfalls die AG zum Thema Nachrichtendienste nur durch US und MS bestellt wird (ohne KOM). Die Aufgabendefinition der geplanten AG zum Datenschutz ist noch nicht klar absehbar. Die Präsidentschaft beabsichtigt hier wohl, über den Bereich der EU-Rechtsakte hinauszugehen (und damit auch ND-spezifischen Datenschutz einzubeziehen). Auch für diesen Fall wird BMI bestrebt sein, die Einbindung der KOM angemessen zu gestalten.

Viele Grüße
Michael Rensmann

Von: Rensmann, Michael
Gesendet: Mittwoch, 3. Juli 2013 13:23
An: Konow, Christian; Nell, Christian; Gothe, Stephan
Cc: Bartodziej, Peter; Hornung, Ulrike
Betreff: WG: EIlt sehr: 2459. AStV (Teil 2) am 04.07.2013 - Nachforderung von Weisungen; TOP 30 (Prism)
Wichtigkeit: Hoch

Liebe Kollegen,

MAT A BK-1-4s.pdf, Blatt 16

000002

anliegenden Weisungsentwurf des BMI auch für Sie z.K.

Viele Grüße
Michael Rensmann

Von: Spitzer, Patrick, Dr.
Gesendet: Mittwoch, 3. Juli 2013 12:46
An: BMJ Harms, Katharina; BMJ Henrichs, Christoph; BMJ Sangmeister, Christian
Cc: OESI3AG_; Peters, Reinhard; AA Oelfke, Christian; BK Rensmann, Michael; AA Eickelpasch, Jörg; Pinargote Vera, Alice; Taube, Matthias; Jergl, Johann; Lesser, Ralf; Schäfer, Ulrike
Betreff: EIlt sehr: 2459. AStV (Teil 2) am 04.07.2013 - Nachforderung von Weisungen; TOP 30 (Prism)
Wichtigkeit: Hoch

Sehr geehrte Damen und Herren,

anbei übersende ich einen Entwurf einer Weisung für den – nachgemeldeten - TOP 30 für die morgige Sitzung des AStV mit der Bitte um Prüfung und Mitzeichnung bis **heute (3. Juli) 13. 45 Uhr**. Ich bitte um Verständnis für die sehr kurze Frist. Das Vorbereitungspapier des lit. Vors. wurde erst heute Vormittag verteilt.

Herzlichen Dank und Freundliche Grüße

im Auftrag

Dr. Patrick Spitzer

Bundesministerium des Innern

Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,

BKA-Gesetz, Datenschutz im Sicherheitsbereich)

Alt-Moabit 101D, 10559 Berlin

Telefon: +49 (0)30 18681-1390

E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

000003 - 000004

Die an dieser Stelle entnommenen Blätter
befinden sich im VS-Ordner
Aktenzeichen: 603-15100-Bu10NA2, Band 14a

Item High Level Group, point 30

Statement by the Chair of Coreper (to be included in the minutes of Coreper on 4 July but not distributed to delegations)

I have concluded the following today:

We need to work quickly. A process will be launched today which will begin with a meeting on Monday in Washington DC. The object of the meeting is to clarify as much as possible the issues at stake. The meeting will deal with data protection and privacy rights of EU citizens falling within the competence of the EU, addressing the scope and composition of future meetings.

There is no remit and format agreed for the process. This issue will be the subject of further reflection by COREPER. We will get back on this next week in the light of the report from the meeting in Washington.

Without prejudice to the division of competences, the EU will be represented at this meeting by the Commission, the Presidency and the EEAS. The meeting will be co-chaired on the EU side by the Commission and the Presidency. Any Member State wishing to participate should inform the Presidency by [insert date]. The Lithuanian government will represent the interests of Member States not represented at this meeting. If, during the discussions matters relating to national security or intelligence, which fall within Member States sole competence, arise only the Member States and the US will participate in those discussions.

Following the meeting, the Commission, EEAS and Presidency will report back to COREPER.

Decisions about the further development of the process will become the subject of appropriate considerations, including appropriate attendance. At this stage, the holding of the meeting does not prejudge this issue. COREPER will begin an examination of this at its next meeting.

Gelöscht: ¶
¶

Gelöscht: an initial

Gelöscht: . ¶
¶
Should any issue relating to the competence of the member States arise at the meeting, the Lithuanian government will represent the interests of the Member States.¶
¶

Gelöscht: Coreper

Gelöscht: ¶
¶
The

Gelöscht: and

Gelöscht: ¶
¶
The

Gelöscht: oreper

Gelöscht: and will receive regular reports on progress of the development of the process.

Gelöscht: ¶
Member States are invited to designate appropriate experts for the further process as soon as possible and preferably before 11 July.¶
¶

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Freitag, 5. Juli 2013 08:52
An: AL-6; Schäper, Hans-Jörg; ref601
Cc: ref603
Betreff: WG: EILT: Proposed compromise text for COREPER agreement on EU-US

Anlagen: 130705 COREPER declaration track changes FINAL.doc



130705 COREPER declaration tra...

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 08:50
An: Meyer-Landrut, Nikolaus; Neueder, Franz; Rensmann, Michael; Hornung, Ulrike; Jung, Alexander; Gothe, Stephan; Nell, Christian
Betreff: WG: EILT: Proposed compromise text for COREPER agreement on EU-US

z.K., es ging gestern abend noch munter hin und her. Neuer Text ist - auf Wunsch UK - wesentlich sensibler hinsichtlich Kompetenzverteilung EU/MS und versucht zudem, Zusammensetzung der Expertengruppen noch nicht zu präjudizieren.

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: .MOBILEU BRUE-POL-EU2-1 Dieter, Robert [mailto:pol-eu2-1-eu@brue.auswaertiges-amt.de]
Gesendet: Freitag, 5. Juli 2013 07:56
An: Konow, Christian; Felsheim, Georg; E-B-2 Schoof, Peter; .BRUEEU L Tempel, Peter; peter.tempel@stv-eu.info; .BRUEEU POL-IN2-2 Eickelpasch, Joerg; E05-RL Grabherr, Stephan
Betreff: EILT: Proposed compromise text for COREPER agreement on EU-US

Hier jetzt der zwischen den genannten Delegation vereinbarte Text für die AStV-Erklärung. Vereibart ist, dass sie jetzt noch einmal unter Verschweigen gestellt wird, damit sie dann zügig das Licht der Welt erblicken kann.

Gruß
RD

-------- Original-Nachricht --------
Betreff: Proposed compromise text for COREPER agreement on EU-US
Datum: Fri, 5 Jul 2013 00:22:52 +0000
Von: Iain.Frew@fco.gov.uk
An: Nerijus.ALEKSIEJUNAS@eu.mfa.lt, antici@eu.mfa.lt
CC: cyril.piquemal@diplomatie.gouv.fr,

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Freitag, 5. Juli 2013 11:28
An: ref603
Betreff: WG: EILT: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.

Wichtigkeit: Hoch

Anlagen: 130705 COREPER declaration track changes FINAL.doc



130705 COREPER declaration tra...

Das sollte zu StäV und AL

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 605

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Posanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.Gothe@bk.bund.de
E-Mail: ref605@bk.bund.de

----- Ursprüngliche Nachricht -----
Von: Rensmann, Michael <Michael.Rensmann@bk.bund.de>
Gesendet: Freitag, 5. Juli 2013 11:06
An: ref601 <ref601@bk.bund.de>; ref603 <ref603@bk.bund.de>
Cc: Bartodziej, Peter <Peter.Bartodziej@bk.bund.de>
Betreff: EILT: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.

Liebe Kolleginnen und Kollegen,

ich würde eine Teilnahme durch DEU (im Rahmen des terminlich/logistisch Möglichen) hier grundsätzlich ebenfalls befürworten.

Vor dem Hintergrund der klaren ND-Ausrichtung, auf die ja nicht zuletzt im Zusammenhang mit der Beteiligung der KOM mehrfach verwiesen wird und der zu erwartenden Inhalte wäre aber die Frage der Teilnahme m.E. durch Abt. 6 gemeinsam mit BMI zu entscheiden. Insofern wäre ich für entsprechende Übernahme dankbar.

Mit freundlichen Grüßen
Michael Rensmann

Dr. Michael Rensmann
Bundeskanzleramt
Referat 132
Angelegenheiten des Bundesministeriums des Innern
Tel.: 030-18-400-2135
Fax: 030-18-10-400-2135
e-Mail: Michael.Rensmann@bk.bund.de

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 11:03

An: Konow, Christian; Gothe, Stephan; Rensmann, Michael; Nell, Christian; Neueder, Franz; Meyer-Landrut, Nikolaus; Hornung, Ulrike; Baumann, Susanne; Bartodziej, Peter; Felsheim, Georg
Betreff: D-Vertreter bei Auftaktveranstaltung mE dringend geboten
Wichtigkeit: Hoch

FRA und GBR werden auf jeden Fall Vertreter schicken, etliche andere MS vss. auch (vorläufige Liste folgt gleich). Ich halte es unter diesen Umständen ehrlich gesagt für völlig undenkbar, wenn die Bundesregierung niemanden schickte!

Zur Ebene: Ist offenbar noch offen. Habe Antici gebeten, uns zu informieren, sobald Erkenntnisse vorliegen (auch zu KOM, EAD, Präs). GBR und FRA sind angeblich auf Teilnahme auf vergleichbarer Ebene interessiert; vss. gehobene Arbeitsebene (unter Botschafter). Wie sieht BMI das? Ist ja auch ein politisches Zeichen, das man mit der Wahl der Ebene setzt...

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 10:01
An: Baumann, Susanne
Cc: Gothe, Stephan; Rensmann, Michael; Nell, Christian; Neueder, Franz; Meyer-Landrut, Nikolaus; Hornung, Ulrike
Betreff: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.
Wichtigkeit: Hoch

Liebe Frau Baumann,

ja, das könnte man überlegen, der müsste nach aktuellem Erklärungstext, der mit Verschweigefrist 12.00 Uhr im AStV-Verteiler zirkuliert wurde (anbei), allerdings bis heute, 18.00 Uhr benannt werden. Bin mir nicht sicher, ob die Bundesregierung das schafft; federführend wäre BMI. Vielleicht kann 132 ja insofern mal auf BMI zugehen.

Eine Alternative könnte sein, es für die Auftaktveranstaltung dabei zu belassen, dass die Präsidentschaft die MS vertritt. Insofern sollte AA auch noch mal bei den anderen MS erfragen, ob diese teilnehmen wollen. Wir sollten mE weder der einzige MS sein, der neben Präsidentschaft teilnimmt, noch einer der wenigen, die nicht anwesend sind...!

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: Baumann, Susanne
Gesendet: Freitag, 5. Juli 2013 09:46
An: Konow, Christian
Cc: Gothe, Stephan; Rensmann, Michael; Nell, Christian
Betreff: WG: EILT: Proposed compromise text for COREPER agreement on EU-US

Lieber Herr Konow,

Wenn das Treffen am 8.7. jetzt für MS geöffnet werden soll, halten wir Teilnahme eines dt. Vertreters für geboten.

Gruß
Susanne Baumann

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 08:50
An: Meyer-Landrut, Nikolaus; Neueder, Franz; Rensmann, Michael; Hornung, Ulrike; Jung, Alexander; Gothe, Stephan; Nell, Christian
Betreff: WG: EILT: Proposed compromise text for COREPER agreement on EU-US

z.K., es ging gestern abend noch munter hin und her. Neuer Text ist - auf Wunsch UK - wesentlich sensibler hinsichtlich Kompetenzverteilung EU/MS und versucht zudem, Zusammensetzung der Expertengruppen noch nicht zu präjudizieren.

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: .MOBILEU BRUE-POL-EU2-1 Dieter, Robert [mailto:pol-eu2-1-eu@brue.auswaertiges-amt.de]
Gesendet: Freitag, 5. Juli 2013 07:56
An: Konow, Christian; Felsheim, Georg; E-B-2 Schoof, Peter; .BRUEEU L Tempel, Peter; peter.tempel@stv-eu.info; .BRUEEU POL-IN2-2 Eickelpasch, Joerg; E05-RL Grabherr, Stephan
Betreff: EILT: Proposed compromise text for COREPER agreement on EU-US

Hier jetzt der zwischen den genannten Delegation vereinbarte Text für die AStV-Erklärung. Vereibart ist, dass sie jetzt noch einmal unter Verschweigen gestellt wird, damit sie dann zügig das Licht der Welt erblicken kann.

Gruß
RD

-------- Original-Nachricht --------
Betreff: Proposed compromise text for COREPER agreement on EU-US
Datum: Fri, 5 Jul 2013 00:22:52 +0000
Von: Iain.Frew@fco.gov.uk
An: Nerijus.ALEKSIEJUNAS@eu.mfa.lt, antici@eu.mfa.lt
CC: cyril.piquemal@diplomatie.gouv.fr, ulrika.funered@foreign.ministry.se, Robert.Dieter@diplo.de

Dear Nerijus,

With apologies again for the long delay, please see attached proposed changes to the statement you presented today. This follows extensive consultations between the delegations copied here, and I hope can find the approval of COREPER under silence procedure tomorrow.

Best Regards,
Iain

Iain Frew | First Secretary (Antici) | UK Permanent Representation to the EU
Email: iain.frew@fco.gov.uk | Tel: +32 (0) 2287 8283 | FTN: 8316 5283 |
Mob: +32 (0) 473 242 940

****
Visit http://www.gov.uk/fco for British foreign policy news and travel advice and http://blogs.fco.gov.uk to read our blogs.

This email (with any attachments) is intended for the attention of the addressee(s) only. If you are not the intended recipient, please inform the sender straight away before deleting the message without copying, distributing or disclosing its contents to any other person or organisation. Unauthorised use, disclosure, storage or copying is not permitted.
Any views or opinions expressed in this e-mail do not necessarily reflect the FCO's policy.
The FCO keeps and uses information in line with the Data Protection Act 1998. Personal information may be released to other UK government departments and public authorities.
All messages sent and received by members of the Foreign & Commonwealth Office and its missions overseas may be automatically logged, monitored and/or recorded in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
****

MAT A BK-1-4s.pdf, Blatt 23

000010

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Freitag, 5. Juli 2013 11:51
An: ref603
Betreff: WG: Erganzung zur Teilnahme an Auftaktveranstaltung: KOM ist vertreten durch Direktor Priebe und den Direktor Nemitz, Grüße, CK

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 605

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Posanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.Gothe@bk.bund.de
E-Mail: ref605@bk.bund.de

Von: Konow, Christian <Christian.Konow@bk.bund.de>
Gesendet: Freitag, 5. Juli 2013 11:41
An: Konow, Christian <Christian.Konow@bk.bund.de>; Gothe, Stephan <Stephan.Gothe@bk.bund.de>; Rensmann, Michael <Michael.Rensmann@bk.bund.de>; Nell, Christian <Christian.Nell@bk.bund.de>; Neueder, Franz <Franz.Neueder@bk.bund.de>; Meyer-Landrut, Nikolaus <Nikolaus.Meyer-Landrut@bk.bund.de>; Hornung, Ulrike <Ulrike.Hornung@bk.bund.de>; Baumann, Susanne <Susanne.Baumann@bk.bund.de>; Bartodziej, Peter <Peter.Bartodziej@bk.bund.de>; Felsheim, Georg <georg.felsheim@bk.bund.de>
Betreff: Erganzung zur Teilnahme an Auftaktveranstaltung: KOM ist vertreten durch Direktor Priebe und den Direktor Nemitz, Grüße, CK

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Freitag, 5. Juli 2013 13:39
An: AL-6; Schäper, Hans-Jörg
Cc: ref601; ref603
Betreff: WG: EILT: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.

Wichtigkeit: Hoch

Anlagen: 130705 COREPER declaration track changes FINAL.doc



130705 COREPER declaration tra...

Habe auf Bitte BND gerade mit Hr. Selen im BMI telefoniert (dieser hatte BND in der Sache angesprochen, u.a. hinsichtlich Beteiligung BND), mit folgendem Tenor: Wir haben die Überlegungen bislang nur mitgelesen, aber nicht aktiv betrieben, sondern uns auf die nationale Delegation konzentriert; ansonsten Verweis auf FF beim BMI. Hr. Selen erwartet, dass US-Seite ein Abkommen zur künftigen Kooperation vorschlägt; ich regte an, dies im Vorfeld im nationalen Rahmen zu prüfen; BfV ist laut Hr. Selen eher ablehnend. Insgesamt Konsens einer weiteren Abstimmung in der Sache.

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

-----Ursprüngliche Nachricht-----
Von: Polzin, Christina
Gesendet: Freitag, 5. Juli 2013 11:27
An: Schäper, Hans-Jörg; Heiß, Günter
Cc: ref603; ref601
Betreff: WG: EILT: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.
Wichtigkeit: Hoch

Lieber Herr Schäper, lieber Herr Heiß,

hier müssten wir uns schnell entscheiden, ob wir uns bei der Auftaktveranstaltung mit einem Vertreter (Abt 6 oder BND) teilnehmen möchten, oder ob wir das Feld dem BMI überlassen wollen.

In jedem Fall müssten wir uns mit BMI (Herrn Peters oder Referat ÖS I 3) absprechen. Dem Vernehmen nach möchte BMI nicht so gerne an der Veranstaltung teilnehmen, wenn nicht auch jemand für den Bereich BND /BK-Amt teilnimmt.

Lieber Herr Schäper, vielleicht bietet sich dazu ein Telefonat zwischen Ihnen und Herrn Peters an zur Abstimmung.

Das Ganze müsste heute geklärt werden, da Frist zur Meldung der Teilnehmer heute 18 h ist.

Gruß,

Christina Polzin
Bundeskanzleramt
Referatsleiterin 601
Willy-Brandt-Straße 1
10557 Berlin
Tel: +49 (0) 30 18 400 -2612
Fax.:+49-(0) 30 18 10 400-2612
E-Mail: christina.polzin@bk.bund.de

-----Ursprüngliche Nachricht-----
Von: Rensmann, Michael
Gesendet: Freitag, 5. Juli 2013 11:06
An: ref601; ref603
Cc: Bartodziej, Peter
Betreff: EILT: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.
Wichtigkeit: Hoch

Liebe Kolleginnen und Kollegen,

ich würde eine Teilnahme durch DEU (im Rahmen des terminlich/logistisch Möglichen) hier grundsätzlich ebenfalls befürworten.

Vor dem Hintergrund der klaren ND-Ausrichtung, auf die ja nicht zuletzt im Zusammenhang mit der Beteiligung der KOM mehrfach verwiesen wird und der zu erwartenden Inhalte wäre aber die Frage der Teilnahme m.E. durch Abt. 6 gemeinsam mit BMI zu entscheiden. Insofern wäre ich für entsprechende Übernahme dankbar.

Mit freundlichen Grüßen
Michael Rensmann

Dr. Michael Rensmann
Bundeskanzleramt
Referat 132
Angelegenheiten des Bundesministeriums des Innern
Tel.: 030-18-400-2135
Fax: 030-18-10-400-2135
e-Mail: Michael.Rensmann@bk.bund.de

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 11:03
An: Konow, Christian; Gothe, Stephan; Rensmann, Michael; Nell, Christian; Neueder, Franz; Meyer-Landrut, Nikolaus; Hornung, Ulrike; Baumann, Susanne; Bartodziej, Peter; Felsheim, Georg
Betreff: D-Vertreter bei Auftaktveranstaltung mE dringend geboten
Wichtigkeit: Hoch

FRA und GBR werden auf jeden Fall Vertreter schicken, etliche andere MS vss. auch (vorläufige Liste folgt gleich). Ich halte es unter diesen Umständen ehrlich gesagt für völlig undenkbar, wenn die Bundesregierung niemanden schickte!

Zur Ebene: Ist offenbar noch offen. Habe Antici gebeten, uns zu informieren, sobald Erkenntnisse vorliegen (auch zu KOM, EAD, Präs). GBR und FRA sind angeblich auf Teilnahme auf vergleichbarer Ebene interessiert; vss. gehobene Arbeitsebene (unter Botschafter). Wie sieht BMI das? Ist ja auch ein politisches Zeichen, das man mit der Wahl der Ebene setzt...

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 10:01
An: Baumann, Susanne
Cc: Gothe, Stephan; Rensmann, Michael; Nell, Christian; Neueder, Franz; Meyer-Landrut, Nikolaus; Hornung, Ulrike

Betreff: D-Vertreter für Auftaktveranstaltung müsste bis heute, 18.00 Uhr benannt werden.
Wichtigkeit: Hoch

Liebe Frau Baumann,

ja, das könnte man überlegen, der müsste nach aktuellem Erklärungstext, der mit Verschweigefrist 12.00 Uhr im AStV-Verteiler zirkuliert wurde (anbei), allerdings bis heute, 18.00 Uhr benannt werden. Bin mir nicht sicher, ob die Bundesregierung das schafft; federführend wäre BMI. Vielleicht kann 132 ja insofern mal auf BMI zugehen.

Eine Alternative könnte sein, es für die Auftaktveranstaltung dabei zu belassen, dass die Präsidentschaft die MS vertritt. Insofern sollte AA auch noch mal bei den anderen MS erfragen, ob diese teilnehmen wollen. Wir sollten mE weder der einzige MS sein, der neben Präsidentschaft teilnimmt, noch einer der wenigen, die nicht anwesend sind...!

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: Baumann, Susanne
Gesendet: Freitag, 5. Juli 2013 09:46
An: Konow, Christian
Cc: Gothe, Stephan; Rensmann, Michael; Nell, Christian
Betreff: WG: EILT: Proposed compromise text for COREPER agreement on EU-US

Lieber Herr Konow,

Wenn das Treffen am 8.7. jetzt für MS geöffnet werden soll, halten wir Teilnahme eines dt. Vertreters für geboten.

Gruß
Susanne Baumann

-----Ursprüngliche Nachricht-----
Von: Konow, Christian
Gesendet: Freitag, 5. Juli 2013 08:50
An: Meyer-Landrut, Nikolaus; Neueder, Franz; Rensmann, Michael; Hornung, Ulrike; Jung, Alexander; Gothe, Stephan; Nell, Christian
Betreff: WG: EILT: Proposed compromise text for COREPER agreement on EU-US

z.K., es ging gestern abend noch munter hin und her. Neuer Text ist - auf Wunsch UK - wesentlich sensibler hinsichtlich Kompetenzverteilung EU/MS und versucht zudem, Zusammensetzung der Expertengruppen noch nicht zu präjudizieren.

Grüße
CK

-----Ursprüngliche Nachricht-----
Von: .MOBILEU BRUE-POL-EU2-1 Dieter, Robert [mailto:pol-eu2-1-eu@brue.auswaertiges-amt.de]
Gesendet: Freitag, 5. Juli 2013 07:56
An: Konow, Christian; Felsheim, Georg; E-B-2 Schoof, Peter; .BRUEEU L Tempel, Peter; peter.tempel@stv-eu.info; .BRUEEU POL-IN2-2 Eickelpasch, Joerg; E05-RL Grabherr, Stephan
Betreff: EILT: Proposed compromise text for COREPER agreement on EU-US

Hier jetzt der zwischen den genannten Delegation vereinbarte Text für die AStV-Erklärung. Vereibart ist, dass sie jetzt noch einmal unter Verschweigen gestellt wird, damit sie dann zügig das Licht der Welt erblicken kann.

Gruß
RD

-------- Original-Nachricht --------
Betreff: Proposed compromise text for COREPER agreement on EU-US
Datum: Fri, 5 Jul 2013 00:22:52 +0000

Von: Iain.Frew@fco.gov.uk
An: Nerijus.ALEKSIEJUNAS@eu.mfa.lt, antici@eu.mfa.lt
CC: cyril.piquemal@diplomatie.gouv.fr,
ulrika.funered@foreign.ministry.se, Robert.Dieter@diplo.de

Dear Nerijus,

With apologies again for the long delay, please see attached proposed changes to the statement you presented today. This follows extensive consultations between the delegations copied here, and I hope can find the approval of COREPER under silence procedure tomorrow.

Best Regards,
Iain

Iain Frew | First Secretary (Antici) | UK Permanent Representation to the EU
Email: iain.frew@fco.gov.uk | Tel: +32 (0) 2287 8283 | FTN: 8316 5283 |
Mob: +32 (0) 473 242 940

****
Visit http://www.gov.uk/fco for British foreign policy news and travel advice and http://blogs.fco.gov.uk to read our blogs.

This email (with any attachments) is intended for the attention of the addressee(s) only. If you are not the intended recipient, please inform the sender straight away before deleting the message without copying, distributing or disclosing its contents to any other person or organisation. Unauthorised use, disclosure, storage or copying is not permitted.
Any views or opinions expressed in this e-mail do not necessarily reflect the FCO's policy.
The FCO keeps and uses information in line with the Data Protection Act 1998. Personal information may be released to other UK government departments and public authorities.
All messages sent and received by members of the Foreign & Commonwealth Office and its missions overseas may be automatically logged, monitored and/or recorded in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
****

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Freitag, 5. Juli 2013 18:21
An: Lindemann, Karina; Heiß, Günter; AL-6
Cc: Schäper, Hans-Jörg; ref603
Betreff: WG: Bitte um Freigabe

Anlagen: 130708_Sprachregelung_BND_AND (4).doc

Liebe Frau Lindemann,
bitte um Entschuldigung, ich meinte den 4. Anstrich. Daher anbei ein Vorschlag:

130708_Sprachreg
elung_BND_AND ...

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Gothe, Stephan
Gesendet: Freitag, 5. Juli 2013 18:15
An: Lindemann, Karina; 'Günter Heiß'; Heiß, Günter
Betreff: AW: Bitte um Freigabe

Liebe Frau Lindemann,
vielen Dank. Wir regen an, den dritten Punkt ("Was die Presseveröffentlichungen angeht...") zu streichen bzw. als reaktiv von den anderen drei Punkten abzusetzen. Der Punkt ist zwar inhaltlich richtig, hat aber vermutlich mit dem angekündigten Spiegel-Artikel nichts zu tun. Nach dem, was wir jetzt wissen, will der Spiegel die Kooperation BND-NSA an sich thematisieren, mglw. auch vor dem Hintergrund von Prism, aber losgelöst davon. Insofern kann dieser Punkt ggf. reaktiv eingesetzt werden, sollte Prism direkt zur Sprache kommen.

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Lindemann, Karina
Gesendet: Freitag, 5. Juli 2013 18:04
An: 'Günter Heiß'; Heiß, Günter

Cc: Gothe, Stephan
Betreff: Bitte um Freigabe

Lieber Herr Heiß, lieber Herr Gothe,

ich bitte um fachliche Durchsicht folgender Sprachregelung antizipierend für das Wochenende und den Spiegel.

Für Anregungen und Vorschläge bin ich dankbar.

Mit besten Grüßen
Karina Lindemann

< Datei: 130708_Sprachregelung_BND_AND (4).doc >>

SPRECHZETTEL REAKTIV

Aktuelle Presseberichterstattung zur Kooperation des BND mit Partnern

08. Juli 2013

Referat 603, Stephan Gothe, Hausruf 2630

abgestimmt mit: BKAmt/ AL 6

Anlass:

Aktuell berichten berichtet der Spiegel vor dem Hintergrund von „Prism“ etc. über die Kooperation des BND mit Partnerdiensten.

- Für die Bundesregierung ist der Schutz ihrer Bürger oberstes Gebot. Das ist gleichsam der Schutz vor terroristischen Bedrohungen wie auch der Schutz der Privatsphäre. Bei allem, was Regierungen und Nachrichtendienste tun, muss die Verhältnismäßigkeit gewahrt werden hat nach Recht und Gesetz zu erfolgen.

- Der BND sammelt auf der Grundlage des BND-Gesetzes die erforderlichen Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Der BND und seine Arbeit unterliegen dabei der strengen parlamentarischen Kontrolle. Im Rahmen seines gesetzlichen Auftrags arbeitet der BND auch mit Partnerdiensten zusammen.

- Die Bundesregierung unterrichtet zu geheimhaltungsbedürftigen Angelegenheiten der Nachrichtendienste des Bundes grundsätzlich nur die dafür vorgesehenen besonderen parlamentarischen Gremien des Deutschen Bundestages. All das aber, was wir öffentlich bekannt machen können, werden wir auch öffentlich machen.

- [Reaktiv, sollte nach Prism gefragt werden]: Was die Presseveröffentlichungen angeht, befindet sich die Bundesregierung in der Phase der Sachaufklärung. Diese dauert an. Wie Sie wissen haben wir mit den USA verabredet, dass in den kommenden Tagen eine ressortübergreifende Delegation nach Washington reist, um dort mit den US-amerikanischen Kollegen die Sachverhaltsaufklärung voranzutreiben.

MAT A BK-1-4s.pdf, Blatt 31

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Mittwoch, 10. Juli 2013 09:15
An: AL-6; ref601; ref603
Betreff: WG: Eilt sehr: 2460. AStV (Teil 2) am 04.07.2013 - TOP EU-US-High level expert group on security and data protection (Prism)
Wichtigkeit: Hoch
Anlagen: 130907__Weisung_HLEG_Prism_AA_BMJ.doc; 130907__Weisung_HLEG_Prism.doc

H.e. können wir verschweigen.

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Rensmann, Michael
Gesendet: Mittwoch, 10. Juli 2013 09:02
An: ref501; ref601; ref603
Cc: Bartodziej, Peter; Konow, Christian
Betreff: WG: Eilt sehr: 2460. AStV (Teil 2) am 04.07.2013 - TOP EU-US-High level expert group on security and data protection (Prism)
Wichtigkeit: Hoch

Liebe Kolleginnen und Kollegen,

anliegenden überarbeiteten Weisungsentwurf mit Änderungen BMI, BMJ und AA z.K. (mit Verschweigefrist bis 9.25 Uhr).

Mit freundlichen Grüßen
Michael Rensmann

Von: Patrick.Spitzer@bmi.bund.de [mailto:Patrick.Spitzer@bmi.bund.de]
Gesendet: Mittwoch, 10. Juli 2013 08:58
An: bader-jo@bmj.bund.de; Rensmann, Michael; e05-2@auswaertiges-amt.de; Kirsten.Scholl@bmwi.bund.de; henrichs-ch@bmj.bund.de
Cc: Reinhard.Peters@bmi.bund.de; t.pohl@diplo.de; GII3@bmi.bund.de; Alice.PinargoteVera@bmi.bund.de; Matthias.Taube@bmi.bund.de; Johann.Jergl@bmi.bund.de; Ralf.Lesser@bmi.bund.de; PGDS@bmi.bund.de; Daniel.Meltzian@bmi.bund.de; Anna.Deutelmoser@bmi.bund.de; IT1@bmi.bund.de; Andre.Riemer@bmi.bund.de; OESI3AG@bmi.bund.de
Betreff: WG: Eilt sehr: 2460. AStV (Teil 2) am 04.07.2013 - TOP EU-US-High level expert group on security and data protection (Prism)
Wichtigkeit: Hoch

MAT A BK-1-4s.pdf, Blatt 32

<<130907__Weisung_HLEG_Prism_AA_BMJ.doc>> Liebe Kolleginnen und Kollegen,

anbei übermittele ich eine konsolidierte und – im Lichte der gestern Abend eingetroffenen zusätzlichen Dokumente - zum Teil fortgeschriebene Fassung der AStV-Weisung mit der Bitte, diese kurzfristig zu überprüfen und Änderungswünsche mitzuteilen. Inhaltlich haben sich m.E. keine grundsätzlichen Änderungen ergeben. Bitte teilen Sie mir Änderungen bis spätestens **9.25 Uhr** mit, damit eine Übermittlung des Dokuments bis 10.00 Uhr noch gewährleistet werden kann.

Freundliche Grüße und herzlichen Dank

Patrick Spitzer

im Auftrag

Dr. Patrick Spitzer

Bundesministerium des Innern

Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,

BKA-Gesetz, Datenschutz im Sicherheitsbereich)

Alt-Moabit 101D, 10559 Berlin

Telefon: +49 (0)30 18681-1390

E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: Spitzer, Patrick, Dr.
Gesendet: Dienstag, 9. Juli 2013 12:04
An: BMJ Henrichs, Christoph; BMJ Bader, Jochen; BK Rensmann, Michael; AA Oelfke, Christian; BMWI Scholl, Kirsten
Cc: OESI3AG_; 'thomas.pohl@diplo.de'; GII3_; Pinargote Vera, Alice; Taube, Matthias; Jergl, Johann; Lesser, Ralf; PGDS_; Meltzian, Daniel, Dr.; Deutelmoser, Anna, Dr.; IT1_; Riemer, André
Betreff: Eilt sehr: 2460. AStV (Teil 2) am 04.07.2013 - TOP EU-US-High level expert group on security and data protection (Prism)
Wichtigkeit: Hoch

<<130907__Weisung_HLEG_Prism.doc>>

Liebe Kolleginnen und Kollegen,

anbei übersende ich den angekündigten Entwurf einer Weisung für die morgige Sitzung des AStV zum TOP: „EU-US-High level expert group on security and data protection" mit der Bitte um Prüfung und Mitzeichnung bis heute **(9. Juli) 14. 00 Uhr**. Ich bitte um Verständnis für die sehr kurze Frist.

MAT A BK-1-4s.pdf, Blatt 33

000020

Herzlichen Dank und Freundliche Grüße

im Auftrag

Dr. Patrick Spitzer

Bundesministerium des Innern

Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,

BKA-Gesetz, Datenschutz im Sicherheitsbereich)

Alt-Moabit 101D, 10559 Berlin

Telefon: +49 (0)30 18681-1390

E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Auswärtiges Amt
EU-Koordinierungsgruppe (E-KR)

Erstellt von Referat: ÖS I 3
Beteiligte Referate im Haus und in anderen Ressorts: BK, AA, BMJ, BMWi

2460. AStV 2 am 10. Juli 2013

II-Punkt

TOP **EU-US High level expert group on security and data protection**

Dok. ---

Weisung

1. Ziel des Vorsitzes

- **Bericht** über das **erste EU–US Treffen** in Washington **am 8. Juli** unter Teilnahme von KOM, EAD, Vorsitz und einer Vielzahl von MS sowie je einem Vertreter des Justizministeriums (DoJ), Außenministeriums (DoS) sowie des Office of the Director of National Intelligence (ODNI).
- Fortsetzung der Diskussion vom 4. Juli 2013 zu **Mandat** und **Zusammensetzung** der EU-US-High level expert group on security and data protection auf der Grundlage der von LTU PRÄS vorgestellten Optionen, mti besodnerem Fokus auf die zusätzlich übersandten Fragen (Dok. 12118/13).

Formatiert: Schriftart: (Standard) Arial, Nicht Fett, (Asiatisch) Chinesisch (VR China)

Gelöscht: .

2. Deutsches Verhandlungsziel/ Weisungstenor

- **Kenntnisnahme des Berichts** der KOM und des Vors. von den Verhandlungen. Betonung, dass weiterhin auf schnelle Sachaufklärung gedrängt werden soll und eine rein formale Diskussion über die Art und Weise der Gesprächsführung nicht ausreicht.
- **Klarstellung**, dass DEU - weiterhin - die seitens der LTU PRÄS unter Ziffer 7 Buchstabe C skizzierte Differenzierung zwischen datenschutzrechtlichen und die die Tätigkeit der Nachrichtendienste betreffenden Fragestellungen für erforderlich hält.
- Bei der **Zusammensetzung** der (verschiedenen) Arbeitsgruppen (datenschutzrechtliche/ grundrechtliche Fragestellungen einerseits; nachrichten-

dienstliche Themen andererseits), ist zu berücksichtigen, dass die EU keine Kompetenz für nachrichtendienstliche Fragestellungen (auch nicht für datenschutzrechtliche Fragen im Zusammenhang mit Nachrichtendiensten) hat.

- Eine Teilnahme von KOM/EAD kommt aus Sicht von DEU an einer datenschutzrechtlichen Gruppe in Frage (wobei hier der „Teilnahmestatus" der KOM z. Zt. noch nicht abschließend geklärt werden muss). Eine solche Teilnahme wäre indes kompetenzrechtlich nicht geboten und würde deshalb ohne Anerkennung einer solchen Kompetenz ausschließlich mit Rücksicht auf die gegebene unmittelbare Betroffenheit auch von EU-Institutionen erfolgen.
- Unabhängig von einer Klärung der noch ausstehenden Fragen (u.a. Zusammensetzung/ Mandat der Arbeitsgruppe(n)): Beteiligung von DEU an den Arbeitsgruppen sollte vorgesehen werden.
- Mit Blick auf die vom Vorsitz am 9. Juli übermittelten Fragen sollte zumindest festgehalten werden, dass im Vordergrund eine Aufklärung durch USA stehen muss, auch, wenn man sich dem Wunsch zur gegenseitigen Unterrichtung nicht ganz verschließen kann.
- Sollte – im Anschluss an das Treffen vom 08. Juli in Washington - die Bildung nur einer zentralen Arbeitsgruppe zur Aufklärung der Sachverhalte diskutiert werden, so gilt:

  Eine zentrale Arbeitsgruppe ist aus o.g. kompetenzrechtlichen Gründen abzulehnen, bzw. kann nur ohne KOM/EAD (stattdessen: bi-/multilateral MS-US) ihre Arbeit aufnehmen.

3. Sprechpunkte

- **DEU will sich an einer HLEG beteiligen.**
- **Schwerpunkt der Arbeit der HLEG muss die zeitnahe Sachverhaltsaufklärung sein, mit dem Ziel baldmöglichst öffentlich weitergabefähige Inhalte öffentlich zu kommunizieren.** DEU plädiert – weiterhin - dafür, entsprechend der von LTU PRÄS unter Ziffer 7 Buchstabe C aufgezeigten Handlungsoption zwischen die **Nachrichtendienste betreffenden datenschutzrechtlichen** Fragen und Fragen, die die **Tätigkeit der Nachrichtendienste** betreffen, klar zu differenzieren. Hierfür spricht, dass – abgesehen von kompetenzrechtlichen Erwägungen - hierfür unterschiedliche Personen für die Diskussion rechtlicher und technischer Fragen geeignet sind.
- Soweit die USA von Ihrem Vorschlag der Behandlung des Themas in zwei getrennten Gruppenabrücken sollten, so würde DEU die Zusammenführung in einer Gruppe nicht befürworten.
- Aus Sicht von DEU wäre eine **Teilnahme von KOM/EAD** an der in Ziffer 7 Buchst. C skizzierten nachrichtendienstlichen Gruppe kompetenzrechtlich nicht möglich.
- Eine Aufklärung die – wie es dem Wunsch der USA entspricht – im „Gegenseitigkeitsverhältnis steht" - wird man sich nicht verschließen können. Im Vordergrund muss aber die Aufklärung durch die USA stehen.
- Demgegenüber sollte KOM an der datenschutzrechtlichen Gruppe teilnehmen.
- Für die weitere Diskussion ist schließlich noch erforderlich, dass der Untersuchungsgegenstand der beiden Gruppen näher festgelegt wird.

Gelöscht: allenfalls

Gelöscht: ¶

Gelöscht: <#>der wichtigste Schwerpunkt der Bemühungen sein muss, zeitnah Sachverhalte zu klären und insb. öffentlich weitergabefähige Inhalte rasch zu kommunizieren;¶ <#>hierfür unterschiedliche Personen für die Diskussion rechtlicher und technischer Fragen geeignet sind.¶

Gelöscht: ;

Gelöscht: sie ist seitens der USA zudem nicht erwünscht (Schreiben Holder vom 1. Juli 2013). Auch für eine Teilnahme an der datenschutzrechtlichen Gruppe fehlt es KOM de iure an einer Kompetenz. Da aber der Verdacht im Raum steht, dass auch EU-Institutionen von den nachrichtendienstlichen Tätigkeiten der USA betroffen sind, erscheint eine Teilnahme der KOM an der datenschutzrechtlichen Gruppe aus Gründen politischer Rücksichtnahme zumindest möglich (über Leitung dieser Gruppe muss noch diskutiert werden; maßgeblich sollte hier auch besondere sachliche Expertise sein).

Gelöscht: <#>Die Ergebnisse des Treffens vom 8. Juli (hier: Bericht des BMI-Verbindungsbeamten in Washington vom 9. Juli) können dahingehend gedeutet werden, dass USA vom ursprünglichen Vorschlag (siehe Schreiben von US-Justizminister Holder vom 1. Juli), die Gespräche thematisch in zwei Gruppen durchzuführen, abzurücken scheint. Es sollte ggü USA deutlich gemacht werden, dass das dem ursprünglichen Vorschlag von US-Justizminister Holder vom 1. Juli 2013 widerspricht und darüber hinaus aus kompetenzrechtlichen Gründen problematisch ist.¶

Gelöscht: ¶

4. Hintergrund/ Sachstand

Hintergrund zur „High level expert group“

Mit Schreiben vom 19. Juni 2013 haben Frau Kommissarin Reding und Frau Kommissarin Malmström die von US-Justizminister Holder vorgeschlagene Idee, eine eine EU/US High level expert group zu bilden, aufgenommen. Mit Schreiben vom 1. Juli 2013 hat Herr US-Justizminister Holder eine Aufteilung der zu behandelnden Themen nach Zuständigkeiten vorgeschlagen:

1. Dialog über die staatliche Kontrolle der Tätigkeit der Nachrichtendienste unter Beteiligung der KOM und MS.
2. Austausch über die (Art und Weise) der Erhebung nachrichtendienstlicher Informationen (discussion of intelligence collection) zwischen den Mitgliedstaaten und der US-Seite (keine Beteiligung KOM) auf nachrichtendienstlicher Fachebene („senior intelligence agency officials).

Im AStV am 4. Juli 2013 konzentrierte sich die Diskussion mit Blick auf den für den 8. Juli vorgesehenen Beginn der TTIP-Verhandlungen auf die Frage, ob sich eine EU-Delegation (KOM, EAD und Vors.) bereits am 8. Juli, in einem Auftaktgespräch mit USA in Washington treffen solle, um Fakten zum weiteren Vorgehen mit USA abzustimmen. Mit Ausnahme von GBR und SWE unterstützten alle wortnehmenden MS (FRA, DEU, DNK, NLD, BEL, AUT, ITA, GRC, LVA, PRT, FIN, HUN und BGR) diesen Ansatz, sowie KOM und EAD.

Am Montag, den 08. Juli begann die Tätigkeit der EU-US-Expertengruppe unter Beteiligung der KOM, des Europäischen Auswärtigen Dienstes, der LTU Präsidentschaft unter Beteiligung einiger MS (darunter DEU, vertreten durch den Verbindungsbeamten des BMI beim DHS, Herrn Dr. Vogel).Dabei ging es ausweislich des Berichts des Verbindungsbeamten des BMI beim DHS vom 9. Juli insbesondere um folgende Punkte :

- EU KOM sieht eine Vertrauenskrise in der EU ggü. den USA und befürchtet, dass deshalb die enge und vertrauensvolle Sicherheitskooperation mit den USA (z. B. PNR, TFTP, SWIFT etc.) Schaden nehmen könnte.
- Deshalb sei es wichtig, dass die USA die EU über ihr Handeln aufklären.
- USA sind zu einem umfassenden Dialog bereit, möchten zur Aufklärung beitragen und Vertrauen aufbauen.
- Dies schließe konsequenterweise auch Gespräche darüber ein, wie Nachrichtendienste (ND) der EU MS ggü. US-Bürgern und EU-Bürgern agieren.
- Es sei nicht einzusehen, warum nur die USA sich zu ND-Praktiken erklären sollen, wenn EU MS ähnlich agieren (ggü. eigenen und US-Bürgern).
- Wenn die EU KOM kein Mandat habe, derartige Themen zu diskutieren, stelle sich die Frage nach dem richtigen Gesprächsrahmen. ND-Themen lassen sich nicht aus dem Gesamtkomplex zugunsten einer reinen Diskussion auf Grundrechtsebene isolieren.

- Zunächst müsse nach einem angemessenen Format gesucht werden, bevor über Inhalte gesprochen werden kann. Das nächste Treffen in Brüssel könne hierzu dienen.
- Die EU-Delegation wird an AStV berichten, dass auf beiden Seiten Gesprächsbedarf gesehen wird, das Treffen ein erster Schritt zur Klärung gewesen sei und Vertreter der USA und der EU in Kürze zu erneuten Gesprächen zusammen kommen werden. Ggf. wird es eine entsprechende Presseerklärung seitens der EU geben.

USA hat in einer Demarche v. 9. Juli 2013 zum Ausdruck gebracht, dass sie für einen Austausch über die nachrichtendienstliche Details in erster Linie die MS für die richtigen Ansprechpartner hält (im Rahmen eines „structured set of bilateral (or, where appropriate, multilateral) dialogues)". Eine EU-Beteiligung sollte sich nach Ansicht USA auf die Planung des organisatorischen Rahmens beschränken („schedule und structure)".

Vorsitz hat im Nachgang zum Treffen am 8. Juli in Washington drei Fragen zur Diskussion gestellt:

- 1. How should the Union react to the US message that it is not willing to engage in a one-sided dialogue; and that not only US, but also Member State oversight mechanisms should be looked at in the context of the EU-US 'process'?
- 2. In case there would be a willingness on behalf of Member State to extend an EU-US process to Member State surveillance programmes and the relevant oversight mechanisms, in which format should these be discussed?
- 3. How do Member States view the link between the first and second track proposed by the US. Should both tracks be discussed in the same or a different format?

Formatiert: Einzug: Links: 1,26 cm, Keine Aufzählungen oder Nummerierungen

Formatiert: Einzug: Links: 0 cm, Abstand Vor: 0 pt

Formatiert: Schriftart: (Standard) Arial, (Asiatisch) Chinesisch (VR China), (Andere) Englisch (USA)

Formatiert: Standard (Web), Block, Einzug: Links: 0,63 cm, Hängend: 0,63 cm, Abstand Vor: 6 pt, Aufgezählt + Ebene: 1 + Ausgerichtet an: 0,63 cm + Tabstopp nach: 0 cm + Einzug bei: 1,27 cm, Abstand zwischen asiatischem und westlichem Text anpassen, Abstand zwischen asiatischem Text und Zahlen anpassen

Formatiert: Englisch (USA)

Formatiert: Schriftart: (Standard) Arial, (Asiatisch) Chinesisch (VR China), (Andere) Englisch (USA)

Formatiert: Schriftart: (Standard) Arial, (Asiatisch) Chinesisch (VR China), (Andere) Englisch (USA)

Formatiert: Englisch (USA)

Formatiert: Schriftart: (Standard) Arial, (Asiatisch) Chinesisch (VR China), (Andere) Englisch (USA)

Formatiert: Schriftart: (Standard) Arial, (Asiatisch) Chinesisch (VR China), (Andere) Englisch (USA)

Formatiert: Einzug: Links: 0,63 cm, Hängend: 0,63 cm, Aufgezählt + Ebene: 1 + Ausgerichtet an: 0,63 cm + Tabstopp nach: 0 cm + Einzug bei: 1,27 cm

Formatiert: Englisch (USA)

Formatiert: Schriftart: (Standard) Arial, (Asiatisch) Chinesisch (VR China), (Andere) Englisch (USA)

Formatiert: Englisch (USA)

Klostermeyer, Karin

Von: Gothe, Stephan
Gesendet: Freitag, 12. Juli 2013 15:06
An: 'wolfgang.kurth@bmi.bund.de'
Cc: 'KS-CA-1 Knodt, Joachim Peter'; IT3@bmi.bund.de; ref132; ref603
Betreff: WG: MZ AA: Sitzung FoP am 15.7.2013

Anlagen: 130712_5 Sitzung Cyber FoP_Weisung.docx

130712_5 Sitzung Cyber FoP_We...

Lieber Herr Kurth,
anbei eine Änderung unsererseits zu einer von AA eingefügten Ergänzung (S. 3; die AA-Ergänzung war nicht zutreffend). Das AA habe ich bereits informiert und gebeten, eine entsprechend geänderte Version zu zirkulieren. Bitte entschuldigen Sie die verspätete Rückmeldung.

Mit freundlichen Grüßen
Im Auftrag

Stephan Gothe
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 18400-2630
E-Mail: stephan.gothe@bk.bund.de
E-Mail: ref603@bk.bund.de

-----Ursprüngliche Nachricht-----
Von: Rensmann, Michael
Gesendet: Freitag, 12. Juli 2013 14:11
An: ref131; ref603; ref501; ref114
Betreff: WG: MZ AA: Sitzung FoP am 15.7.2013

Liebe Kolleginnen und Kollegen,

die Anmerkungen des AA auch für Sie z.K.

Mit freundlichen Grüßen
Michael Rensmann

-----Ursprüngliche Nachricht-----
Von: KS-CA-1 Knodt, Joachim Peter [mailto:ks-ca-1@auswaertiges-amt.de]
Gesendet: Freitag, 12. Juli 2013 14:08
An: Wolfgang.Kurth@bmi.bund.de
Cc: IT3@bmi.bund.de; Rainer.Mantz@bmi.bund.de; Johannes.Dimroth@bmi.bund.de; Michael.Pilgermann@bmi.bund.de; ref132; Werner.Beulertz@BMFSFJ.BUND.DE; BMVgPolII3@BMVg.BUND.DE; BMVgPolII@BMVg.BUND.DE; K13@bkm.bmi.bund.de; Schmidt, Matthias; Marko.Borchardt@BMFSFJ.BUND.DE; ANGELIKA.HAAS@BMELV.BUND.DE; Marta.Kujawa@bmwi.bund.de; Joerg.Hadameck@bmz.bund.de; KS-CA-L Fleischer, Martin; SaschaZarthe@BMVg.BUND.DE; StefanSohm@BMVg.BUND.DE; MatthiasMielimonka@BMVg.BUND.DE; Maria.Lueken@bkm.bmi.bund.de; schmierer-ev@bmj.bund.de; 122@BMELV.BUND.DE; 321@BMELV.BUND.DE; Richard.Schulz@bmf.bund.de; Basse, Sebastian; entelmann-la@bmj.bund.de; zc1@bmf.bund.de; EA4@bmf.bund.de
Betreff: MZ AA: Sitzung FoP am 15.7.2013

Lieber Herr Kurth,

anbei mit besten Grüßen von Martin Fleischer die MZ des AA, s. inkl. Anmerkungen.

Viele Grüße,

i.A.
Joachim Knodt

—

Joachim P. Knodt
Koordinierungsstab für Cyber-Außenpolitik / International Cyber Policy Coordination Staff Auswärtiges Amt / Federal Foreign Office Werderscher Markt 1 D - 10117 Berlin
phone: +49 30 5000-2657 (direct), +49 30 5000-1901 (secretariat), +49 1520 4781467 (mobile)
e-mail: KS-CA-1@diplo.de

-----Ursprüngliche Nachricht-----
Von: Wolfgang.Kurth@bmi.bund.de [mailto:Wolfgang.Kurth@bmi.bund.de]
Gesendet: Donnerstag, 11. Juli 2013 14:14
An: ref132@bk.bund.de; Werner.Beulertz@BMFSFJ.BUND.DE; BMVgPolII3@BMVg.BUND.DE; BMVgPolII@BMVg.BUND.DE; K13@bkm.bmi.bund.de; Matthias.Schmidt@bk.bund.de; Marko.Borchardt@BMFSFJ.BUND.DE; ANGELIKA.HAAS@BMELV.BUND.DE; Marta.Kujawa@bmwi.bund.de; Joerg.Hadameck@bmz.bund.de; KS-CA-L Fleischer, Martin; KS-CA-1 Knodt, Joachim Peter; SaschaZarthe@BMVg.BUND.DE; StefanSohm@BMVg.BUND.DE; MatthiasMielimonka@BMVg.BUND.DE; Maria.Lueken@bkm.bmi.bund.de; schmierer-ev@bmj.bund.de; 122@BMELV.BUND.DE; 321@BMELV.BUND.DE; Richard.Schulz@bmf.bund.de; Sebastian.Basse@bk.bund.de; entelmann-la@bmj.bund.de; zc1@bmf.bund.de; EA4@bmf.bund.de
Cc: VI4@bmi.bund.de; OESI3AG@bmi.bund.de; GII2@bmi.bund.de; OESIII3@bmi.bund.de; IT1@bmi.bund.de; IT5@bmi.bund.de; IT3@bmi.bund.de; Rainer.Mantz@bmi.bund.de; KM4@bmi.bund.de; RegIT3@bmi.bund.de; Johannes.Dimroth@bmi.bund.de; Michael.Pilgermann@bmi.bund.de; Rotraud.Gitter@bmi.bund.de
Betreff: Sitzung FoP am 15.7.2013

BMI IT 3
Berlin, 11.7.2013

IT3 623 480/0#39

Sehr geehrte Damen und Herren,

anliegend übersende ich Ihnen die Weisung zu der Sitzung der FoP Cyber am 15. Juli 2013 mit der Bitte um Zustimmung.

Sollten Sie Änderungen wünschen, bitte ich, diese bis Freitag, 12.Juli 2013, 14 Uhr, an das Referatspostfach IT3 (It3@bmi.bund.de) zu übermitteln, anderenfalls gehe ich von Ihrer Zustimmung aus.

<<130711_Verhandlungslinie.docx>>

Die beigefügten Dokumente wurden als Unterlagen zur Sitzung übermittelt.

Tagesordnung
<<CM03581.EN13.pdf>>

TOP 3

<<ds01563.en13.doc>>
TOP 4

<<ds01564.en13.doc>>

TOP 5

<<Presentation NCSS FoP ENISA.PDF>>

Mit freundlichen Grüßen

Wolfgang Kurth
Bundesministerium des Innern
Referat IT 3
Alt-Moabit 101 D
10559 Berlin
SMTP: Wolfgang.Kurth@bmi.bund.de
Tel.: 030/18-681-1506
PCFax 030/18-681-51506

Erstellt von: BMI/ IT3, Dr. Dimroth (-1993); AA/ KS-CA, J. Knodt (-2657)

Abgestimmt mit: BMWi, BMJ, BMF, BMELV, BMVg, BMFSFJ, BMZ, BKAmt, BKM

VS-Nur für den Dienstgebrauch

5. Sitzung der "Friends of the Presidency on Cyber Issues" (FoP Cyber)

am 15. Juli 2013

TOP 1: Adoption of the agenda

Ziel: Kenntnisnahme

TOP 2: Information from the Presidency, Commission & EEAS

- Informal Council JAI in Vilnius (18.-19.7.2013),
- Cyberspace conference (Seoul 17./ 18.10.2013),
- the state of play of the EU-US Working Group on Cyber Security an Cybercrime and the Global Alliance against Child Sexual Abuse Online
- *ggf. ist mit der Erörterung zu Auswirkungen von PRISM etc. zu rechnen*

Gelöscht: i
Gelöscht: c
Gelöscht: 7
Gelöscht: 8

Ziel: Kenntnisnahme

Sprechpunkte (reaktiv):

- Belastbare Informationen zu den in der Presse geschilderten Maßnahmen der NSA liegen der Bundesregierung derzeit nicht vor. Die Medienberichte legen zwar einige Rückschlüsse nahe, die jedoch noch nicht abschließend zu verifizieren sind.

Gelöscht: dem BMI und den Behörden seines Geschäftsbereichs

- Aus diesem Grund steht die Aufklärung des Sachverhalts zurzeit im Vordergrund. Delegationen auf EU- und nationaler Ebene haben dazu Gespräche mit der US-Seite aufgenommen.
- Auch Herr Minister BMI Dr. Friedrich hat am vergangenen Freitag ausführliche politische Gespräche mit Vertretern der US-Regierung zu den NSA-Aktivitäten und ihren Auswirkungen auf Deutschland geführt. Diese Gespräche schlossen an Gespräche an, die von Experten der Bundesregierung mit den US-

Erstellt von: BMI/ IT3, Dr. Dimroth (-1993); AA/ KS-CA, J. Knodt (-2657)

Abgestimmt mit: BMWi, BMJ, BMF, BMELV, BMVg, BMFSFJ, BMZ, BKAmt, BKM

VS-Nur für den Dienstgebrauch

Sicherheitsbehörden zu diesem Thema geführt wurden. Schnelle Ergebnisse dieser Reise sind nicht zu erwarten, da es inhaltlich um komplexe Sachverhalte geht, deren vertiefte Aufarbeitung einige Zeit in Anspruch nehmen wird.

- DEU unterstützt auch die Bemühungen auf EU-Ebene um Aufklärung. Bei der Zusammenstellung entsprechender Arbeitsgruppen ist die Abgrenzung der Kompetenzen zwischen EU und MS in den relevanten Themenbereichen zu beachten.

Sachstand: Internetüberwachung / Datenerfassungsprogramme NSA

Formatiert: Deutsch (Deutschland)

Aufgrund der Veröffentlichungen von Edward Snowden berichten Medien, dass die U.S. National Security Agency (NSA):

Formatiert: Deutsch (Deutschland)

Formatiert: Deutsch (Deutschland)

(1) bei **neun US-Internetdienstleistern** (u.a. Microsoft, Google, Facebook, Apple, Yahoo, Skype) die Kommunikation von ca. 120.000 ausländischen Personen im „dauerhaften Zielfokus" abgreift; Codename: „**PRISM**";

(2) **mit britischen Diensten** beim **Anzapfen („full take") von weltweit ca. 200 Glasfaserkabel** zusammenarbeitet und die dabei gewonnenen Daten speichert (Inhalte drei Tage, Verbindungsdaten 30 Tage); Codename: „**TEMPORA**";

Formatiert: Schriftart: Fett

(3) **Internationale Kommunikationsdaten speichert** und in Echtzeit darstellen kann; allein aus Deutschland 500 Millionen Datensätze im Monat; Codename „**BOUNDLESS INFORMANT**";

(4) das **EU-Ratsgebäude in Brüssel** und **Auslandsvertretungen in den USA abgehört** habe. Betroffen seien 38 Auslandsvertretungen der EU sowie FRA, ITA, GRC, IND, JAP in Washington und New York;

(5) auf **Millionen chinesischer SMS-Nachrichten** sowie auf **eines der größten Glasfasernetze in der Asien-Pazifik-Region** („Pacnet"), betrieben an der Tsinghua-Universität, zugreift;

Erstellt von: BMI/ IT3, Dr. Dimroth (-1993); AA/ KS-CA, J. Knodt (-2657)

Abgestimmt mit: BMWi, BMJ, BMF, BMELV, BMVg, BMFSFJ, BMZ, BKAmt, BKM

VS-Nur für den Dienstgebrauch

(6) in **Brasilien eine flächendeckende Telekommunikationsüberwachung** mit Hilfe von US- und BRA-Kommunikationsdienstleister durchführt, Codename „**FAIRVIEW**".

Die **US-Regierung betont die Rechtmäßigkeit der NSA-Aktivitäten** auf Grundlage des U.S. Foreign Intelligence Surveillance Act und des Patriot Act.

In internationalen Medien wird auch über weitreichende **Datenerfassungsprogramme in Frankreich** ("le Big Brother Francais") berichtet.

Außerdem wird berichtet, US-Nachrichtendienste hätten unmittelbaren Zugriff auch auf Internetknoten in Deutschland. Dies wird von Betreiberseite jedoch dementiert. Die Aufklärung des Sachverhalts steht zurzeit im Vordergrund. Von der Seite der BReg. sind dazu insbesondere folgende Maßnahmen eingeleitet worden:

(u.a.)

- Kontakte des BMI mit der US-Botschaft auf Arbeitsebene, Übermittlung Fragenkatalog
- Gespräche BK'n Merkel – Präsident Obama
- Der Bundesaußenminister und hohe Beamte des AA haben in Gesprächen mit der US- bzw. GBR-Seite auf Aufklärung gedrängt.
- Telefonat Herr Minister BMI – US-Justizminister Holder
- Schreiben BMJ (BM'n) an US-Justizminister Holder, Forderung nach Sachverhaltsaufklärung
- Bilaterale Sachverhaltsaufklärung durch DEU Delegation ab 10. Juli (BM BMI ab 12. Juli)
- Zwischen EU und USA wird die Einrichtung einer „High level expert working goup on security and data protection" angestrebt. Eine Vordelegation (KOM, EAD, MS – auch DEU) hat am 8. Juli ein erstes Sondierungstreffen durchgeführt. Dabei wurde deutlich, dass die USA erwarten, dass auch EU-Mitgliedsstaaten sich zu ihren Datenerfassungspraktiken erklären.

Gelöscht: Prism¶
Sachstand:¶
Laut Presseberichten (The Guardian und Washington Post) soll die National Security Agency (NSA) umfangreich Telekommunikationsdaten (E-Mail, Telefon, SMS usw.) sowie personenbezogene Daten bei insgesamt neun Betreibern von Suchmaschinen (Google, Microsoft usw.), von sozialen Netzwerken (Facebook, Google usw.) und Cloudanbietern (Apple usw.) erheben und speichern. ¶
Nach den Medienberichten sollen die neun US-Unternehmen der NSA unmittelbaren Zugriff auf ihre Daten gewähren; zumindest hätten sie die Einrichtung spezieller Schnittstellen gestattet. ¶
Die Informationen der Presse beruhen im Wesentlichen auf Aussagen des 30-jährigen US-Amerikaners Edward Snowden, der nach eigenen Angaben in den vergangenen vier Jahren als Mitarbeiter externer Unternehmen für die NSA tätig gewesen sei.¶

Gelöscht: Offen bleibt die Frage nach Wissen und Einbindung deutscher Nachrichtendienste.¶

Gelöscht:

Gelöscht: Min

Gelöscht: 1

Gelöscht: Auf

Gelöscht: -Ebene

Erstellt von: BMI/ IT3, Dr. Dimroth (-1993); AA/ KS-CA, J. Knodt (-2657)

Abgestimmt mit: BMWi, BMJ, BMF, BMELV, BMVg, BMFSFJ, BMZ, BKAmt, BKM

VS-Nur für den Dienstgebrauch

- Zurzeit wird die Zusammensetzung und das Mandat der EU-US Gruppe diskutiert (insbesondere: Teilnahme KOM/EAD). Es besteht Einigkeit unter den EU-MS, zwischen **datenschutzrechtlichen** Fragen und Fragen, die die **Tätigkeit der Nachrichtendienste** betreffen, klar zu differenzieren.

Gelöscht:
Gelöscht: Nachrichtendienste betreffenden

- Aus Sicht von DEU ist zu berücksichtigen, dass die EU keine Kompetenz für nachrichtendienstliche Fragestellungen (auch nicht für datenschutzrechtliche Fragen im Zusammenhang mit Nachrichtendiensten) hat. Eine **Teilnahme von KOM/EAD** an einer nachrichtendienstlichen Gruppe ist deshalb kompetenzrechtlich nicht möglich; sie ist seitens der USA zudem nicht erwünscht. Auch für eine Teilnahme an der datenschutzrechtlichen Gruppe fehlt es KOM de iure an einer Kompetenz und ist allenfalls aus Gründen politischer Rücksichtnahme in Betracht zu ziehen.

TOP 3: State of play & Ongoing implementation of the Council Conclusions on the Joint Communication on Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace

- LTU PRÄS hat am 10.7 ein Dokument mit Optionen betr. der weiteren Umsetzung der EU CSS zirkuliert (DS 1563/13)
- Cyber-Attachés GBR/FRA/SWE/NLD/DEU hatten am 24.6. im 5er-Kreis ein Strategiedokument zu weiteren Arbeitsschwerpunkten der FoP zirkuliert

Ziel: Kenntnisnahme PRÄS-Dokument und Unterstützung Strategiepapier GBR/FRA/SWE/NLD/DEU zur künftigen Rolle Cyber-FoP

Gelöscht: Ziel: ¶

Sprechpunkte (aktiv)

- The document circulated by the Presidency on 10th of July underlines the shared responsibility of COM, EEAS and the Member States through the respective Council working groups to implement the EU Cyber Security Strategy. Thus, the importance of consistency between the implementing

stakeholders cannot be underestimated. Germany would like to express its preference for Option 3

- Additionally, in the light of increasing importance of digital issues within the EU, in EU-external relations and in global settings, highlighted by the European Council on the "Digital Agenda" in late October, an extension of the FoP mandate beyond the initial one year [=end of 2013] should be considered.
- I would like to recall that the current mandate of the FoP states to "provide a comprehensive cross-cutting forum for coordination and exchange of information encompassing various fields (…) The FoP group could also provide a forum which could flag to COREPER and to the Council general issues requiring their guidance". Thus, we should neither limit the FoP group's focus on merely following the EU Cyber Security Strategy nor duplicating existing working groups on specific cyber issues.
- The FoP should also provide common EU language for important international cyber events (Seoul Conference, ITU-meetings, ICANN GAC), thus seeking stronger linkage to the 'High Level Group on Internet Governance'.
- Additionally, we could ask the Council secretariat to set up a "Cyber Foresight Timeline" for Working groups and Councils where cyber issues are scheduled to be discussed. Providing overarching strategic guidance for our PermReps in Brussels and our HQs is an added value the FoP group should provide.
-

Gelöscht: Die FoP wurde gegründet zur ganzheitlichen Koordinierung und Einbeziehung auch von angrenzenden Themen wie Netzpolitik und Außenaspekten der Cyberpolitik. Die Koordinierung umfasst sowohl die Entwicklung als auch die Umsetzung der Cyber-Sicherheitsstrategie. Dies sollte bedacht werden, wenn es darum geht die Ausführungen zu den möglichen Aufgaben zu bewerten. Es muss darauf geachtet werden, dass eine zu enge Begrenzung der Aufgabenstellung vermieden wird.

TOP 4: CSDP aspects of the EU Cyber Security Strategy

Sprechpunkte (aktiv)

allgemein:

- Die Bundesregierung begrüßt, dass die Strategie Aufgaben für die EU, den EAD und die Mitgliedstaaten zum besseren Schutz der verteidigungspolitischen und zivilen GSVP-Strukturen aufzeigt. Rasche Konkretisierung und Umsetzung sind erforderlich.
- Der Schutz der militärischen GSVP-Missionen darf sich nicht nach geringeren Standards richten als in der NATO üblich. Dazu müssen Schwierigkeiten in der

EU-NATO-Kooperation überwunden und engere Abstimmung der Cyber-Abwehr von EU und NATO erreicht werden.

- Die zivilen Missionen der EU bedürfen ebenfalls eines hohen Schutzniveaus. Dazu müssen – unter Einhaltung der gebotenen Trennung ziviler und militärischer Strukturen – Synergien genutzt und Dopplungen vermieden werden.

FRA-Papier zu CSDP (DS 1564/13):

- We thank our French colleagues for the working paper and we share the comments by our British colleagues that we need to define and distinguish clearly the terms "cyber defence" versus "cyber resilience".

Gelöscht: support the proposal put forward

Gelöscht: which underline

- We should also clarify where cyber security issues are inextricably linked to CSDP and where not, since CSDP is a foreign policy instrument whereas the responsibility for protection of IT networks - notwithstanding their importance for CSDP missions and operations - lies elsewhere.

- The possibilities of developing a common encryption standard for CSDP missions and operations should be explored with due consideration given to existing encryption systems already used in ongoing CSDP missions and operations (EURAT), and possible interoperability with NATO encryption standards.

- We strongly support the notion of training and exercises in the field of cyber security and cyber defence which from our point of view would benefit significantly from participation of NATO in order to ensure harmonization of procedures. NATO CCDCOE could be EU's NATO interlocutor with regards to training and exercise programs.

TOP 5: Exchange of best practices:

- presentation by ENISA on assisting the preparation of National Cyber Security Strategies by Member States
- presentation by EUROPOL on practical examples of successful cooperation in combating cybercrime

Erstellt von: BMI/ IT3, Dr. Dimroth (-1993); AA/ KS-CA, J. Knodt (-2657)

Abgestimmt mit: BMWi, BMJ, BMF, BMELV, BMVg, BMFSFJ, BMZ, BKAmt, BKM

VS-Nur für den Dienstgebrauch

Ziel: Kenntnisnahme

Sprechpunkt (reaktiv)

- ENISA: Auf die Aufgaben laut neuem Mandat ist hinzuweisen; insbesondere ist darauf hinzuweisen, dass ENISA für MS nur dann tätig werden kann, wenn ENISA dazu von MS aufgefordert wurde.

TOP 6: AOB

000035

#AL6 13.1. i.U.
m.d. B.u. Stellungnahme
bis 17.1., DS!
Bitte auch BMI einbeziehen!
Rg. 601 14/1
603 n.R.
13/1

EUROPEAN PARLIAMENT

2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs i.U. 13.1.

2013/2188(INI)

23.12.2013

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

(2013/2188(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION 3

EXPLANATORY STATEMENT 35

ANNEX I: LIST OF WORKING DOCUMENTS 42

ANNEX II: LIST OF HEARINGS AND EXPERTS..... **Fehler! Textmarke nicht definiert.**

ANNEX III: LIST OF EXPERTS WHO DECLINED PARTICIPATING IN THE LIBE INQUIRY PUBLIC HEARINGS..... **Fehler! Textmarke nicht definiert.**

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

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

The European Parliament,

– having regard to the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10, 11 and 21 thereof,

– having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 15, 16 and 218 and Title V thereof,

– having regard to Protocol 36 on transitional provisions and Article 10 thereof and to Declaration 50 concerning this protocol,

– having regard to the Charter on Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof,

– having regard to the European Convention on Human Rights, notably its Articles 6, 8, 9, 10 and 13, and the protocols thereto,

– having regard to the Universal Declaration of Human Rights, notably its Articles 7, 8, 10,11,12 and 14[1],

– having regard to the International Covenant on Civil and Political Rights, notably its Articles 14, 17, 18 and 19,

– having regard to the Council of Europe Convention on Data Protection (ETS No 108) and its 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 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 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[3],

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

– 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[1], 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[2], Polish and British[3] courts, as well as before the European Court of Human Rights[4], in relation to systems of mass surveillance,

– having regard to the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, and in particular to Title III thereof[5],

– having regard to Commission Decision 520/2000 of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour privacy principles and the related frequently asked questions (FAQs) issued by the US Department of Commerce,

– having regard to the Commission assessment reports on the implementation of the Safe Harbour privacy principles of 13 February 2002 (SEC(2002)196) and of 20 October 2004 (SEC(2004)1323),

– having regard to the Commission Communication of 27 November 2013 (COM(2013)847) on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU and the Commission Communication of 27 November 2013 on rebuilding trust in EU-US data flows (COM(2013)846),

– having regard to the European Parliament 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

---

[1] http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
[2] 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 against X; Tribunal de Grande Instance of Paris.
[3] Cases by Privacy International and Liberty in the Investigatory Powers Tribunal.
[4] Joint Application Under Article 34 of Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (Applicants) - v - United Kingdom (Respondent).
[5] OJ C 197, 12.7.2000, p. 1.

of Commerce, which took the view that the adequacy of the system could not be confirmed[1], 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)844),

– 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)630, 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 US 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 legislative proposals currently under examination in the US Congress, in particular the draft US Freedom Act,

– 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,

– 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 and 7 November 2002 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),

– having regard to its resolution of 21 May 2013 on the EU Charter: standard settings for media freedom across the EU[2],

– 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, whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter[3],

– having regard to its resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken[4],

– having regard to its resolution of 23 October 2013 on the suspension of the TFTP

[1] Council document 16987/13.
[2] Texts adopted, P7_TA(2013)0203.
[3] Texts adopted, P7_TA-(2013)0322.
[4] Texts adopted, P7_TA(2013)0444.

agreement as a result of US National Security Agency surveillance[1],

– having regard to its resolution of 10 December 2013 on unleashing the potential of cloud computing[2],

– 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[3],

– 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 (A70000/2013),

The impact of mass surveillance

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

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

C. whereas in September 2001 the world entered a new phase which resulted in the fight against terrorism being listed among the top priorities of most governments; whereas the revelations based on leaked documents from Edward Snowden, former NSA contractor, put democratically elected leaders under an obligation to address the challenges of the increasing capabilities of intelligence agencies in surveillance activities and their implications for the rule of law in a democratic society;

D. 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 high risk of violation of EU legal standards, fundamental rights and data protection standards;
- the degree of trust between EU and US 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 degree of control and effective oversight by the US political authorities and certain EU Member States over their intelligence communities;

[1] Texts adopted, P7_TA(2013)0449.
[2] Texts adopted, P7_TA(2013)0535.
[3] OJ C 353 E, 3.12.2013, p.156-167.

- the possibility of these mass surveillance operations being used for reasons other than national security and the strict fight against terrorism, for example economic and industrial espionage or profiling on political grounds;
- 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;
- the threats to privacy in a digital era;

E. whereas the unprecedented magnitude of the espionage revealed requires full investigation by the US authorities, the European Institutions and Members States' governments and national parliaments;

F. whereas the US authorities have denied some of the information revealed but not contested the vast majority of it; whereas the public debate has developed on a large scale in the US and in a limited number of EU Member States; whereas EU governments too often remain silent and fail to launch adequate investigations;

G. 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 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

H. 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];

I. 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];

J. whereas in its report of 12 December 2013, the President's Review Group on Intelligence and Communication Technology proposes 45 recommendations to the President of the US; 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 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

[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.

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 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;

K. whereas in respect of intelligence activities about non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental issue of respect for privacy and human dignity 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;

Legal framework

Fundamental rights

L. 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 not helped sufficiently with establishing 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;

M. 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 on Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy;

Union competences in the field of security

N. 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 disposes of certain competences on matters relating to the collective security of the Union; whereas the EU has exercised competence in matters of internal security 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;

O. 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;

P. whereas, under 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; whereas this also goes for cooperation with other States' authorities in the field of national security;

Extra-territoriality

Q. whereas the extra-territorial 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 exceptional circumstances, it is necessary to take action at the EU level to ensure that the rule of law, and the rights of natural and legal persons are respected within the EU, in particular by removing, neutralising, blocking or otherwise countering the effects of the foreign legislation concerned;

International transfers of data

R. 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 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;

Transfers to the US based on the US Safe Harbour

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

T. whereas, in order to enable EU data controllers to transfer personal data to an entity in the US, the Commission, in its Decision 520/2000, has declared the adequacy of the protection provided by the Safe Harbour privacy principles and the related FAQs issued by the US Department of Commerce for personal data transferred from the Union to organisations established in the United States that have joined the Safe Harbour;

U. whereas in its resolution of 5 July 2000 the European 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;

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

V. whereas Commission Decision 520/2000 stipulates that the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Safe Harbour principles, in order to protect individuals with regard to the processing of their personal data in cases where there is a substantial likelihood that the Safe Harbour principles are being violated or that the continuing transfer would create an imminent risk of grave harm to data subjects;

W. whereas Commission Decision 520/2000 also states that when 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 said Decision or limiting its scope;

X. whereas in its first two reports on the implementation of the Safe Harbour, of 2002 and 2004, the Commission identified several deficiencies as regards the proper implementation of the Safe Harbour and made several recommendations to the US authorities with a view to rectifying them;

Y. 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;

Z. whereas on 28-31 October 2013 the delegation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) to Washington D.C. met 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;

AA. 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 such an exception should not be used in a way that

undermines the protection afforded by EU data protection law and the Safe Harbour principles;

AB. whereas large-scale access by US intelligence agencies has seriously eroded transatlantic trust and negatively impacted on the trust for 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

AC. 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 and Canada 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;

AD. whereas Commission Decisions 2013/65[1] and 2/2002 of 20 December 2001[2] have declared the adequate level of protection ensured by the New Zealand and the Canadian Personal Information Protection and Electronic Documents Act; 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

AE. 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;

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

AG. whereas Directive 95/46/EC empowers the Commission to decide that specific standard contractual clauses offer sufficient safeguards required by the Directive and whereas on this basis the Commission has adopted three models of standard contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;

AH. 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 when 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

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

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;

AI. 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;

Transfers based on TFTP and PNR agreements

AJ. whereas in its resolution of 23 October 2013 the European Parliament expressed serious concerns about 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 Agreement, in particular Article 1 thereof;

AK. whereas the European Parliament asked the Commission to suspend the Agreement and requested that all relevant information and documents be made available immediately for Parliament's deliberations;

AL. 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;

AM. whereas during the LIBE delegation to Washington of 28-31 October 2013 the 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 LIBE Committee inquiry that the NSA and GCHQ had targeted SWIFT networks;

AN. whereas the Belgian and Dutch 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[1];

AO. whereas according to the Joint Review of the EU-US PNR agreement, the United States 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;

AP. 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

AQ. whereas the EU-US Agreement on mutual legal assistance in criminal matters of 6 June 2003[2] entered into force on 1 February 2010 and is intended to facilitate cooperation between the EU and 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')

AR. 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;

AS. whereas this agreement should provide for clear and precise legally binding data-processing principles and should in particular recognise EU citizens' right to access, 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 and independent oversight of the data-processing activities;

AT. 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;

AU. 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

[1] 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

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

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

AV. 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;

AW. 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;

AX. 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, the Council has been unable to arrive at a general approach on the General Data Protection Regulation and the Directive[3];

IT security and cloud computing

AY. whereas the resolution of 10 December[4] emphasises the economic potential of 'cloud computing' business for growth and employment;

AZ. 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;

BA. whereas mass surveillance activities give intelligence agencies access to personal data stored by EU individuals under cloud services agreements with major US cloud providers; whereas the US intelligence authorities have accessed personal data stored in servers located on EU soil by tapping into the internal networks of Yahoo and Google[5]; whereas such activities constitute a violation of international obligations; 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;

---

[1] COM(2012) 11, 25.1.2012.
[2] COM(2012) 10, 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[4] AT-0353/2013 PE506.114V2.00.
[5] The Washington Post , 31 October 2013.

Democratic oversight of intelligence services

BB. whereas intelligence services perform an important function in protecting democratic society against internal and external threats; whereas they are given special powers and capabilities to this end; whereas these powers are to be used within the rule of law, as otherwise they risk losing legitimacy and eroding the democratic nature of society;

BC. whereas the high level of secrecy that is intrinsic to the intelligence services in order to avoid endangering ongoing operations, revealing *modi operandi* or putting at risk the lives of agents impedes full transparency, public scrutiny and normal democratic or judicial examination;

BD. whereas technological developments have led to increased international intelligence cooperation, also involving the exchange of personal data, and often blurring the line between intelligence and law enforcement activities;

BE. whereas most of existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid technological developments over the last decade;

BF. whereas democratic oversight of intelligence activities is still 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;

Main findings

1. Considers that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, 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 and 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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill); believes that the existence of programmes of a similar nature, even if on a more limited scale, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA);

3. Notes the allegations of 'hacking' or tapping into the Belgacom systems by the UK intelligence agency GCHQ; reiterates the indication by Belgacom that it could not

confirm that EU institutions were targeted or affected, and that the malware used was extremely complex and required the use of extensive financial and staffing resources for its development and use that would not be available to private entities or hackers;

4. States that trust has been profoundly shaken: trust between the two transatlantic partners, trust among EU Member States, trust between citizens and their governments, trust in the respect of the rule of law, and trust in the security of IT services; believes that in order to rebuild trust in all these dimensions a comprehensive plan is urgently needed;

5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; wholeheartedly supports the fight against terrorism, but strongly believes that it can never in itself be a justification for untargeted, secret and sometimes even illegal mass surveillance programmes; expresses concerns, therefore, regarding the legality, necessity and proportionality of these programmes;

6. Considers it very doubtful that data collection of such magnitude is only guided by the fight against terrorism, as it involves the collection of all possible data of all citizens; points therefore to the possible existence of other power motives such as political and economic espionage;

7. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Title I and Title VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4 paragraph 3 of the Treaty on European Union and the principle that the Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';

8. 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 and for democratic accountability;

9. Condemns in the strongest possible terms the vast, systemic, blanket collection of the personal data of innocent people, often comprising intimate personal information; emphasises that the systems of mass, indiscriminate surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but that it is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on the freedom of the press, thought and speech, as well as a significant potential for abuse of the information gathered against political adversaries; emphasises that these mass surveillance activities appear also to entail illegal actions by intelligence services and raise questions regarding the extra-territoriality of national laws;

10. 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, promoting instead a mix of law enforcement and intelligence activities with blurred legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in

that 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;

11. Is adamant that secret laws, treaties 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, surveillance activities such as those examined by this inquiry may not be automatically recognised or enforced, but must be submitted individually to the appropriate national procedures on mutual recognition and legal assistance, including rules imposed by bilateral agreements;

12. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments; considers that, 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 of all kinds that puts at risk the integrity of the person, the scale of this problem is unprecedented;

13. Regards it as a clear finding, as emphasised by the technology experts who testified before the inquiry, that at the current stage of technological development there is no guarantee, either for EU public institutions or for citizens, that their IT security or privacy can be protected from intrusion by well-equipped third countries or EU intelligence agencies ('no 100% IT security'); notes that this alarming situation can only be remedied if Europeans are willing to dedicate sufficient resources, both human and financial, to preserving Europe's independence and self-reliance;

14. Strongly rejects the notion that these issues are purely a matter of national security and therefore the sole competence of Member States; 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'[2]; 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 is not only legitimate, but also a matter of EU autonomy and sovereignty;

15. Commends the current discussions, inquiries and reviews concerning the subject of this inquiry in several parts of the world; points to the Global Government Surveillance Reform signed up to by the world's leading technology companies, which calls for sweeping changes to national surveillance laws, including an international ban on bulk collection of data to help preserve the public's trust in the internet; notes with great interest the recommendations published recently by the US President's Review Group on Intelligence and Communications Technologies; strongly urges governments to take these calls and recommendations fully into account and to overhaul their national frameworks for the intelligence services in order to implement appropriate safeguards and oversight;

---

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

16. 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;

17. 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;

18. Intends to request strong political undertakings from the European Commission to be designated after the May 2014 elections to implement the proposals and recommendations of this Inquiry; expects adequate commitment from the candidates in the upcoming parliamentary hearings for the new Commissioners;

Recommendations

19. Calls on the US authorities and the EU Member States to prohibit blanket mass surveillance activities and bulk processing of personal data;

20. Calls on certain EU Member States, including the UK, Germany, France, Sweden and the Netherlands, to revise where necessary their national legislation and practices governing the activities of intelligence services so as to ensure that they are in line with the standards of the European Convention on Human Rights and comply with their fundamental rights obligations as regards data protection, privacy and presumption of innocence; in particular, given the extensive media reports referring to mass surveillance in the UK, would emphasise that the 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 – should be revised;

21. Calls on the Member States 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;

22. 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 and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law;

23. 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';

24. 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 EU 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);

25. 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 and to sign the Additional Protocol allowing for complaints by individuals under the ICCPR;

26. Strongly opposes any conclusion of an additional protocol or guidance to the Council of Europe Cybercrime Convention (Budapest Convention) on transborder access to stored computer data which could provide for a legitimisation of intelligence services' access to data stored in another jurisdiction without its authorisation and without the use of existing mutual legal assistance instruments, since this could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions and would be in conflict with Council of Europe Convention 108;

27. 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 for transfers of personal data;

International transfers of data

US data protection legal framework and US Safe Harbour

28. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by 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 (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); expresses its concerns on the fact that these organisations admitted that they do not encrypt information and communications flowing between their data centres, thereby enabling intelligence services to intercept information[1];

29. Considers that large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not per se meet the criteria for derogation under 'national security';

30. 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

[1] The Washington Post, 31 October 2013.

under other instruments, such as contractual clauses or BCRs setting out specific safeguards and protections;

31. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles, and of the related FAQs issued by the US Department of Commerce;

32. Calls on Member States' competent authorities, namely 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, provided they contain the necessary safeguards and protections with respect to the protection of the privacy and fundamental rights and freedoms of individuals;

33. Calls on the Commission to present by June 2014 a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities in response to the fact that the EU and the US legal systems for protecting personal data are drifting apart;

Transfers to other third countries with adequacy decision

34. 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;

35. Recalls that Directive 95/46/EC 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 data transfer operations; likewise recalls 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; whereas Directive 95/46/EC also empowers the Commission to declare that a third country does not ensure an adequate level of protection;

36. 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;

37. Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New Zealand and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by Commission Decisions 2013/651 and 2/2002 of 20 December 2001, have been affected by the involvement of their national intelligence agencies in the mass surveillance of EU

---

1 OJ L 28, 30.1.2013, p. 12.

citizens and, if necessary, to take appropriate measures to suspend or revers the adequacy decisions; expects the Commission to report to the European Parliament on its findings on the abovementioned countries by December 2014 at the latest;

Transfers based on contractual clauses and other instruments

38. Recalls that national data protection authorities have indicated that neither standard contractual clauses nor BCRs were written 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;

39. 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 established that the law to which the data importer is subject imposes upon him requirements which go beyond the restrictions necessary in a democratic society and which are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or because continuing transfer would create an imminent risk of grave harm to the data subjects;

40. 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;

41. Calls on the Commission to examine 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

42. Calls on the Commission to conduct before the end 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 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;

EU mutual assistance in criminal matters

43. Asks the Council and the 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 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

44. 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;

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

46. Calls on the European 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')

47. Considers that a satisfactory solution under the 'Umbrella agreement' is a pre-condition for the full restoration of trust between the transatlantic partners;

48. Asks for an immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should provide for clear rights for EU citizens and effective and enforceable administrative and judicial remedies in the US without any discrimination;

49. Asks the Commission and the Council not to initiate any new sectorial agreements or arrangements for the transfer of personal data for law enforcement purposes as long as the 'Umbrella Agreement' has not entered into force;

50. 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

51. Calls on the Council Presidency and the majority of Member States who support a high level of data protection to show a sense of leadership and responsibility and accelerate their work on the whole Data Protection Package to allow for adoption in 2014, so that EU citizens will be able to enjoy better protection in the very near future;

52. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals and therefore must 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;

Cloud computing

53. Notes that trust in US cloud computing and cloud providers has been negatively affected by the abovementioned practices; emphasises, therefore, the development of European clouds as an essential element for growth and employment and trust in cloud computing services and providers and for ensuring a high level of personal data protection;

54. Reiterates its serious concerns about 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, and about direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

55. Regrets 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;

56. Calls on the Commission and the Member States to speed up the work of establishing a European Cloud Partnership;

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

Transatlantic Trade and Investment Partnership Agreement (TTIP)

58. 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 and for the ability of both the EU and the US to set future global regulatory standards;

59. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that the European Parliament will only consent to the final TTIP agreement provided the agreement fully respects fundamental rights recognised by the EU Charter, and that the protection of the privacy of individuals in relation to the processing and dissemination of personal data must continue to be governed by Article XIV of the GATS;

Democratic oversight of intelligence services

60. 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 an adequate technical capability and expertise, the

majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

61. Invites, as it has done in the case of Echelon, 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 national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means to be able to effectively control intelligence services;

62. Calls for the setting up of a high-level group to strengthen cooperation in the field of intelligence at EU level, combined with a proper oversight mechanism ensuring both democratic legitimacy and adequate technical capacity; stresses that the high-level group should cooperate closely with national parliaments in order to propose further steps to be taken for increased oversight collaboration in the EU;

63. Calls on this high-level group to define minimum European standards or guidelines on the (ex ante and ex post) oversight of intelligence services on the basis of existing best practices and recommendations by international bodies (UN, Council of Europe);

64. Calls on the high-level group to set strict limits on the duration of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority;

65. Calls on the high-level group to develop criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'[1];

66. Intends to organise a conference with national oversight bodies, whether parliamentary or independent, by the end of 2014;

67. 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;

68. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);

69. Urges the Commission to present, by September 2014, a proposal for a legal basis for the activities of the EU Intelligence Analysis Centre (IntCen), as well as a proper oversight mechanism adapted to its activities, including regular reporting to the European Parliament;

70. Calls on the Commission to present, by September 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

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

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;

71. Recalls the provisions of 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 that should be used to improve oversight at EU level;

EU agencies

72. 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 has been lawfully acquired by national authorities, particularly if the information or data was initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data;

73. Calls on Europol to ask the competent authorities of the Member States, in line with its competences, to initiate investigations with regard to possible cybercrimes and cyber attacks committed by governments or private actors in the course of the activities under scrutiny;

Freedom of expression

74. Expresses deep concern about the developing 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';

75. Considers that the detention of Mr Miranda and the seizure of the material in his possession under Schedule 7 of the Terrorism Act 2000 (and also the request to *The Guardian* to destroy or hand over the material) constitutes an interference with the right of freedom of expression as recognised by Article 10 of the ECHR and Article 11 of the EU Charter;

76. Calls on the Commission to put forward a proposal for a comprehensive framework for the protection of whistleblowers in the EU, with particular attention to the specificities of whistleblowing in the field of intelligence, for which provisions relating to whistleblowing in the financial field may prove insufficient, and including strong guarantees of immunity;

EU IT security

77. 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; notes that these attacks require such financial and human resources that they are likely to originate from state entities acting on behalf of foreign governments or even from certain EU national governments that support them; in this context, regards the case of the hacking or tapping of the telecommunications company Belgacom as a worrying example of an attack against the EU's IT capacity;

78. 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 an autonomous IT key-resource capability for the mid term; 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;

79. Is highly concerned by indications that foreign intelligence services sought to lower IT security standards and to install backdoors in a broad range of IT systems;

80. Calls on all the Members States, the Commission, the Council and the European Council to address the EU's dangerous lack of autonomy in terms of IT tools, companies and providers (hardware, software, services and network), and encryption and cryptographic capabilities;

81. Calls on the Commission, standardisation bodies and ENISA to develop, by September 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; believes that such standards should be set in an open and democratic process, not 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;

82. Points out that both telecom companies and the EU and national telecom regulators 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 encryption of communications;

83. Supports the EU cyber strategy but considers that it does not cover all possible threats and should be extended to cover malicious state behaviours;

84. Calls on the Commission, by January 2015 at the latest, to present an Action Plan to develop more 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);

85. Calls on the Commission, in the framework of the next Work Programme of the

Horizon 2020 Programme, to assess whether more resources should be directed towards boosting European research, development, innovation and training in the field of IT technologies, in particular privacy-enhancing technologies and infrastructures, cryptology, secure computing, open-source security solutions and the Information Society;

86. Asks the Commission to map out current responsibilities and to review, by June 2014 at the latest, the need for a broader mandate, better coordination and/or additional resources and technical capabilities for Europol's CyberCrime Centre, ENISA, CERT-EU and the EDPS in order to enable them to be more effective in investigating major IT breaches in the EU and in performing (or assisting Member States and EU bodies to perform) on-site technical investigations regarding major IT breaches;

87. Deems it necessary for the EU to be supported by an EU IT Academy that brings together the best European experts in all related fields, tasked with providing all relevant EU Institutions and bodies with scientific advice on IT technologies, including security-related strategies; as a first step asks the Commission to set up an independent scientific expert panel;

88. Calls on the European Parliament's Secretariat to carry out, by September 2014 at the latest, a thorough review and assessment of the European 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 the EP's IT systems; believes that such an assessment should at the least provide information analysis and recommendations on:

- the need for regular, rigorous, 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 specific IT security/privacy requirements, including the possibility of a requirement for Open Source Software as a condition of purchase;
- the list of US companies under contract with the European Parliament in the IT and telecom fields, taking into account revelations about NSA contracts with a company such as RSA, whose products the European Parliament is using to supposedly protect remote access to their data by its Members and staff;
- the reliability and resilience of third-party 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;
- the use of more open-source systems and fewer off-the-shelf commercial systems;
- the impact of the increased use of mobile tools (smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;

- the security of the communications between different workplaces of the European Parliament and of the IT systems used at the European Parliament;
- the use and location of servers and IT centres for the EP'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 storage by the EP, including what kind of data is stored on the cloud, how the content and access to it is protected and where the cloud is located, clarifying the applicable data protection legal regime;
- 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 signature in email;
- an analysis of the benefits of using the GNU Privacy Guard as a default encryption standard for emails which would at the same time allow for the use of digital signatures;
- the possibility of setting up a secure Instant Messaging service within the European Parliament allowing secure communication, with the server only seeing encrypted content;

89. Calls on all the EU Institutions and agencies to perform a similar exercise, by December 2014 at the latest, in particular the European Council, the Council, the 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;

90. 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;

91. 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, should be developed and operated in such a way as to ensure that data is not compromised as a result of US requests under the Patriot Act; asks eu-LISA to report back to Parliament on the reliability of the systems in place by the end of 2014;

92. 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 (such as Brazil), and 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;

93. Calls for the overall architecture of the internet in terms of data flows and storage to be reconsidered, striving for more data minimisation and transparency and less centralised mass storage of raw data, as well as avoiding unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy;

94. Calls on the Member States, in cooperation with ENISA, Europol's CyberCrime Centre, CERTs and national data protection authorities and cybercrime units, to start 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 'digital hygiene', encryption and safe cloud computing, making full use of the public interest information platform provided for in the Universal Service Directive;

95. Calls on the Commission, by September 2014, to evaluate the possibilities of encouraging software and hardware manufacturers to introduce more security and privacy through default features in their products, including the possibility of introducing legal liability on the part of manufacturers for unpatched known vulnerabilities or the installation of secret backdoors, and disincentives for the undue and disproportionate collection of mass personal data, and if appropriate to come forward with legislative proposals;

Rebuilding trust

96. Believes that the inquiry has shown the need for the US to restore trust with its partners, as US intelligence agencies' activities are primarily at stake;

97. 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 the rule of law and the credibility of democratic safeguards in a digital society;

Between the EU and the US

98. 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;

99. 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;

100. 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; insists, however, that clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership;

101. Is ready actively 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 privacy rights of EU citizens are addressed, equal information rights and privacy protection in US courts guaranteed and the current discrimination not perpetuated;

102. Insists that necessary reforms be undertaken and effective guarantees given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is limited by clearly specified conditions and related to reasonable suspicion or probable cause of terrorist or criminal activity; stresses that this purpose must be subject to transparent judicial oversight;

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

104. Urges the EU 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;

105. 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 among the transatlantic allies;

106. 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

107. Also believes that that the involvement and activities of EU Members States has led to a loss of trust; is of the opinion that only full clarity as to purposes and means of surveillance, public debate and, ultimately, revision of legislation, including a strengthening of the system of judicial and parliamentary oversight, will be able to

re-establish the trust lost;

108. Is aware that some EU Member States are pursuing bilateral communication with the US authorities on spying allegations, and that some of them have concluded (United Kingdom) or envisage concluding (Germany, France) so-called 'anti-spying' arrangements; underlines that these Member States need to observe fully the interests of the EU as a whole;

109. Considers that such arrangements should not breach European Treaties, especially the principle of sincere cooperation (under Article 4 paragraph 3 TEU), or undermine EU policies in general and, more specifically, the internal market, fair competition and economic, industrial and social development; reserves its right to activate Treaty procedures in the event of such arrangements being proved to contradict the Union's cohesion or the fundamental principles on which it is based;

Internationally

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

111. 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 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'; asks the High Representative/Vice-President of the Commission and the External Action Service to take a proactive stance;

112. Calls on the Member States to develop a coherent and strong strategy within the United Nations, supporting in particular the resolution on 'The right to privacy in the digital age' initiated by Brazil and Germany, as adopted by the third UN General Assembly Committee (Human Rights Committee) on 27 November 2013;

Priority Plan: A European Digital Habeas Corpus

113. Decides to submit to EU citizens, Institutions and Member States the abovementioned recommendations as a Priority Plan for the next legislature;

114. Decides to launch A European Digital Habeas Corpus for protecting privacy based on the following 7 actions with a European Parliament watchdog:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella Agreement ensuring proper redress mechanisms for EU citizens 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 have been properly addressed;

Action 5: Protect the rule of law and the fundamental rights of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 6: Develop a European strategy for IT independence (at national and EU level);

Action 7: Develop the EU as a reference player for a democratic and neutral governance of the internet;

115. Calls on the EU Institutions and the Member States to support and promote the European Digital Habeas Corpus; undertakes to act as the EU citizens' rights watchdog, with the following timetable to monitor implementation:

- April-July 2014: a monitoring group based on the LIBE inquiry team responsible for monitoring any new revelations in the media 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 in the guidelines to be adopted under Article 68 TFEU;
- Autumn 2014: a commitment that the European Digital Habeas Corpus and related recommendations will serve as key criteria for the approval of the next Commission;
- 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;
- 2015: 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;

116. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the parliaments and governments of the Member States, 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, the Government and the Parliament of the Federative Republic of Brazil, and the United Nations Secretary-General.

EXPLANATORY STATEMENT

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

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

Methodology

From July 2013, the LIBE Committee of Inquiry was responsible for the extremely challenging task of fulfilling the mandate[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

---

[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).

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 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 State's 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

[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

parliaments have launched inquiries.

5 reasons to act

– The "mass surveillance argument": in which society do we want to live?

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

– The "fundamental rights argument":

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

– The "EU internal security argument":

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

– The "deficient oversight argument"

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

– The "chilling effect on media" and the protection of whistleblowers

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

---

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

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

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

Habeas Corpus in a Surveillance Society

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

Habeas Corpus is recognised as a fundamental legal instrument to safeguarding individual freedom against arbitrary state action. What is needed today is an extension of Habeas Corpus to the digital era. Right to privacy, respect of the integrity and the dignity of the individual are at stake. Mass collections of data with no respect for EU data protection rules and specific violations of the proportionality principle in the data management run counter to the constitutional traditions of the Member States and the 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 for protecting privacy based on 7 actions:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella agreement ensuring proper redress mechanisms for EU citizens in case of data transfers from the EU to the US for law-enforcement purposes;

Action 3: Suspend Safe Harbour until a full review is 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 EU highest standards;

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

Action 5: Protect the rule of law and the fundamental rights of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 6: Develop a European strategy for IT independence (at national and EU level);

Action 7: Develop the EU as a reference player for a democratic and neutral governance of Internet;

After the conclusion of the Inquiry the European Parliament should continue acting as EU citizens' rights watchdog 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 in the media concerning the Inquiries 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 in the guidelines to be adopted under Article 68 TFEU;

- Autumn 2014: a commitment that the European Digital Habeas Corpus and related recommendations will serve as key criteria for the approval of the next Commission;

- 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 European intelligence oversight bodies of European national parliaments;

- 2015: a conference gathering high-level European experts in the various fields conducive to IT security (including mathematics, cryptography, privacy enhancing technologies, …) to help foster an EU IT strategy for the next legislature;

ANNEX I: LIST OF WORKING DOCUMENTS

LIBE Committee Inquiry

Rapporteur & Shadows as co-authors	Issues	EP resolution of 4 July2013 (see paragraphs 15-16)
Mr Moraes (S&D)	US and EU Member Surveillance programmes and their impact on EU citizens fundamental rights	16 (a) (b) (c) (d)
Mr Voss (EPP)	US surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation	16 (a) (b) (c)
Mrs. In't Veld (ALDE) & Mrs. Ernst (GUE)	Democratic oversight of Member State intelligence services and of EU intelligence bodies.	15, 16 (a) (c) (e)
Mr Albrecht (GREENS/EFA)	The relation between the surveillance practices in the EU and the US and the EU data protection provisions	16 (c) (e) (f)
Mr Kirkhope (ECR)	Scope of International, European and national security in the EU perspective	16 (a) (b)
AFET 3 Members	Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens	16 (a) (b) (f)

ANNEX II: LIST OF HEARINGS AND EXPERTS

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

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

Date	Subject	Experts
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 • Jacob APPELBAUM, investigative journalist, software developer and computer security researcher with the Tor Project • 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 • Gerhard SCHMID (former MEP and Rapporteur of the ECHELON report 2001) • Duncan CAMPBELL, investigative journalist and author of the STOA report "Interception Capabilities 2000"
12th September 2013 10.00 – 12.00	- Feedback of the meeting of the EU-US Transatlantic group of experts on data protection of 19/20	• Darius ŽILYS, Council Presidency, Director International Law Department,

(STR)	September 2013 - working method and cooperation with the LIBE Committee Inquiry (In camera)	Lithuanian Ministry of Justice (co-chair of the EU-US ad hoc working group on data protection) • Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection) • 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) **With AFET**	- Allegations of NSA tapping into the SWIFT data used in the TFTP programme	• Cecilia MALMSTRÖM, Member of the European Commission • Rob WAINWRIGHT, Director of Europol • 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) • Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection) • 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) • Greg NOJEIM, Senior Counsel

	- Effectiveness of surveillance in fighting crime and terrorism in Europe - Presentation of the study on the US surveillance programmes and their impact on EU citizens' privacy	and Director of Project on Freedom, Security & Technology, Center for Democracy & Technology (CDT) (via videoconference) • Dr Reinhard KREISSL, Coordinator, Increasing Resilience in Surveillance Societies (IRISS) (via videoconference) • 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) **With AFET**	- Exchange of views with US Civil Society (Part II) - Whistleblowers' activities in the field of surveillance and their legal protection	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU) Statements by whistleblowers: • Thomas DRAKE, ex-NSA Senior Executive • J. Kirk WIEBE, ex-NSA Senior analyst • Annie MACHON, ex-MI5 Intelligence officer Statements by NGOs on legal protection of whistleblowers: • Jesselyn RADACK, lawyer and representative of 6 whistleblowers, Government Accountability Project • John DEVITT, Transparency International Ireland
3rd October 2013 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. • Mr Dirk LYBAERT, Secretary

		General, BELGACOM S.A. • 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 - impact of us surveillance programmes on other instruments for international transfers (contractual clauses, binding corporate rules)	• Dr. Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (GERMANY) • Christopher CONNOLLY – Galexia • Peter HUSTINX, European Data Protection Supervisor (EDPS) • Ms. Isabelle FALQUE-PIERROTIN, President of CNIL (FRANCE)
14th October 2013 15.00 - 18.30 (BXL)	- Electronic Mass Surveillance of EU Citizens and International, Council of Europe and EU Law - Court cases on Surveillance Programmes	• 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" • Judge Bostjan ZUPANČIČ, Judge at the ECHR (via videoconference) • Douwe KORFF, Professor of Law, London Metropolitan University • Dominique GUIBERT, Vice-Président of the "Ligue des Droits de l'Homme" (LDH) • Nick PICKLES, Director of Big Brother Watch • Constanze KURZ, Computer Scientist, Project Leader at Forschungszentrum für Kultur und Informatik

7th November 2013 9.00 – 11.30 and 15.00 - 18h30 (BXL)	- The role of EU IntCen in EU Intelligence activity (in Camera)	• Mr Ilkka SALMI, Director of EU Intelligence Analysis Centre (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 • 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) (Venice Commission) (UK)	• Mr Iain CAMERON, Member of the European Commission for Democracy through Law - "Venice Commission" • Mr Ian LEIGH, Professor of Law, Durham University • Mr David BICKFORD, Former Legal Director of the Security and intelligence agencies MI5 and MI6 • Mr Gus HOSEIN, Executive Director, Privacy International
	- EU-US transatlantic experts group	• Mr Paul NEMITZ, Director - Fundamental Rights and Citizenship, DG JUST, European Commission • Mr Reinhard PRIEBE, Director - Crisis Management and Internal Security, DG Home, European Commission
11th November 2013 15h-18.30 (BXL)	- US surveillance programmes and their impact on EU citizens' privacy (statement by Mr Jim SENSENBRENNER, Member of the US Congress)	• Mr Jim SENSENBRENNER, US House of Representatives, (Member of the Committee on the Judiciary and Chairman of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations)
	- 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)

	- US NSA programmes for electronic mass surveillance and the role of IT Companies (Microsoft, Google, Facebook)	• Mr A.H. VAN DELDEN, Chair of the Dutch independent Review Committee on the Intelligence and Security Services (CTIVD • Ms Dorothee BELZ, Vice-President, Legal and Corporate Affairs Microsoft EMEA (Europe, Middle East and Africa) • Mr Nicklas LUNDBLAD, Director, Public Policy and Government Relations, Google • Mr Richard ALLAN, Director EMEA Public Policy, Facebook
14th November 2013 15.00 – 18.30 (BXL) **With AFET**	- IT Security of EU institutions (Part I) (EP, COM (CERT-EU), (eu-LISA) - The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part III)(BE, DA)	• Mr Giancarlo VILELLA, Director General, DG ITEC, European Parliament • Mr Ronald PRINS, Director and co-founder of Fox-IT • Mr Freddy DEZEURE, head of task force CERT-EU, DG DIGIT, European Commission • Mr Luca ZAMPAGLIONE, Security Officer, eu-LISA • Mr Armand DE DECKER, Vice-Chair of the Belgian Senate, Member of the Monitoring Committee of the Intelligence Services Oversight Committee • Mr Guy RAPAILLE, Chair of the Intelligence Services Oversight Committee (Comité R) • 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 –	- The role of Parliamentary oversight of intelligence services at	• Mr Michael TETZSCHNER, member of The Standing

18.30 (BXL)	national level in an era of mass surveillance (Part IV) (Norway)	Committee on Scrutiny and Constitutional Affairs, Norway (Stortinget)
5th December 2013, 15.00 – 18.30 (BXL)	- IT Security of EU institutions (Part II) - The impact of mass surveillance on confidentiality of lawyer-client relations	• Mr Olivier BURGERSDIJK, Head of Strategy, European Cybercrime Centre, EUROPOL • Prof. Udo HELMBRECHT, Executive Director of ENISA • Mr Florian WALTHER, Independent IT-Security consultant • Mr Jonathan GOLDSMITH, Secretary General, Council of Bars and Law Societies of Europe (CCBE)
9th December 2013 (STR)	- Rebuilding Trust on EU-US Data flows - Council of Europe Resolution 1954 (2013) on "National security and access to information"	• Ms Viviane REDING, Vice President of the European Commission • 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) IT means of protecting privacy	• Ms Vanessa GRAZZIOTIN, Chair of the Parliamentary Committee of Inquiry on Espionage • Mr Ricardo DE REZENDE FERRAÇO, Rapporteur of the Parliamentary Committee of Inquiry on Espionage • Mr Bart PRENEEL, Professor in Computer Security and Industrial Cryptography in the University KU Leuven, Belgium • Mr Stephan LECHNER, Director, Institute for the Protection and Security of the Citizen (IPSC), - Joint Research Centre(JRC), European Commission • Dr. Christopher SOGHOIAN,

	Exchange of views with the journalist having made public the facts (Part II) (Videoconference)	Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union • Christian HORCHERT, IT-Security Consultant, Germany • Mr Glenn GREENWALD, Author and columnist with a focus on national security and civil liberties, formerly of the Guardian

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

1. Experts who declined the LIBE Chair's Invitation

US

- Mr Keith Alexander, General US Army, Director NSA[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

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, Manager Public Policy, Amazon Senior

---

[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

Germany

- Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Netherlands

- Ms Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, Nederland
- Mr Rob Bertholee, Directeur Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Sweden

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

000087

EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

LIBE(2014)0109_1

DRAFT AGENDA

Meeting

Thursday 9 January 2014, 9.00 – 12.30 and 14.00 – 15.30

Brussels

Room: József Antall (2Q2)

9 January 2014, 9.00 – 10.00

In camera

1. **Coordinators' meeting**

9 January 2014, 10.00 – 10.05

2. **Chair's announcements**

   PLEASE NOTE THAT ALL TIME SLOTS ARE ONLY INDICATIVE AND ARE SUBJECT TO CHANGE DURING THE MEETING!

3. **Adoption of agenda**

4. **Approval of minutes of meeting of:**
   - 8-9 July 2013 — PV – PE524.666v01-00
   - 5 September 2013 — PV – PE516.906v01-00
   - 4-5 November 2013 — PV – PE522.824v02-00

- 28 November 2013 — PV – PE524.815v01-00

9 January 2014, 10.05 – 10.40

**** Electronic vote ****

5. **Combating Violence Against Women**
LIBE/7/14404
2013/2004(INL)

Rapporteur for the opinion: Roberta Angelilli (PPE) — PA – PE524.504v01-00, AM – PE524.778v01-00

Responsible: FEMM – Antonyia Parvanova (ADLE) — PR – PE522.850v01-00, AM – PE524.683v01-00, AM – PE524.579v01-00, DT – PE516.665v01-00

- Adoption of draft opinion

6. **High common level of network and information security across the Union**
LIBE/7/11963
***I 2013/0027(COD) COM(2013)0048 – C7-0035/2013

Rapporteur for the opinion: Carl Schlyter (Verts/ALE) — PA – PE514.755v01-00, AM – PE521.696v01-00

Responsible: IMCO* – Andreas Schwab (PPE) — PR – PE514.882v01-00, AM – PE519.685v01-00

- Adoption of draft report and of the decision to enter into negotiations with Council (rule 70)

7. **General provisions - Asylum and Migration Fund and Internal Security Fund**
LIBE/7/07982
***I 2011/0367(COD) COM(2011)0752 – C7-0444/2011

Rapporteur: Lorenzo Fontana (EFD) — PR – PE489.460v02-00, AM – PE494.863v05-00

Responsible: LIBE –
Opinions: BUDG – Monika Hohlmeier (PPE) — AD – PE492.552v02-00, AM – PE494.562v01-00

- Adoption of draft report

8. **Internal Security Fund - External borders and visas**
LIBE/7/07972
***I 2011/0365(COD) COM(2011)0750 – C7-0441/2011

Rapporteur: Marian-Jean Marinescu (PPE)

PR – PE489.446v02-00
AM – PE496.290v01-00
CM – PE501.980v01-00

Responsible: LIBE –
Opinions: AFET – Hélène Flautre (Verts/ALE)

AD – PE489.432v02-00
AM – PE491.259v01-00

DEVE – Decision: no opinion
BUDG – Monika Hohlmeier (PPE)

AD – PE492.555v02-00
AM – PE494.565v01-00

EMPL – Decision: no opinion

- Adoption of draft report

9. Internal Security Fund - Police cooperation, preventing and combating crime and crisis management

LIBE/7/07985
***I 2011/0368(COD) COM(2011)0753 – C7-0445/2011

Rapporteur: Salvatore Iacolino (PPE)

PR – PE491.240v01-00
AM – PE494.833v03-00
CM – PE501.981v01-00
CM – PE502.026v01-00

Responsible: LIBE –
Opinions: BUDG – Dominique Riquet (PPE)

AD – PE492.554v02-00
AM – PE494.564v01-00

- Adoption of draft report

10. Asylum and Migration Fund

LIBE/7/07977
***I 2011/0366(COD) COM(2011)0751 – C7-0443/2011

Rapporteur: Sylvie Guillaume (S&D)

PR – PE491.289v01-00
AM – PE494.640v02-00
CM – PE501.991v01-00

Responsible: LIBE –
Opinions: AFET – Sophocles Sophocleous (S&D)

AD – PE487.900v02-00
AM – PE491.116v01-00

DEVE – Michèle Striffler (PPE)

AD – PE489.591v02-00
AM – PE492.944v01-00

BUDG – Monika Hohlmeier (PPE)

AD – PE492.558v02-00
AM – PE494.560v02-00

EMPL – Decision: no opinion

- Adoption of draft report

*** ***End of electronic vote*** ***

9 January 2014, 10.40 – 11.00

11. Third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement
LIBE/7/14678
***I 2013/0415(COD) COM(2013)0853 – C7-0430/2013

Rapporteur: Tanja Fajon (S&D)
Responsible: LIBE –
Opinions: AFET –

- Consideration of draft report
- Decision on deadline for tabling amendments

9 January 2014, 11.00 – 12.30

Joint debate (art. 51) with ECON committee in meeting room József Antall (4Q1)

(see also separate draft agenda)

12. Prevention of the use of the financial system for the purpose of money laundering and terrorist financing
CJ12/7/14261
***I 2013/0025(COD) COM(2013)0045 – C7-0032/2013

Rapporteurs	Krišjānis Kariņš (PPE) Judith Sargentini (Verts/ALE)		PR – PE523.003v01-00 AM – PE524.801v02-00 AM – PE524.784v02-00
Responsible:	ECON, LIBE –		
Opinions:	DEVE –	Bill Newton Dunn (ADLE)	AD – PE514.725v02-00 AM – PE516.924v01-00
	IMCO – Decision: no opinion		
	JURI –	Antonio López-Istúriz White (PPE)	AD – PE516.897v02-00 AM – PE519.758v01-00
	PETI – Decision: no opinion		

13. Information accompanying transfers of funds
CJ12/7/14263
***I 2013/0024(COD) COM(2013)0044 – C7-0034/2013

Rapporteurs	Mojca Kleva Kekuš (S&D) Timothy Kirkhope (ECR)		PR – PE523.016v01-00 AM – PE524.701v01-00
Responsible:	ECON, LIBE –		
Opinions:	DEVE –	Nirj Deva (ECR)	AD – PE516.643v02-00 AM – PE516.923v01-00
	IMCO – Decision: no opinion		
	JURI –	Tadeusz Zwiefka (PPE)	AD – PE519.491v02-00 AM – PE521.631v01-00
	PETI – Decision: no opinion		

- Consideration of amendments

9 January 2014, 14.00 – 15.00

Possibly

14. The US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs
LIBE/7/13778
2013/2188(INI)

Rapporteur: Claude Moraes (S&D)

DT – PE524.632v01-00
DT – PE524.799v01-00
DT – PE523.025v01-00
DT – PE524.633v01-00

Responsible: LIBE –
Opinions: AFET – Decision: no opinion
INTA – Decision: no opinion
ITRE –

- Consideration of draft report
- Decision on deadline for tabling amendments

9 January 2014, 15.00 – 15.30

15. European single market for electronic communications
LIBE/7/13789
***I 2013/0309(COD) COM(2013)0627 – C7-0267/2013

Rapporteur for the opinion: Salvador Sedó i Alabart (PPE) — PA – PE523.069v01-00

Responsible: ITRE* – Pilar del Castillo Vera (PPE) — PR – PE522.762v01-00

- Consideration of draft opinion

16. Any other business

17. Next meeting(s)

- 13 January 2014 (Strasbourg)

Klostermeyer, Karin

000092

Von: transfer@bnd.bund.de
Gesendet: Freitag, 10. Januar 2014 09:34
An: Klostermeyer, Karin
Betreff: WG: EILT! Mail an BK-Amt, hier: Anfrage zu Berichterstattung zum
Anlagen: Schreiben_CommitteLIBE.pdf

Mit freundlichen Grüßen

IT-Leitstand

An das
Bundeskanzleramt
Frau Klostermeyer
- o.V.i.A. -

11012 Berlin

Sehr geehrte Frau Klostermeyer,
ergänzend zu der gestrigen E-Mail (s.u.) bzgl. der Medienberichte zum Entwurf des Berichts des LIBE Committees sende ich Ihnen im Auftrag von Leiter PLS folgende Informationen für die heutige Regierungs-PK:

Entgegen gestriger Medienberichte und der Informationen im Berichtsentwurf des "Committee on Civil Liberties, Justice and Home Affairs" erfolgte am 20. November 2013 durch Präsident Schindler eine Antwort auf die Einladung des LIBE Committee. In diesem Antwortschreiben begrüßt Präsident Schindler ausdrücklich die Arbeit und Zielsetzung des Komitees, wenngleich er die konkrete Einladung nicht annehmen konnte.

Hinsichtlich den eigentlichen Inhalten des Berichtes erhalten Sie schnellstmöglich weitere Informationen über die Kollegen von PLSA.

Mit freundlichen Grüßen
K[redacted] H[redacted]
PLSE, Tel. 8[redacted]

-------- Original-Nachricht --------

Betreff: Reaktion auf Berichterstattung zum LIBE Committee

Datum: Thu, 09 Jan 2014 17:48:03 +0100

Von: Pressestelle BND <Pressestelle@bundesnachrichtendienst.de>

An: "Schäper, Hans-Jörg" <Hans-Joerg.Schaeper@bk.bund.de>,
albert.karl@bk.bund.de,
margit.lampe@bk.bund.de

Sehr geehrter Herr Schäper,
sehr geehrter Herr Karl,

im Auftrag von Herrn S[redacted] sende ich Ihnen folgende Informationen zur heutigen Berichterstattung bzgl. des LIBE Committees:

Zur Richtigstellung der Berichterstattung über eine fehlende Antwort des Präsident BND auf die Einladung des LIBE Committees wurden die entsprechenden Journalisten der Welt, der Zeit und der dpa kontaktiert und über die erfolgte Antwort informiert. Im Anschluss daran erhielten die Journalisten das Antwortschreiben in Kopie per E-Mail (siehe Anhang).

Mit freundlichen Grüßen
i.A. K[redacted] H[redacted]

--
Bundesnachrichtendienst
Presse- und Öffentlichkeitsarbeit
Gardeschützenweg 71 - 101
12203 Berlin
Tel.: 030/20 45 36 30
Fax: 030/20 45 36 31

www.bundesnachrichtendienst.de

(See attached file: Schreiben_CommitteLIBE.pdf)

Bundesnachrichtendienst

Gerhard Schindler
Präsident

20. November 2013

Herrn
Juan Fernando López Aguilar
Vorsitzender
Committee on Civil Liberties, Justice
and Home Affairs
Europäisches Parlament
Brüssel

Belgien

Sehr geehrter Herr López Aguilar,

zunächst bedanke ich mich für Ihr Schreiben vom 14. Oktober 2013, in dem sie mich zu einer Anhörung des von Ihnen geleiteten Komitees einladen.

Die Arbeit und Zielsetzung Ihres Komitees begrüße ich ausdrücklich; hierbei beziehe ich mich insbesondere auf die Wahrung der Rechte der EU – Bürgerinnen und – Bürger, die im Einklang mit der Europäischen Menschenrechtskonvention stehen. Diese wird in der Bundesrepublik Deutschland in höchstem Maße gewürdigt und selbstverständlich auch von den deutschen Nachrichtendiensten geachtet.

Die drei deutschen Nachrichtendienste sind dem deutschen Gesetz gegenüber verpflichtet und richten ihre Arbeit daran aus, dies gilt auch für den Umgang mit Informationen, die nicht selbst erhoben wurden. Das deutsche Parlament hat hierauf stets sein Augenmerk gerichtet und wird dies auch in Zukunft tun. Um dies zu gewährleisten, wurden geeignete Mechanismen entwickelt, wie Gremien zur Aufsicht, Kontrolle und Überwachung.

Auch wenn ich bedauerlicherweise Ihre Einladung nicht annehmen kann, wünsche ich Ihnen alles Gute und eine glückliche Hand für ihre Arbeit.

Mit freundlichen Grüßen

(Gerhard Schindler)

EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

LIBE(2014)0113_1

DRAFT AGENDA

Extraordinary meeting

Monday 13 January 2014, 19.00 – 21.30

Strasbourg

Room: Louise Weiss (N1.3)

1. **Adoption of agenda**

2. **Chair's announcements**

   PLEASE NOTE THAT ALL TIME SLOTS ARE ONLY INDICATIVE AND ARE SUBJECT TO CHANGE DURING THE MEETING!

13 January 2014, 19.00 – 21.00

**** Electronic vote ****

3. **The review of the European Arrest Warrant**
   LIBE/7/12924
   2013/2109(INL)

   Rapporteur: Baroness Sarah Ludford (ADLE)

   PR – PE522.805v02-00
   AM – PE524.766v02-00

   Responsible: LIBE –

   - Adoption of draft report

4. The situation of fundamental rights in the European Union (2012)
LIBE/7/12550
2013/2078(INI)

Rapporteur: Louis Michel (ADLE)

PR – PE519.501v01-00
AM – PE524.505v01-00
AM – PE521.653v01-00
DT – PE514.668v01-00
DT – PE514.669v02-00

Responsible: LIBE –
Opinions: EMPL – Ádám Kósa (PPE)

AD – PE519.701v02-00
AM – PE522.779v01-00

FEMM – Antigoni Papadopoulou (S&D)

AD – PE519.746v02-00
AM – PE521.841v01-00

PETI – Decision: no opinion

- Adoption of draft report

5. High common level of network and information security across the Union
LIBE/7/11963
***I 2013/0027(COD) COM(2013)0048 – C7-0035/2013

Rapporteur for the opinion: Carl Schlyter (Verts/ALE)

PA – PE514.755v01-00
AM – PE521.696v01-00

Responsible: IMCO* – Andreas Schwab (PPE)

PR – PE514.882v01-00
AM – PE519.685v01-00

- Adoption of draft opinion (Rule 50)

*** ***End of electronic vote*** ***

13 January 2014, 21.00 – 21.30

Possibly

6. The US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs
LIBE/7/13778
2013/2188(INI)

Rapporteur: Claude Moraes (S&D)

PR – PE526.085v01-00
DT – PE524.632v01-00
DT – PE523.025v02-00
DT – PE524.799v01-00
DT – PE524.633v01-00

Responsible: LIBE –
Opinions: AFET – Decision: no opinion
INTA – Decision: no opinion

ITRE –

- Consideration of draft report

7. **Any other business**

8. **Next meeting(s)**
   - 21 January 2014, 15.00 – 18.30 (Brussels)
   - 22 January 2014, 9.00 – 12.30 and 15.00 – 18.30 (Brussels)
   - 23 January 2014, 9.00 – 12.30 and 15.00 – 18.30 (Brussels)

Neist, Dennis

Von: Neist, Dennis
Gesendet: Dienstag, 14. Januar 2014 11:44
An: 'leitung-lage@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Anlagen: LIBE_Committee_DraftReport_NSA_Surveillance.pdf

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted],

mit Blick auf den o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs (LIBE-Bericht) wird BND zur Unterrichtung des StS Fritsche um eine Einschätzung und Bewertung - insbesondere hinsichtlich möglicher Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen - gebeten.

LIBE_Committee_DraftReport_NSA...

Für eine Rückäußerung bis 16. Januar 2014, DS wären wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Neist, Dennis

Von: Neist, Dennis
Gesendet: Dienstag, 14. Januar 2014 13:05
An: 'PGNSA@bmi.bund.de'
Cc: ref603; 'OeSI3AG@bmi.bund.de'; ref132
Betreff: Bitte um Einschätzung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Anlagen: 20140108_LIBE-Bericht_DRAFT.doc

Sehr geehrte Damen und Herren,

St Frische bittet um eine Einschätzung und Bewertung insbesondere zu möglichen Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen zum o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs.



20140108_LIBE-Ber
icht_DRAFT.do...

Für eine Antwort bis 16. Januar 2014, DS sind wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Neist, Dennis

An: Ulrich.Weinbrenner@bmi.bund.de

Cc: Johannes.Dimroth@bmi.bund.de; PGNSA@bmi.bund.de; Gregor.Kutzschbach@bmi.bund.de; ref603; ref132

Betreff: AW: Bitte um Einschätzung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Sehr geehrter Herr Weinbrenner,

besten Dank für Ihre Rückmeldung und den Hinweis auf die im BMI ohenhin in Bearbeitung befindliche Stellungnahme zum o.a. Berichtsentwurf.
Gerne greife ich Ihr Angebot auf, diese Stellungnahme bis zum 17.01.14 zu erhalten.

Vielen Dank.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Ulrich.Weinbrenner@bmi.bund.de [mailto:Ulrich.Weinbrenner@bmi.bund.de]
Gesendet: Dienstag, 14. Januar 2014 13:42
An: Neist, Dennis
Cc: Johannes.Dimroth@bmi.bund.de; PGNSA@bmi.bund.de; Gregor.Kutzschbach@bmi.bund.de
Betreff: AW: Bitte um Einschätzung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Sehr geehrter Herr Neist,

wir sind im BMI aufgefordert, bis 17.Januar zu dem Berichtsentwurf Stellung zu nehmen. Ich gehe davon aus, dass Ihnen geholfen ist, wenn wir Ihnen die Stellungnahme dann zuleiten.

Mit freundlichem Gruß

Ulrich Weinbrenner
Bundesministerium des Innern
Leiter der Arbeitsgruppe ÖS I 3
Polizeiliches Informationswesen, BKA-Gesetz,
Datenschutz im Sicherheitsbereich
Tel.: + 49 30 3981 1301
Fax.: + 49 30 3981 1438
PC-Fax.: 01888 681 51301
Ulrich.Weinbrenner@bmi.bund.de

14.01.2014

Von: Neist, Dennis [mailto:Dennis.Neist@bk.bund.de]
Gesendet: Dienstag, 14. Januar 2014 13:05
An: PGNSA
Cc: ref603; OESI3AG_; ref132
Betreff: Bitte um Einschätzung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Sehr geehrte Damen und Herren,

St Frische bittet um eine Einschätzung und Bewertung insbesondere zu möglichen Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen zum o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs.

Für eine Antwort bis 16. Januar 2014, DS sind wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Maas, Carsten

Von: Semmler, Jörg
Gesendet: Dienstag, 14. Januar 2014 16:12
An: Heusgen, Christoph; Maas, Carsten; Schäper, Hans-Jörg
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA
Anlagen: moraes_1014703_en.pdf
Zur (vertraulichen) Kenntnis, JS

Von: VOSS Axel [mailto:axel.voss@europarl.europa.eu]
Gesendet: Freitag, 10. Januar 2014 18:16
An: Semmler, Jörg
Betreff: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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" mit der Bitte um Weiterleitung an Herrn BM Peter Altmaier.

Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Herr Voss hat mich vor allem darum gebeten, Herrn MB Altmaier auf folgende Absätze hinzuweisen: Absatz 2 (Seite 16); Absatz 10 (Seite 17); Absatz 20 (Seite19).

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

Neist, Dennis

000103

Von: Neist, Dennis
Gesendet: Mittwoch, 15. Januar 2014 09:57
An: 'leitung-lage@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted]

in Erweiterung der u.a. Anfrage wird BND gebeten neben der angefragten Einschätzung/Bewertung zusätzlich Ideen oder Anregungen für Änderungsvorschläge in Bezug auf den Berichtsentwurf mitzuteilen - dies gilt insbesondere für die Textpassagen Absatz 2 (Seite 16), Absatz 10 (Seite 17) und Absatz 20 (Seite19) im Abschnitt 'Main findings'.

Die u.a. Terminsetzung bleibt bestehen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Neist, Dennis
Gesendet: Dienstag, 14. Januar 2014 11:44
An: 'leitung-lage@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted]

mit Blick auf den o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs (LIBE-Bericht) wird BND zur Unterrichtung des StS Fritsche um eine Einschätzung und Bewertung - insbesondere hinsichtlich möglicher Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen - gebeten.

(Anhang gelöscht)

Für eine Rückäußerung bis 16. Januar 2014, DS wären wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

000104

Neist, Dennis

000105

Von: transfer@bnd.bund.de
Gesendet: Donnerstag, 16. Januar 2014 17:38
An: Neist, Dennis
Cc: ref603
Betreff: WG: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Jome Affairs zum NSA Überwachungsprogramm (2013/2188(INI))
Anlagen: 140116_Pr-LIBE-Ausschuss_Reaktion auf Draft Report.pdf

---

Betr.: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
hier: Stellungnahme
Bezug: E-Mails BKAmt, Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD, vom 14. und 15. Januar 2014

Sehr geehrter Herr Neist,

mit Bezug hatten Sie hinsichtlich des vorgenannten Berichts um einen Einschätzung und Bewertung auch zu möglichen Auswirkungen der durch das Komitee vorgeschlagenen Maßnahmen gebeten. Darüber hinaus hatten Sie um Mitteilung von Ideen oder Anregungen für Änderungsvorschläge bzgl. des Berichtsentwurfs gebeten. Hierzu kann ich Folgendes mitteilen:

Der Berichtsentwurf stellt die Vermutung auf, der BND betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu ist festzustellen, dass für einen solchen Vergleich die Grundlage fehlt. Die Aktivitäten der NSA sind seit dem vergangenen Sommer Gegenstand medialer Berichterstattung. Unterstellt wird dabei, dass die NSA Daten von Bürgerinnen und Bürgern der EU anlasslos und massenhaft in einem den Zweck der Terrorismusabwehr übersteigenden Maß sammelt und speichert. Für den Bundesnachrichtendienst ist festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetzt.

Der Präsident des Bundesnachrichtendienstes hat heute das beigefügte Schreiben an den Vorsitzenden des LIBE-Ausschusses gerichtet. Darüber hinaus besteht beim Bundesnachrichtendienst kein weiterer fachlicher Änderungs- oder Kommentierungsbedarf hinsichtlich des Berichtsentwurfs.

(See attached file: 140116_Pr-LIBE-Ausschuss_Reaktion auf Draft Report.pdf)

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]

-----Weitergeleitet von leitung-lage IVBB-BND-BIZ/BIZDOM am 15.01.2014 10:02 -----
An: "'leitung-lage@bnd.bund.de'" <leitung-lage@bnd.bund.de>
Von: "Neist, Dennis" <Dennis.Neist@bk.bund.de>
Datum: 15.01.2014 09:57
Kopie: ref603 <ref603@bk.bund.de>
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm

(2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted],

in Erweiterung der u.a. Anfrage wird BND gebeten neben der angefragten Einschätzung/Bewertung zusätzlich Ideen oder Anregungen für Änderungsvorschläge in Bezug auf den Berichtsentwurf mitzuteilen - dies gilt insbesondere für die Textpassagen Absatz 2 (Seite 16), Absatz 10 (Seite 17) und Absatz 20 (Seite19) im Abschnitt 'Main findings'.

Die u.a. Terminsetzung bleibt bestehen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Neist, Dennis
Gesendet: Dienstag, 14. Januar 2014 11:44
An: 'leitung-lage@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted],

mit Blick auf den o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs (LIBE-Bericht) wird BND zur Unterrichtung des StS Fritsche um eine Einschätzung und Bewertung - insbesondere hinsichtlich möglicher Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen - gebeten..

(Anhang gelöscht)

Für eine Rückäußerung bis 16. Januar 2014, DS wären wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen

Im Auftrag

000107

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Neist, Dennis

Von: Neist, Dennis
Gesendet: Freitag, 17. Januar 2014 11:04
An: 'leitung-grundsatz@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Übersendung - Einladungsschreibens des LIBE-Ausschuss an BND vom 14.10.2013

Leitungsstab
PLSA
z.Hd. Herrn Dr. K[redacted] o.V.i.A.
Az. 603 - 151 00 Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr Dr. K[redacted]

ich danke für die mit u.a. Mail von Fr. F[redacted] übermittelte Stellungnahme des BND zum LIBE-Bericht.

Zur Komplettierung des Vorgangs wird - wie telefonisch bereits angekündigt - um zeitnahe Übermittlung des Einladungsschreibens des LIBE-Ausschussvorsitzenden an Herrn Pr BND vom 14.10.2013 gebeten.

Für eine Rückäußerung bis 17. Januar 2014, 12:00 Uhr wären wir dankbar.

Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: transfer@bnd.bund.de [mailto:transfer@bnd.bund.de]
Gesendet: Donnerstag, 16. Januar 2014 17:38
An: Neist, Dennis
Cc: ref603
Betreff: WG: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Jome Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Betr.: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
hier: Stellungnahme
Bezug: E-Mails BKAmt, Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD, vom 14. und 15. Januar 2014

17.01.2014

Sehr geehrter Herr Neist,

mit Bezug hatten Sie hinsichtlich des vorgenannten Berichts um einen Einschätzung und Bewertung auch zu möglichen Auswirkungen der durch das Komitee vorgeschlagenen Maßnahmen gebeten. Darüber hinaus hatten Sie um Mitteilung von Ideen oder Anregungen für Änderungsvorschläge bzgl. des Berichtsentwurfs gebeten. Hierzu kann ich Folgendes mitteilen:

Der Berichtsentwurf stellt die Vermutung auf, der BND betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu ist festzustellen, dass für einen solchen Vergleich die Grundlage fehlt. Die Aktivitäten der NSA sind seit dem vergangenen Sommer Gegenstand medialer Berichterstattung. Unterstellt wird dabei, dass die NSA Daten von Bürgerinnen und Bürgern der EU anlasslos und massenhaft in einem den Zweck der Terrorismusabwehr übersteigenden Maß sammelt und speichert. Für den Bundesnachrichtendienst ist festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetzt.

Der Präsident des Bundesnachrichtendienstes hat heute das beigefügte Schreiben an den Vorsitzenden des LIBE-Ausschusses gerichtet. Darüber hinaus besteht beim Bundesnachrichtendienst kein weiterer fachlicher Änderungs- oder Kommentierungsbedarf hinsichtlich des Berichtsentwurfs.

(See attached file: 140116_Pr-LIBE-Ausschuss_Reaktion auf Draft Report.pdf)

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]

-----Weitergeleitet von leitung-lage IVBB-BND-BIZ/BIZDOM am 15.01.2014 10:02 -----
An: "'leitung-lage@bnd.bund.de'" <leitung-lage@bnd.bund.de>
Von: "Neist, Dennis" <Dennis.Neist@bk.bund.de>
Datum: 15.01.2014 09:57
Kopie: ref603 <ref603@bk.bund.de>
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted],

in Erweiterung der u.a. Anfrage wird BND gebeten neben der angefragten Einschätzung/Bewertung zusätzlich Ideen oder Anregungen für Änderungsvorschläge in Bezug auf den Berichtsentwurf mitzuteilen - dies gilt insbesondere für die Textpassagen Absatz 2 (Seite 16), Absatz 10 (Seite 17) und Absatz 20 (Seite19) im Abschnitt 'Main findings'.

Die u.a. Terminsetzung bleibt bestehen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist

MAT A BK-1-4s.pdf, Blatt 123

Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Neist, Dennis
Gesendet: Dienstag, 14. Januar 2014 11:44
An: 'leitung-lage@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted]

mit Blick auf den o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs (LIBE-Bericht) wird BND zur Unterrichtung des StS Fritsche um eine Einschätzung und Bewertung - insbesondere hinsichtlich möglicher Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen - gebeten..

(Anhang gelöscht)

Für eine Rückäußerung bis 16. Januar 2014, DS wären wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

MAT A BK-1-4s.pdf, Blatt 124

Neist, Dennis

Von: transfer@bnd.bund.de
Gesendet: Freitag, 17. Januar 2014 11:10
An: Neist, Dennis
Cc: ref603
Betreff: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
Anlagen: 131014_Einladung.pdf

Betr.: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
hier: Übersendung der Einladung zur Anhörung
Bezug: laufender Vorgang; zuletzt: E-Mail BND/Frau F[redacted] vom 16. Januar 2014

Sehr geehrter Herr Neist,

anliegend lasse ich Ihnen in vorgenannter Angelegenheit die ursprüngliche Einladung des LIBE-Committees zur Anhörung des Präsidenten des BND mit der Bitte um Kenntnisnahme zukommen. Die Einladung ist im BND per E-Mail am 14. Oktober 2013 eingegangen.

(See attached file: 131014_Einladung.pdf)

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]

ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA 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

Committee on Civil Liberties, Justice and Home Affairs
The Chairman

Gerhard Schindler
Präsident des Bundesnachrichtendienstes

Subject: ***LIBE Committee Inquiry on Electronic mass surveillance of EU citizens***

Dear Mr Schindler,

As you are probably aware, the European Parliament, in its Resolution of 4 July 2013, instructed the LIBE Committee to conduct an inquiry on US NSA surveillance programmes, surveillance bodies in various Member States and their impact on EU citizens' privacy and to report its findings to the plenary of the European Parliament by the end of 2013.

The LIBE Committee is currently holding several hearings to highlight and investigate this important issue from different angles. Therefore, the LIBE Committee is inviting representatives from a select number of national intelligence agencies to share with the Committee their experiences on national level.

I would like to invite you to appear before the LIBE Committee Inquiry on 17 October (15-18.30), 7 November (9-11.30 and 15-18.30) or 11 November (15-18.30) 2013. The hearings will take place in the European Parliament in Brussels. Should it prove difficult for you to attend the hearing in person, your participation by way of videoconference would be highly appreciated.

The participation to this LIBE Committee inquiry should be considered as a priority for all EU institutions, bodies and Member States in order to enlighten EU citizens as to the scope and impact of mass surveillance programmes by intelligence services and to the role parliaments should play in ensuring proper democratic oversight and control. I therefore believe that your presence to one of the above mentioned hearings is very important.

The LIBE Secretariat would be happy to try to find the most suitable timing for your participation in order to accommodate as much as possible your diary.

Yours sincerely,

Juan Fernando LÓPEZ AGUILAR

CC: Peter Tempel, Permanent Representative, Permanent Representation of Germany to the EU

B-1047 Bruxelles - Tel +32 2 28 43508 - Fax 0032 2 28 44941
F-67070 Strasbourg - Tel +33 3 88 1 74022 - Fax 0033 3 88 1 79040

Bundeskanzleramt

VS – NUR FÜR DEN DIENSTGEBRAUCH

000113

1. Vfg.

Bundeskanzleramt, 11012 Berlin

per Kryptofax

Bundesnachrichtendienst
Leiter Leitungsstab
z.Hd. Herrn S[redacted] o.V.i.A.
Gardeschützenweg 71 – 101

12171 Berlin

Albert Karl
Referatsleiter 603

HAUSANSCHRIFT Willy-Brandt-Straße 1, 10557 Berlin
POSTANSCHRIFT 11012 Berlin

TEL +49 30 18 400-2627
FAX +49 30 18 10 400-2627
E-MAIL albert.karl@bk.bund.de

Berlin, 17. Januar 2014

BETREFF Unterrichtung des BKAmtes

AZ 603 – 151 19 – Co 1/14 VS-NfD

BEZUG Schreiben Pr BND an den LIBE-Vorsitzenden des EU-Parlaments vom 20. November 2013

Sehr geehrter Herr S[redacted]

um eine frühzeitige und umfassende Kenntnis des Bundeskanzleramtes zu gewährleisten, wird gebeten, BND-Äußerungen bzw. - Stellungnahmen gegenüber nationalen und internationalen Organen und Gremien grundsätzlich im Vorfeld der Herausgabe dem BKAmt zur Freigabe schriftlich 2 vorzulegen. Dies betrifft auch Sprachregelungen, die der Presse zur Verfügung gestellt werden.

Mit freundlichen Grüßen
Im Auftrag

(Albert Karl)

2. Über
   Herrn StäV AL 6
   Herrn AL 6 mit der Bitte um Billigung
3. WV 603 / ab
4. Herrn Staatssekretär mit der Bitte um Kenntnisnahme
5. WV 603
6. RL 601, 602, 604, 605 z.g.K.
7. WV 603

Bundeskanzleramt

VS – NUR FÜR DEN DIENSTGEBRAUCH

Kopie von _____ Ausf.
INFOTEC-Kontr. Nr. - 26 -
Ausg.: 17.01.14 Zeit: 11.20

Bundeskanzleramt, 11012 Berlin

Albert Karl
Referatsleiter 603

HAUSANSCHRIFT Willy-Brandt-Straße 1, 10557 Berlin
POSTANSCHRIFT 11012 Berlin

TEL +49 30 18 400-2627
FAX +49 30 18 10 400-2627
E-MAIL albert.karl@bk.bund.de

per Kryptofax

Bundesnachrichtendienst
Leiter Leitungsstab
z.Hd. Herrn S[redacted] o.V.i.A.
Gardeschützenweg 71 – 101

12171 Berlin

Berlin, 17. Januar 2014

BETREFF Unterrichtung des BKAmtes

AZ 603 – 151 19 – Co 1/14 VS-NfD 3a 10 NA 2

BEZUG Schreiben Pr BND an den LIBE-Vorsitzenden des EU-Parlaments vom 20. November 2013

Sehr geehrter Herr S[redacted]

um eine frühzeitige und umfassende Kenntnis des Bundeskanzleramtes zu gewährleisten, wird gebeten, BND-Äußerungen bzw. - Stellungnahmen gegenüber nationalen und internationalen Organen und Gremien grundsätzlich im Vorfeld der Herausgabe dem BKAmt zur Freigabe vorzulegen. Dies betrifft auch Sprachregelungen, die der Presse zur Verfügung gestellt werden.

Mit freundlichen Grüßen
Im Auftrag

(Albert Karl)

17. JAN. 2014 11:20 BUNDESKANZLERAMT BND LEITUNGSSTAB 7 Jan 2014 11:25 NR. 462 S. 1 S. 1

Kryptobetriebsstelle im Bundeskanzleramt

Kontrollblatt „Kryptofax-Ausgang" → Bitte per Kryptofax sofort zurück an 03018/400–1461 (–1451)

Absender:	Bundeskanzleramt	**Datum:**	17.01.14
Tgb. Nr. oder Aktenzeichen:	603-15119-Co 1114 VS-NfD	**Blattzahl (ohne Kontrollblatt):**	-01-
Ausgangs-Nr.:	-26-	**Blattzahl → GEHEIM:**	/
Empfänger:	BND LStab K. [redacted] o.V.i.A.	**Blattzahl → VS-Vertraulich:**	/
		Blattzahl → VS-NfD:	-01-
		Blattzahl → offen / verschlüsselt:	/

Empfangsbestätigung:

Datum:	17.01.14
Name:	Reg. / PLS Heb.
Eingangs-Nr.:	0010/14

EILT ! Sofort auf den Tisch ☐

BK-Amt VS-Reg. erhalten:

Datum:	
Name:	

Vielen Dank! Für telefonische Rückfragen erreichen Sie uns unter: 03018/400-1400

MAT A BK-1-4s.pdf, Blatt 129

VS-Nur für den Dienstgebrauch

000117

Referat 603

Berlin, 17. Januar 2014

603 - 151 00 – Bu 10/14 NA 2 VS-NfD

ORR Neist

Hausruf: 2662

1. Vfg.

Über

Herrn Referatsleiter 603

Herrn Ständigen Vertreter AL 6

Herrn Abteilungsleiter 6

Herrn Staatssekretär

Betr.: Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) zum NSA Überwachungsprogramm
hier: Stellungnahme und Einschätzung des BND

Anlage: 1. Stellungnahme des BND vom 16.Januar 2014
2. Schreiben Pr BND an Vorsitzenden LIBE-Ausschuss vom 16. Januar 2014
3. Email Büro MdEP Voss an Herrn Dr. Semmler vom 10. Januar 2014
4. Einladungsschreiben LIBE-Ausschuss an Pr BND vom 14. Oktober 2013
5. Schreiben Pr BND an Vorsitzenden LIBE-Ausschuss vom 20. November 2013

I. Votum

[Kenntnisnahme] und Befassung ChBK

II. Sachverhalt

Im Zuge des Bekanntwerdens der globalen Aufklärungsaktivitäten der NSA hat das Europäische Parlament per Entschließungsantrag am 04. Juli 2013 eine

...

Arbeitsgruppe im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet und damit beauftragt, zur großflächigen elektronischen Aufklärung gegen EU Bürger und Einrichtungen durch die amerikanischen Nachrichtendienste zu berichten. Zu den 15 Anhörungen wurden u.a. Experten aus den USA und der EU geladen und befragt. Auch der Präsident des BND wurde mit Schreiben vom 14. Oktober 2013 (Anlage 4) zur Stellungnahme geladen, kommunizierte mit Schreiben vom 20. November 2013, dass er dieser jedoch nicht Folgen leisten könne (Anlage 5).

Die Ergebnisse der Untersuchung sowie daraus abgeleitete Handlungsmaßgaben wurden in einem ersten Vorabbericht im Dezember 2013 veröffentlicht. Wesentliche Textteile des Berichts befassen sich mit den großflächigen Überwachungsansätzen der NSA insbesondere mit Blick auf die Gewinnung der Daten von EU-Bürgern und EU-Einrichtungen. Im Berichtsentwurf wird mit deutlich kritischen Worten zum Ausdruck gebracht, dass die massenhafte Erhebung solcher Daten durch US-Dienste ausschließlich zur Terrorbekämpfung unwahrscheinlich erscheint; vor diesem Hintergrund verstoße dieses Vorgehen gegen Gesetze und geschlossene Vereinbarungen. Neben der NSA werden in dem Bericht auch britische, französische, schwedische und deutsche Nachrichtendienste genannt und die Nutzung ähnlicher Praktiken unterstellt.

Der BND widersprach diesem Vorwurf bereits öffentlich mit dem Hinweis, seine Arbeit unter Achtung der EU-Menschenrechtskonvention, der Einhaltung der nationalen gesetzlichen Regelungen sowie der Kontrolle durch das deutsche Parlament durchzuführen.

Der Bericht kann nun durch Änderungsanträge mit Vorlage bis zum 22. Januar 2014 abgeändert werden. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar 2014 und anschließend eine Abstimmung im Plenum im März 2014 vor.

Eine Stellungnahme des BND zum Berichtsentwurf sowie die Vorlage von Änderungsvorschlägen wurden – insbesondere mit Blick auf mögliche

...

Auswirkungen auf die Außenwirkung und die Aufklärungsfähigkeit des BND – durch BKAmt erbeten.

Der BND teilt in seiner Stellungnahme mit, dass der Berichtsentwurf die Vermutung anstelle, der BND betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu sei festzustellen, dass für einen solchen Vergleich die Grundlage fehle. Die Aktivitäten der NSA seien seit dem vergangenen Sommer Gegenstand medialer Berichterstattung. Unterstellt würde dabei, dass die NSA Daten von Bürgerinnen und Bürgern der EU anlasslos und massenhaft in einem den Zweck der Terrorismusabwehr übersteigenden Maß sammele und speichere. Für den BND sei festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetze.
Im Weiteren teilt BND mit, dass der Präsident des BND am 16.01.2014 bereits ein Schreiben an den Vorsitzenden des LIBE-Ausschusses gerichtet hat (Anlage 2). In diesem Schreiben – welches hier vor Absenden nicht vorgelegen hat – wird durch Pr BND darauf hingewiesen, dass zwei Aspekte im Berichtsentwurf nicht zutreffend seien und einer Änderung bedürfen. Dies beziehe sich zum Einen auf den o.a. Aspekt, dass der BND ein technisches Überwachungsprogramm zur massenhaften Ausspähung der Daten von EU-Bürgern betreibe und zum Anderen auf die Aussage, dass Pr BND unter jenen Akteuren aufgeführt wäre, welche nicht auf die Einladung des LIBE-Komitees reagiert hätten.

Darüber hinaus meldet der BND in seiner Stellungnahme gegenüber dem Bundeskanzleramt allerdings keinen weiteren fachlichen Änderungs- oder Kommentierungsbedarf an. Konkrete Änderungsvorschläge hat der BND nicht übersandt.

Das BMI wurde gebeten, eine eigenständige Stellungnahme zum LIBE-Bericht anzufertigen.

...

III. Bewertung

Zur flankierenden formalen Unterstützung des Ansinnens des BND, die in seinem Schreiben vom 16.01.2014 genannten nicht zutreffenden Aussagen im Berichtsentwurf zu ändern, sollte durch ChBK die Möglichkeit der Einbringung einer formalen Änderungsvorlage in Betracht gezogen werden.
Der formale Änderungsvorschlag gemäß Nachricht von Herrn MdEP Voss an Herrn Dr. Semmler vom 10. Januar 2014 ist bis 22. Januar 2014 an Herrn MdEP Voss zu übermitteln. Dazu sollte der BND konkrete Vorschläge erarbeiten.

Referat 601 hat mitgezeichnet.

(Dennis Neist)

2. 601 m.d.B. um Ergänzung und Mitzeichnung
3. ab
4. WV 603

VS-Nur für den Dienstgebrauch

Referat 603

603 - 151 00 – Bu 10/14 NA 2 VS-NfD

ORR Neist

Berlin, 17. Januar 2014

Hausruf: 2662

an StF am 20.1.14/
La

Über

Herrn Referatsleiter 603 17/1

Herrn Ständigen Vertreter AL 6

Herrn Abteilungsleiter 6

i.V.

Herrn Staatssekretär

Betr.: Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) zum NSA Überwachungsprogramm
hier: Stellungnahme und Einschätzung des BND

Anlage: 1. Stellungnahme des BND vom 16.Januar 2014
2. Schreiben Pr BND an Vorsitzenden LIBE-Ausschuss vom 16. Januar 2014
3. Email Büro MdEP Voss an Herrn Dr. Semmler vom 10. Januar 2014
4. Einladungsschreiben LIBE-Ausschuss an Pr BND vom 14. Oktober 2013
5. Schreiben Pr BND an Vorsitzenden LIBE-Ausschuss vom 20. November 2013

I. Votum

[Kenntnisnahme] und Befassung ChBK

Billigung

II. Sachverhalt

Im Zuge des Bekanntwerdens der globalen Aufklärungsaktivitäten der NSA hat das Europäische Parlament per Entschließungsantrag am 04. Juli 2013 eine Arbeitsgruppe im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz

...

und Inneres (LIBE) eingerichtet und damit beauftragt, zur großflächigen elektronischen Aufklärung gegen EU Bürger und Einrichtungen durch die amerikanischen Nachrichtendienste zu berichten. Zu den 15 Anhörungen wurden u.a. Experten aus den USA und der EU geladen und befragt. Auch der Präsident des BND wurde mit Schreiben vom 14. Oktober 2013 (Anlage 4) zur Stellungnahme geladen, kommunizierte mit Schreiben vom 20. November 2013, dass er dieser jedoch nicht Folgen leisten könne (Anlage 5).

Die Ergebnisse der Untersuchung sowie daraus abgeleitete Handlungsmaßgaben wurden in einem ersten Vorabbericht im Dezember 2013 veröffentlicht. Wesentliche Textteile des Berichts befassen sich mit den großflächigen Überwachungsansätzen der NSA insbesondere mit Blick auf die Gewinnung der Daten von EU-Bürgern und EU-Einrichtungen. Im Berichtsentwurf wird mit deutlich kritischen Worten zum Ausdruck gebracht, dass die massenhafte Erhebung solcher Daten durch US-Dienste ausschließlich zur Terrorbekämpfung unwahrscheinlich erscheint; vor diesem Hintergrund verstoße dieses Vorgehen gegen Gesetze und geschlossene Vereinbarungen. Neben der NSA werden in dem Bericht auch britische, französische, schwedische und deutsche Nachrichtendienste genannt und die Nutzung ähnlicher Praktiken unterstellt.

Der BND widersprach diesem Vorwurf bereits öffentlich mit dem Hinweis, seine Arbeit unter Achtung der EU-Menschenrechtskonvention, der Einhaltung der nationalen gesetzlichen Regelungen sowie der Kontrolle durch das deutsche Parlament durchzuführen.

Der Bericht kann nun durch Änderungsanträge mit Vorlage bis zum 22. Januar 2014 abgeändert werden. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar 2014 und anschließend eine Abstimmung im Plenum im März 2014 vor.

Eine Stellungnahme des BND zum Berichtsentwurf sowie die Vorlage von Änderungsvorschlägen wurden – insbesondere mit Blick auf mögliche

...

Auswirkungen auf die Außenwirkung und die Aufklärungsfähigkeit des BND – durch BKAmt erbeten.

Der BND teilt in seiner Stellungnahme mit, dass der Berichtsentwurf die Vermutung anstelle, der BND betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu sei festzustellen, dass für einen solchen Vergleich die Grundlage fehle. Die Aktivitäten der NSA seien seit dem vergangenen Sommer Gegenstand medialer Berichterstattung. Unterstellt würde dabei, dass die NSA Daten von Bürgerinnen und Bürgern der EU anlasslos und massenhaft in einem den Zweck der Terrorismusabwehr übersteigenden Maß sammele und speichere. Für den BND sei festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetze.
Im Weiteren teilt BND mit, dass der Präsident des BND am 16.01.2014 bereits ein Schreiben an den Vorsitzenden des LIBE-Ausschusses gerichtet hat (Anlage 2). In diesem Schreiben – welches hier vor Absenden nicht vorgelegen hat – wird durch Pr BND darauf hingewiesen, dass zwei Aspekte im Berichtsentwurf nicht zutreffend seien und einer Änderung bedürfen. Dies beziehe sich zum Einen auf den o.a. Aspekt, dass der BND ein technisches Überwachungsprogramm zur massenhaften Ausspähung der Daten von EU-Bürgern betreibe und zum Anderen auf die Aussage, dass Pr BND unter jenen Akteuren aufgeführt wäre, welche nicht auf die Einladung des LIBE-Komitees reagiert hätten.

Darüber hinaus meldet der BND in seiner Stellungnahme gegenüber dem Bundeskanzleramt allerdings keinen weiteren fachlichen Änderungs- oder Kommentierungsbedarf an. Konkrete Änderungsvorschläge hat der BND nicht übersandt.

Das BMI wurde gebeten, eine eigenständige Stellungnahme zum LIBE-Bericht anzufertigen.

...

VS-Nur für den Dienstgebrauch

III. Bewertung

Zur flankierenden formalen Unterstützung des Ansinnens des BND, die in seinem Schreiben vom 16.01.2014 genannten nicht zutreffenden Aussagen im Berichtsentwurf zu ändern, sollte durch ChBK die Möglichkeit der Einbringung einer formalen Änderungsvorlage in Betracht gezogen werden.
Der formale Änderungsvorschlag gemäß Nachricht von Herrn MdEP Voss an Herrn Dr. Semmler vom 10. Januar 2014 ist bis 22. Januar 2014 an Herrn MdEP Voss zu übermitteln. Dazu sollte der BND konkrete Vorschläge erarbeiten.

Referat 601 hat mitgezeichnet.

(Dennis Neist)

Klostermeyer, Karin

Von: Klostermeyer, Karin
Gesendet: Montag, 20. Januar 2014 14:11
An: 'leitung-grundsatz@bnd.bund.de'
Cc: ref603
Betreff: Unterrichtung des BKAmtes

Leitungsstab
PLSA
z. Hd. Herrn Dr. K[redacted] o.V.i.A.

Az 603 - 151 19 - Co 1/14 VS-NfD

Lg 603-84 10 NR2

Sehr geehrter Herr Dr. K[redacted]

mit Schreiben vom 17. Januar 2014 (Betreff: Unterrichtung des BKAmtes; Eingangs-Nr. Reg. PLS 0010/14) an Herrn S[redacted]bat RL 603, Äußerungen bzw. Stellungnahmen des BND gegenüber nationalen und internationalen Gremien sowie Presse-Sprachregelungen dem BKAmt grundsätzlich zur Freigabe vorzulegen. In diesem Zusammenhang ergeht der ergänzende Hinweis, dass die jeweiligen Entwürfe vorab **in schriftlicher Form** dem BKAmt vorzulegen [redacted] nd.

Mit freundlichen Grüßen
Im Auftrag

Karin Klostermeyer
Bundeskanzleramt
Referat 603

Tel.: (030) 18400 - 2631
E-Mail: ref603@bk.bund.de
E-Mail: karin.klostermeyer@bk.bund.de

Anlage 2)

000126

Neist, Dennis

Von: transfer@bnd.bund.de
Gesendet: Montag, 20. Januar 2014 15:07
An: Neist, Dennis
Cc: ref603
Betreff: Draft Report des LIBE-Vommittees -Eilt-

2/9

Datum: 20.01.2014 15:00

Betr.: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
hier: Stellungnahme
Bezug: laufender Vorgang; zuletzt: E-Mail BKAmt/Herr Neist vom 20. Januar 2014

Sehr geehrter Herr Neist,

unter Bezugnahme auf die E-Mail des BND vom 16. Januar 2014 kann ich Ihnen in Absprache mit L PLS mitteilen, dass aus hiesiger Sicht folgende inhaltliche Klarstellungen in dem vorgenannten Berichtsentwurf opportun erscheinen:
1. Im Rahmen der "Main Findings" sollte die Aufführung des BND unter Ziffer 2 entfallen.
2. Die Nennung von Präsident Schindler unter denjenigen Experten, die auf eine Einladung des LIBE-Ausschussvorsitzenden nicht reagiert hätten, sollte entfallen und durch eine Nennung bei Ziffer 1 des Annexes III ersetzt werden.

Darüber hinaus hat der BND keinen Kommentierungsbedarf hinsichtlich der vom LIBE-Komitee gefundenen Wertungen und Empfehlungen, wie sie in dem vorgenannten Berichtsentwurf zum Ausdruck kommen.

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]
----- Weitergeleitet von M[redacted] F[redacted]/DAND am 20.01.2014 11:52 -----

Von: TRANSFER/DAND
An: PLSA-HH-RECHT-SI/DAND@DAND
Datum: 20.01.2014 11:23
Betreff: Antwort: WG: EILT! Bitte um Übersendung - Änerungsvorschläge zum Berichtsentwurf des LIBE-Ausschusses zum NSA-Überwachungsprogramm
Gesendet von: ITBA-N

Anbei eine weitergeleitete Nachricht aus dem BIZ Netz.

Freundlich grüßt Sie

Ihr ITB-Leitstand in Pullach
Tel. 8[redacted]

Von: leitung-grundsatz@bnd.bund.de

21.01.2014

An: transfer@bnd.bund.de
Datum: 20.01.2014 11:21
Betreff: WG: EILT! Bitte um Übersendung - Änerungsvorschläge zum Berichtsentwurf des LIBE-Ausschusses zum NSA-Überwachungsprogramm

Bitte an PLSA-HH-RECHT-SI weiterleiten
Danke

-----Weitergeleitet von leitung-grundsatz IVBB-BND-BIZ/BIZDOM am 20.01.2014 11:20 -----
An: "'leitung-grundsatz@bnd.bund.de'" <leitung-grundsatz@bnd.bund.de>
Von: "Neist, Dennis" <Dennis.Neist@bk.bund.de>
Datum: 20.01.2014 11:16
Kopie: ref603 <ref603@bk.bund.de>
Betreff: EILT! Bitte um Übersendung - Änerungsvorschläge zum Berichtsentwurf des LIBE-Ausschusses zum NSA-Überwachungsprogramm

Leitungsstab
PLSA
z.Hd. Herrn Dr. K[redacted] o.V.i.A.
Az. 603 - 151 00 Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr Dr. K[redacted],

in Hinblick auf den o.a. Berichtsentwurf wird BND - wie durch RL 603 mit L PLS am 17.01.14 bereits vorbesprochen - gebeten, konkret auf Basis des LIBE-Berichtstext formulierte und weitergabefähige Änderungsvorschläge zu übermitteln.

Für eine Rückäußerung bis heute, 13:00 Uhr wären wir dankbar.

Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: transfer@bnd.bund.de [mailto:transfer@bnd.bund.de]
Gesendet: Donnerstag, 16. Januar 2014 17:38
An: Neist, Dennis
Cc: ref603
Betreff: WG: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Jome Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Betr.: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
hier: Stellungnahme
Bezug: E-Mails BKAmt, Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD, vom 14. und 15. Januar 2014

Sehr geehrter Herr Neist,

mit Bezug hatten Sie hinsichtlich des vorgenannten Berichts um einen Einschätzung und Bewertung auch zu möglichen Auswirkungen der durch das Komitee vorgeschlagenen Maßnahmen gebeten. Darüber hinaus hatten Sie um Mitteilung von Ideen oder Anregungen für Änderungsvorschläge bzgl. des Berichtsentwurfs gebeten. Hierzu kann ich Folgendes mitteilen:

Der Berichtsentwurf stellt die Vermutung auf, der BND betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu ist festzustellen, dass für einen solchen Vergleich die Grundlage fehlt. Die Aktivitäten der NSA sind seit dem vergangenen Sommer Gegenstand medialer Berichterstattung. Unterstellt wird dabei, dass die NSA Daten von Bürgerinnen und Bürgern der EU anlasslos und massenhaft in einem den Zweck der Terrorismusabwehr übersteigenden Maß sammelt und speichert. Für den Bundesnachrichtendienst ist festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetzt.

Der Präsident des Bundesnachrichtendienstes hat heute das beigefügte Schreiben an den Vorsitzenden des LIBE-Ausschusses gerichtet. Darüber hinaus besteht beim Bundesnachrichtendienst kein weiterer fachlicher Änderungs- oder Kommentierungsbedarf hinsichtlich des Berichtsentwurfs.

(See attached file: 140116_Pr-LIBE-Ausschuss_Reaktion auf Draft Report.pdf)

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]

-----Weitergeleitet von leitung-lage IVBB-BND-BIZ/BIZDOM am 15.01.2014 10:02 -----
An: "'leitung-lage@bnd.bund.de'" <leitung-lage@bnd.bund.de>
Von: "Neist, Dennis" <Dennis.Neist@bk.bund.de>
Datum: 15.01.2014 09:57
Kopie: ref603 <ref603@bk.bund.de>
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted],

in Erweiterung der u.a. Anfrage wird BND gebeten neben der angefragten

Einschätzung/Bewertung zusätzlich Ideen oder Anregungen für Änderungsvorschläge in Bezug auf den Berichtsentwurf mitzuteilen - dies gilt insbesondere für die Textpassagen Absatz 2 (Seite 16), Absatz 10 (Seite 17) und Absatz 20 (Seite19) im Abschnitt 'Main findings'.

Die u.a. Terminsetzung bleibt bestehen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str.. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Neist, Dennis
Gesendet: Dienstag, 14. Januar 2014 11:44
An: 'leitung-lage@bnd.bund.de'
Cc: ref603
Betreff: EILT! Bitte um Bewertung - Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs zum NSA Überwachungsprogramm (2013/2188(INI))

Leitungsstab
PLSB
z.Hd. Herrn C[redacted] o.V.i.A.

Az. 603 - 15 00 - Bu 10 NA 2/14 VS-NfD

Sehr geehrter Herr C[redacted],

mit Blick auf den o.a. Berichtsentwurf des EU-Committee on Civil Liberties, Justice and Home Affairs (LIBE-Bericht) wird BND zur Unterrichtung des StS Fritsche um eine Einschätzung und Bewertung - insbesondere hinsichtlich möglicher Auswirkungen der durch die Kommission vorgeschlagenen Maßnahmen - gebeten..

(Anhang gelöscht)

Für eine Rückäußerung bis 16. Januar 2014, DS wären wir dankbar. Aufgrund der uns gesetzten Frist bitte ich den knappen Bearbeitungszeitraum zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

MAT A BK-1-4s.pdf, Blatt 143

000130

Anlage 1) MAT A BK-1-4s.pdf, Blatt 144

000131

Neist, Dennis

Von: Karl, Albert
Gesendet: Dienstag, 21. Januar 2014 12:45
An: ref603
Betreff: WG: Anmerkungen zum LIBE-Berichtsentwurf NSA
Wichtigkeit: Hoch
Anlagen: 131223 draft report.doc (mit Kommentierungen/Anmerkungen BMI)

Bitte so umsetzen

---

2. Vg. 603 - Bu 10 NA2

Von: Schäper, Hans-Jörg
Gesendet: Dienstag, 21. Januar 2014 12:44
An: Karl, Albert
Betreff: WG: Anmerkungen zum LIBE-Berichtsentwurf NSA
Wichtigkeit: Hoch

Lieber Albert,

die Information solltest Du mitbeachten. Danke und

beste Grüße
Hans-Jörg

Von: Bartodziej, Peter
Gesendet: Dienstag, 21. Januar 2014 12:37
An: Schäper, Hans-Jörg
Betreff: WG: Anmerkungen zum LIBE-Berichtsentwurf NSA
Wichtigkeit: Hoch

Lieber Hans-Jörg,

gerade erfahre ich, dass Büro Voss auch gesondert an BMI herangetreten ist und PSt Schröder die anl. - auf der Ausarbeitung Weinbrenner beruhende - Mail an Voss geschickt hat. Insofern sollte sich BL ChefBK im Telefonat darauf konzentrieren, die StN. BMI zu unterstützen, ggf. zusätzliche BND-Punkte zu nennen und beim Pkt DatSchGrdVO auf die ER-Vorgabe 2015 zu verweisen sowie den sehr bedenklichen Punkt "Moratorium Transatlant. Freihandelsabkommen" anzusprechen. So sollte die Vorlage an BL aufgebaut werden.

Gruss Peter

Von: PStSchröder_
Gesendet: Montag, 20. Januar 2014 11:57
An: 'VOSS Axel'
Cc: AA Eickelpasch, Jörg; Weinbrenner, Ulrich; PStSchröder_
Betreff: Anmerkungen zum LIBE-Berichtsentwurf NSA

Sehr geehrte Frau Toporan,

im Auftrag von Herrn PStS darf ich Ihnen folgende Stellungnahme für Herrn Voss, MdEP zukommen lassen. Diese gliedert sich in einen allgemeinen Sachverhalt / Stellungnahme (I.) und einen Teil mit konkreten Änderungsvorschlägen (II). Schließlich ist
darüber hinaus (!) ein Dokument einigen Anmerkungen/ Kommentierungen beigefügt, die eventl. für die

↑ Anlage

MAT A BK-1-4s.pdf, Blatt 145

weitere Diskussion hilfreich sind.

I. Sachverhalt/Stellungnahme

Der LIBE-Ausschuss hat auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht zur NSA-Überwachungsprogrammen verfasst. Dieser kommt zu dem Schluss, dass die NSA z.T. gemeinsam mit Behörden in UK, Kanada und Neuseeland eine massenhafte Überwachung der elektronischen Kommunikation durchführt und dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten verletzt. Er schlägt ein breites Maßnahmenbündel vor: Überprüfung und Anpassung von Abkommen mit den USA, Stärkung von ENISA, dem Europol-Cybercrime-Center und dem EDPS und diversen Appellen an die Kommission und die Mitgliedstaaten. Schwerpunkt ist eine „Digitaler Habeas Corpus", der 7 Punkte beinhaltet:

1. Abschluss des Datenschutzpakets in 2014
   Stellungnahme: Grds. möglich. Allerdings sind noch eine Vielzahl bedeutedner Frage zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.

2. Abschluss des EU-US-Datenschutzabkommens
   Stellungnahme: Keine Bedenken. Zuständig ist EU –KOM.

3. Aussetzung des Safe-Harbour-Abkommens
   Stellungnahme: Die Bundesregierung hat sich dafür eingesetzt, zur Verbesserung von Safe Harbor in der Datenschutz-Grundverordnung einen rechtlichen Rahmen zu schaffen. Falls die Datenschutz-Grundverordnung nicht bis 2015 verabschiedet werden kann, kann Safe Harbor auch unter der Richtlinie 95/46 überarbeitet und verbessert werden. Die Frage, ob eine Aussetzung des Safe-Harbor-Abkommen in Betracht kommt, wird gemeinsam mit unseren europäischen Partner in Brüssel erörtert.

4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens
   Stellungnahme: Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus unserer Sicht derzeit kein Anlass, das Abkommen auszusetzen.

5. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)
   Stellungnahme: Keine Bedenken.

6. Entwicklung einer Strategie für eine Europäische (unabhängige) IT-Industrie
   Stellungnahme: Zustimmung. Entspricht einer Forderung aus dem Koalitionsvertrag: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings."

7. EU-Politik als Referenz für demokratische und neutrale Internet-Governance
   Stellungnahme: Keine Bedenken.

II. Änderungsvorschläge:
Die Schlussfolgerungen überraschen wenig, auch wenn sie teilweise nicht belegt werden können, sondern nur auf Vermutungen oder Presseberichte zurückgreifen. Einige Punkte sind aus deutscher Sicht jedoch kritisch und sollten daher gestrichen werden. Im Einzelnen:

1) S. 16 (Main findings Nr. 2): Der Ausschuss glaubt, dass (neben Frankreich und Schweden) **auch Deutschland ähnliche Überwachungsprogramme wie PRISM** betreibt. Diesem ist entschieden entgegenzutreten. Deutsche Behörden dürfen Kommunikationsdaten nur im Einzelfall, auf gesetzlicher Grundlage und einer förmlichen Anordnung erheben. Auch die strategische Fernmeldeaufklärung nach § 5 Artikel 10 Gesetz ist nur in eng begrenzten Fällen aufgrund in der Anordnung vorab festgelegter und nach Anordnung der G10-Kommission unter der Kontrolle durch das parlamentarische Kontrollgremium, dass die betroffenen TK-Beziehungen zu bestätigen hat, zulässig. Zudem sieht § 10 Abs. 4 S. 4 G 10 eine Beschränkung auf 20 % des möglichen Aufkommens vor.

2) S. 19 (Recommendations Nr. 20): Dementsprechend ist auch die **Aufforderung an Deutschland** (neben UK, Frankreich, Schweden und den Niederlanden), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten,** zu streichen. Die hier einschlägigen Vorschriften entsprechend den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP.

3) S. 24 (Recommendations Nr. 24): Problematisch ist auch die Aufforderung an alle Mitgliedstaaten, die unterstellten Verletzungen ihrer Souveränität auch gerichtlich geltend zu machen. Es obliegt alleine der Entscheidung des Mitgliedstaats, ob er seine Souveränität verletzt sieht und auf welchem Wege er dagegen ggf. vorgehen will.

Mit freundlichen Grüßen
Im Auftrag
Alexandra Kuczynski

Bundesministerium des Innern
Persönliche Referentin des
Parlamentarischen Staatssekretärs Dr. Ole Schröder
Alt-Moabit 101 D, 10559 Berlin
Telefon: +49 (0)30 18 681 1056
Fax: +49 (0)30 18 681 1137
E-Mail: alexandra.kuczynski@bmi.bund.de

Von: Kuczynski, Alexandra
Gesendet: Freitag, 10. Januar 2014 11:23
An: 'VOSS Axel'
Betreff: AW: JP/ Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrte Frau Toporan,

vielen Dank für die Übersendung des Entwurfs verbunden mit der Möglichkeit, Änderungsvorschläge zu übermitteln. BMI prüft und Herr Voss erhält eine Rückmeldung von Herrn Schröder.

Viele Grüße von der Spree,

MAT A BK-1-4s.pdf, Blatt 147

Alexandra Kuczynski
PR'n PStS

P.S. Bitte übermitteln Sie Herrn Voss auch herzliche Grüße von Herrn Schröder.

Von: VOSS Axel [mailto:axel.voss@europarl.europa.eu]
Gesendet: Donnerstag, 9. Januar 2014 18:19
An: PStSchröder_
Betreff: JP/ Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Schröder,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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". Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

INVALID HTML

EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2013/2188(INI)

23.12.2013

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

(2013/2188(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION 3

EXPLANATORY STATEMENT 34

Gelöscht: MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION . 3¶
EXPLANATORY STATEMENT . 36¶
ANNEX I: LIST OF WORKING DOCUMENTS . 42¶
ANNEX II: LIST OF HEARINGS AND EXPERTS . 43¶
ANNEX III: LIST OF EXPERTS WHO DECLINED PARTICIPATING IN THE LIBE INQUIRY PUBLIC HEARINGS . 51¶

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

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

The European Parliament,

– having regard to the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10, 11 and 21 thereof,

– having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 15, 16 and 218 and Title V thereof,

– having regard to Protocol 36 on transitional provisions and Article 10 thereof and to Declaration 50 concerning this protocol,

– having regard to the Charter on Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof,

– having regard to the European Convention on Human Rights, notably its Articles 6, 8, 9, 10 and 13, and the protocols thereto,

– having regard to the Universal Declaration of Human Rights, notably its Articles 7, 8, 10,11,12 and 14[1],

– having regard to the International Covenant on Civil and Political Rights, notably its Articles 14, 17, 18 and 19,

– having regard to the Council of Europe Convention on Data Protection (ETS No 108) and its 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 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 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[3],

– having regard to the Guidelines on human rights and the fight against terrorism

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

Gelöscht: PR\1013353EN.doc
Gelöscht: PE526.085v01-00

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[1], 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[2], Polish and British[3] courts, as well as before the European Court of Human Rights[4], in relation to systems of mass surveillance,

– having regard to the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, and in particular to Title III thereof[5],

– having regard to Commission Decision 520/2000 of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour privacy principles and the related frequently asked questions (FAQs) issued by the US Department of Commerce,

– having regard to the Commission assessment reports on the implementation of the Safe Harbour privacy principles of 13 February 2002 (SEC(2002)196) and of 20 October 2004 (SEC(2004)1323),

– having regard to the Commission Communication of 27 November 2013 (COM(2013)847) on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU and the Commission Communication of 27 November 2013 on rebuilding trust in EU-US data flows (COM(2013)846),

– having regard to the European Parliament 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, which took the view that the adequacy of the system could not be

[1] http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx
[2] 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 against X; Tribunal de Grande Instance of Paris.
[3] Cases by Privacy International and Liberty in the Investigatory Powers Tribunal.
[4] Joint Application Under Article 34 of Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (Applicants) - v - United Kingdom (Respondent).
[5] OJ C 197, 12.7.2000, p. 1.

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

confirmed[1], 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)844),

– 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],

– 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

---

[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)630, 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.

Gelöscht: PR\1013353EN.doc
Gelöscht: PE526.085v01-00

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 US 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 legislative proposals currently under examination in the US Congress, in particular the draft US Freedom Act,

– 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,

– 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 and 7 November 2002 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),

– having regard to its resolution of 21 May 2013 on the EU Charter: standard settings for media freedom across the EU[2],

– 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, whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter[3],

– having regard to its resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken[4],

– 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[5],

[1] Council document 16987/13.
[2] Texts adopted, P7_TA(2013)0203.
[3] Texts adopted, P7_TA-(2013)0322.
[4] Texts adopted, P7_TA(2013)0444.
[5] Texts adopted, P7_TA(2013)0449.

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

– having regard to its resolution of 10 December 2013 on unleashing the potential of cloud computing[1],

– 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[2],

– 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 (A70000/2013),

The impact of mass surveillance

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

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

C. whereas in September 2001 the world entered a new phase which resulted in the fight against terrorism being listed among the top priorities of most governments; whereas the revelations based on leaked documents from Edward Snowden, former NSA contractor, put democratically elected leaders under an obligation to address the challenges of the increasing capabilities of intelligence agencies in surveillance activities and their implications for the rule of law in a democratic society;

D. 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 high risk of violation of EU legal standards, fundamental rights and data protection standards;
- the degree of trust between EU and US 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 degree 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 strict fight against terrorism, for example economic and industrial espionage or profiling on political grounds;

[1] Texts adopted, P7_TA(2013)0535.
[2] OJ C 353 E, 3.12.2013, p.156-167.

Gelöscht: PR\1013353EN.doc
Gelöscht: PE526.085v01-00

- 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;
- the threats to privacy in a digital era;

E. whereas the unprecedented magnitude of the espionage revealed requires full investigation by the US authorities, the European Institutions and Members States' governments and national parliaments;

F. whereas the US authorities have denied some of the information revealed but not contested the vast majority of it; whereas the public debate has developed on a large scale in the US and in a limited number of EU Member States; whereas EU governments too often remain silent and fail to launch adequate investigations;

G. 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 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

H. 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];

I. 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];

J. whereas in its report of 12 December 2013, the President's Review Group on Intelligence and Communication Technology proposes 45 recommendations to the President of the US; 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 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

[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.

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

intelligence purposes, and not only for counterterrorism purposes, and to receive whistleblowers' complaints, to use Mutual Legal Assistance Treaties to obtain electronic communications, and not to use surveillance to steal industry or trade secrets;

K. whereas in respect of intelligence activities about non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental issue of respect for privacy and human dignity 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;

Legal framework

Fundamental rights

L. 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 not helped sufficiently with establishing 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;

M. 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 on Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy;

Union competences in the field of security

N. 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 disposes of certain competences on matters relating to the collective security of the Union; whereas the EU has exercised competence in matters of internal security 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;

O. 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;

Kommentar [B1]: Beide Schlussfolgerungen ergeben sich so nicht aus den genannten Regelungen; insbesondere die letzte zur Kompetenzanmaßung sollte gestrichen werden

P. whereas, under the ECHR, Member States' agencies and even private parties acting in the field of national security under certain circumstances also have to respect the rights

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

enshrined therein, be they of their own citizens or of citizens of other States; whereas this also goes for cooperation with other States' authorities in the field of national security;

Kommentar [B2]: Was soll das bedeuten? Satz streichen

Extra-territoriality

Q. whereas the extra-territorial 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 exceptional circumstances, it is necessary to take action at the EU level to ensure that the rule of law, and the rights of natural and legal persons are respected within the EU, for example by removing, neutralising, blocking or otherwise countering the effects of the foreign legislation concerned;

Gelöscht: in particular

Kommentar [B3]: Völkerrechtlich hängt die Zulässigkeit der Gegenreaktion von der Art des Verstoßes ab, es gibt keine Generalermächtigung zu bestimmten Maßnahmen

International transfers of data

R. 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 fundamental rights of EU citizens, in particular the rights to privacy and the protection of personal data, could 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;

Kommentar [MJ4]: jedenfalls soweit dies Nachrichtendienste betrifft, geht dies zu weit bzw. besteht hierfür keine EU-Kompetenz; auch die polizeiliche Zusammenarbeit mit Drittstaaten besteht nach unserer Auffassung nur insoweit eine EU-Kompetenz, als dies notwendig ist, um die EU-interne Zusammenarbeit zu regeln

Kommentar [B5]: Ich bezweifle dass jeder Datentranfer eine Verletzung der EMRK oder der Charta darstellt

Gelöscht: would

Kommentar [MJ6]: Die Haftung der MS wäre im Zusammenhang mit Art. 340 AEUV noch eingehender zu prüfen

Gelöscht: does not

Kommentar [MJ7]: zweifelhaft, ob dies so anklagend formuliert werden sollte

Transfers to the US based on the US Safe Harbour

S. whereas the US data protection legal framework should ensure an adequate level of protection for EU citizens;

T. whereas, in order to enable EU data controllers to transfer personal data to an entity in the US, the Commission, in its Decision 520/2000, has declared the adequacy of the protection provided by the Safe Harbour privacy principles and the related FAQs issued by the US Department of Commerce for personal data transferred from the Union to organisations established in the United States that have joined the Safe Harbour;

U. whereas in its resolution of 5 July 2000 the European 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;

V. whereas Commission Decision 520/2000 stipulates that the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Safe Harbour principles, in order to protect individuals with regard to the processing of their personal data in cases where there is a substantial likelihood that the Safe Harbour principles are being

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

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

violated or that the continuing transfer would create an imminent risk of grave harm to data subjects;

W. whereas Commission Decision 520/2000 also states that when 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 said Decision or limiting its scope;

X. whereas in its first two reports on the implementation of the Safe Harbour, of 2002 and 2004, the Commission identified several deficiencies as regards the proper implementation of the Safe Harbour and made several recommendations to the US authorities with a view to rectifying them;

Y. 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;

Z. whereas on 28-31 October 2013 the delegation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) to Washington D.C. met 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;

AA. 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 such an exception should not be used in a way that undermines the protection afforded by EU data protection law and the Safe Harbour principles;

Kommentar [B8]: Welches? die nachfolgendenden Kriterien beziehen sich auf die EMRK, zur Charta gibt es bislang kein entsprechendes Case law

AB. whereas large-scale access by US intelligence agencies has seriously eroded transatlantic trust and negatively impacted on the trust for 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

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

for intelligence purposes;

Transfers to third countries with the adequacy decision

AC. 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 and Canada 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;

AD. whereas Commission Decisions 2013/65[1] and 2/2002 of 20 December 2001[2] have declared the adequate level of protection ensured by the New Zealand and the Canadian Personal Information Protection and Electronic Documents Act; 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

AE. 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;

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

AG. whereas Directive 95/46/EC empowers the Commission to decide that specific standard contractual clauses offer sufficient safeguards required by the Directive and whereas on this basis the Commission has adopted three models of standard contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;

AH. 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 when 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;

AI. whereas national data protection authorities have developed binding corporate rules

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

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

(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;

Transfers based on TFTP and PNR agreements

AJ. whereas in its resolution of 23 October 2013 the European Parliament expressed serious concerns about 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 Agreement, in particular Article 1 thereof;

AK. whereas the European Parliament asked the Commission to suspend the Agreement and requested that all relevant information and documents be made available immediately for Parliament's deliberations;

AL. 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;

AM. whereas during the LIBE delegation to Washington of 28-31 October 2013 the 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 LIBE Committee inquiry that the NSA and GCHQ had targeted SWIFT networks;

AN. whereas the Belgian and Dutch 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[1];

AO. whereas according to the Joint Review of the EU-US PNR agreement, the United States 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;

[1] 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

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

AP. 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

AQ. whereas the EU-US Agreement on mutual legal assistance in criminal matters of 6 June 2003[1] entered into force on 1 February 2010 and is intended to facilitate cooperation between the EU and 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')

AR. 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;

AS. whereas this agreement should provide for clear and precise legally binding data-processing principles and should in particular recognise EU citizens' right to access, 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 and independent oversight of the data-processing activities;

AT. 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;

AU. 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

AV. 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

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

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

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;

AW. 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;

AX. 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, the Council has been unable to arrive at a general approach on the General Data Protection Regulation and the Directive[3];

IT security and cloud computing

AY. whereas the resolution of 10 December[4] emphasises the economic potential of 'cloud computing' business for growth and employment;

AZ. 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;

BA. whereas mass surveillance activities give intelligence agencies access to personal data stored by EU individuals under cloud services agreements with major US cloud providers; whereas the US intelligence authorities have accessed personal data stored in servers located on EU soil by tapping into the internal networks of Yahoo and Google[5]; whereas such activities constitute a violation of international obligations; 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;

Democratic oversight of intelligence services

BB. whereas intelligence services perform an important function in protecting democratic society against internal and external threats; whereas they are given special powers and capabilities to this end; whereas these powers are to be used within the rule of law, as otherwise they risk losing legitimacy and eroding the democratic nature of society;

BC. whereas the high level of secrecy that is intrinsic to the intelligence services in order to avoid endangering ongoing operations, revealing *modi operandi* or putting at risk the lives of agents impedes full transparency, public scrutiny and normal democratic or

[1] COM(2012) 11, 25.1.2012.
[2] COM(2012) 10, 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[4] AT-0353/2013 PE506.114V2.00.
[5] The Washington Post , 31 October 2013.

Gelöscht: PR\1013353EN.doc
Gelöscht: PE526.085v01-00

judicial examination;

BD. whereas technological developments have led to increased international intelligence cooperation, also involving the exchange of personal data, and often blurring the line between intelligence and law enforcement activities;

BE. whereas most of existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid technological developments over the last decade;

BF. whereas democratic oversight of intelligence activities is still 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;

Main findings

1. Considers that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems to collect, store and analyse communication and 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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill);

3. Notes the allegations of 'hacking' or tapping into the Belgacom systems by the UK intelligence agency GCHQ; reiterates the indication by Belgacom that it could not confirm that EU institutions were targeted or affected, and that the malware used was extremely complex and required the use of extensive financial and staffing resources for its development and use that would not be available to private entities or hackers;

4. States that trust has been profoundly shaken: trust between the two transatlantic partners, trust among EU Member States, trust between citizens and their governments, trust in the respect of the rule of law, and trust in the security of IT services; believes that in order to rebuild trust in all these dimensions a comprehensive plan is urgently needed;

5. acknowledges that specific surveillance programmes may be necessary to combat terrorism; wholeheartedly supports the fight against terrorism, but strongly believes that it can never in itself be a justification for illegal mass surveillance programmes; expresses concerns, therefore, regarding the legality, necessity and proportionality of

Gelöscht: designed by US and some Member States' intelligence services

Formatiert: Hervorheben

Kommentar [MJ9: lassen außer acht, da Unionskompetenz fü Nachrichtendienste b Politisch wird man d entsprechenden Aus kaum hindern könne

Gelöscht: believe existence of prograr similar nature, even limited scale, is like countries such as Fi Germany (BND) ar (FRA);

Formatiert: Hervorheben

Gelöscht: Notes that several governments claim

Gelöscht: these

Gelöscht: mass

Gelöscht: are

Gelöscht: untargeted, secret and sometimes even

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

some of these programmes;

6. Considers it very doubtful that data collection of such magnitude is only guided by the fight against terrorism, if it involves the collection of all possible data of all citizens; points therefore to the possible existence of other power motives such as political and economic espionage;

7. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Title I and Title VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4 paragraph 3 of the Treaty on European Union and the principle that the Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';

8. 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 and for democratic accountability;

9. Condemns in the strongest possible terms the vast, systemic, blanket collection of the personal data of innocent people, often comprising intimate personal information; emphasises that the systems of mass, indiscriminate surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but that it is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on the freedom of the press, thought and speech, as well as a significant potential for abuse of the information gathered against political adversaries; emphasises that these mass surveillance activities appear also to entail illegal actions by intelligence services and raise questions regarding the extra-territoriality of national laws;

10. Sees some 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, promoting instead a mix of law enforcement and intelligence activities with blurred legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in that 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;

11. Is adamant that secret laws, treaties 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, surveillance activities such as those examined by this inquiry may not be automatically recognised or enforced, but must be submitted individually to the appropriate national procedures on mutual recognition and legal assistance, including rules imposed by bilateral agreements;

12. Points out that the abovementioned concerns are exacerbated by rapid technological

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

Gelöscht: as

Kommentar [MJ10]: hat das EP hierfür den Belege? Ansonsten wäre diese Aussage doch fragwürdig

Gelöscht: the

Formatiert: Hervorheben

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

and societal developments; considers that, 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 of all kinds that puts at risk the integrity of the person, the scale of this problem is unprecedented;

13. Regards it as a clear finding, as emphasised by the technology experts who testified before the inquiry, that at the current stage of technological development there is no guarantee, either for EU public institutions or for citizens, that their IT security or privacy can be protected from intrusion by well-equipped third countries or EU intelligence agencies ('no 100% IT security'); notes that this alarming situation can only be remedied if Europeans are willing to dedicate sufficient resources, both human and financial, to preserving Europe's independence and self-reliance;

14. 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; 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 is not only legitimate, but also a matter of EU autonomy;

15. Commends the current discussions, inquiries and reviews concerning the subject of this inquiry in several parts of the world; points to the Global Government Surveillance Reform signed up to by the world's leading technology companies, which calls for sweeping changes to national surveillance laws, including an international ban on bulk collection of data to help preserve the public's trust in the internet; notes with great interest the recommendations published recently by the US President's Review Group on Intelligence and Communications Technologies; strongly urges governments to take these calls and recommendations fully into account and to overhaul their national frameworks for the intelligence services in order to implement appropriate safeguards and oversight;

16. 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;

17. 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;

18. Intends to request strong political undertakings from the European Commission to be designated after the May 2014 elections to implement the proposals and

Formatiert: Hervorheben
Gelöscht: these
Formatiert: Hervorheben
Formatiert: Hervorheben
Kommentar [B11]: Die EU hat keine eigene Souveränität im völkerrechtlichen Sinn
Gelöscht: and sovereignty

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

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

recommendations of this Inquiry; expects adequate commitment from the candidates in the upcoming parliamentary hearings for the new Commissioners;

Recommendations

19. Calls on the US authorities and the EU Member States to prohibit blanket mass surveillance activities and bulk processing of personal data;

20. Calls on certain EU Member States, including the UK, Germany, France, Sweden and the Netherlands, to revise where necessary their national legislation and practices governing the activities of intelligence services so as to ensure that they are in line with the standards of the European Convention on Human Rights and comply with their fundamental rights obligations as regards data protection, privacy and presumption of innocence; in particular, given the extensive media reports referring to mass surveillance in the UK, would emphasise that the 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 – should be revised;

Formatiert: Hervorheben

21. Calls on the Member States 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;

22. Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to take measures to protect their citizens from surveillance which violates human rights, including when the aim thereof is to safeguard national security, undertaken by third states and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law;

Kommentar [B12]: Die positiven Schutzpflichten nach der EMRK wären noch zu prüfen, zudem kann kein Schutz garantiert werden sondern nur dem Staat tatsächlich mögliche Maßnahmen

Gelöscht: contrary to its requirements

23. 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';

24. 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 EU 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);

25. 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 and to sign the Additional Protocol allowing for complaints by individuals under the ICCPR;

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

26. Strongly opposes any conclusion of an additional protocol or guidance to the Council of Europe Cybercrime Convention (Budapest Convention) on transborder access to stored computer data which could provide for a legitimisation of intelligence services' access to data stored in another jurisdiction without its authorisation and without the use of existing mutual legal assistance instruments, since this could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions and would be in conflict with Council of Europe Convention 108;

27. 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 for transfers of personal data;

International transfers of data

US data protection legal framework and US Safe Harbour

28. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by 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 (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); expresses its concerns on the fact that these organisations admitted that they do not encrypt information and communications flowing between their data centres, thereby enabling intelligence services to intercept information[1];

29. Considers that large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not per se meet the criteria for derogation under 'national security';

30. 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 setting out specific safeguards and protections;

31. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles, and of the related FAQs issued by the US Department of Commerce;

32. Calls on Member States' competent authorities, namely 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, provided they contain the necessary safeguards and protections with respect to the protection of the privacy and fundamental rights and freedoms of individuals;

33. Calls on the Commission to present by June 2014 a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence

[1] The Washington Post, 31 October 2013.

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

activities in response to the fact that the EU and the US legal systems for protecting personal data are drifting apart;

Transfers to other third countries with adequacy decision

34. 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;

35. Recalls that Directive 95/46/EC 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 data transfer operations; likewise recalls 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; whereas Directive 95/46/EC also empowers the Commission to declare that a third country does not ensure an adequate level of protection;

36. 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;

37. Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New Zealand and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by Commission Decisions 2013/651 and 2/2002 of 20 December 2001, have been affected by the involvement of their national intelligence agencies in the mass surveillance of EU citizens and, if necessary, to take appropriate measures to suspend or revers the adequacy decisions; expects the Commission to report to the European Parliament on its findings on the abovementioned countries by December 2014 at the latest;

Transfers based on contractual clauses and other instruments

38. Recalls that national data protection authorities have indicated that neither standard contractual clauses nor BCRs were written 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;

39. 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 established that the law to which the data importer is subject imposes upon him requirements which go beyond the restrictions necessary in a democratic society and which are likely to have a substantial adverse

[1] OJ L 28, 30.1.2013, p. 12.

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or because continuing transfer would create an imminent risk of grave harm to the data subjects;

40. 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;

41. Calls on the Commission to examine 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

42. Calls on the Commission to conduct before the end 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 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;

EU mutual assistance in criminal matters

43. Asks the Council and the 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 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

44. 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;

45. Reiterates its resolution of 23 October 2013 and asks the Commission for the

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

suspension of the TFTP Agreement;

46. Calls on the European 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')

47. Considers that a satisfactory solution under the 'Umbrella agreement' is a pre-condition for the full restoration of trust between the transatlantic partners;

48. Asks for an immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should provide for clear rights for EU citizens and effective and enforceable administrative and judicial remedies in the US without any discrimination;

49. Asks the Commission and the Council not to initiate any new sectorial agreements or arrangements for the transfer of personal data for law enforcement purposes as long as the 'Umbrella Agreement' has not entered into force;

50. 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

51. Calls on the Council Presidency and the majority of Member States who support a high level of data protection to show a sense of leadership and responsibility and accelerate their work on the whole Data Protection Package to allow for adoption in 2014, so that EU citizens will be able to enjoy better protection in the very near future;

52. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals and therefore must 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;

Cloud computing

53. Notes that trust in US cloud computing and cloud providers has been negatively affected by the abovementioned practices; emphasises, therefore, the development of European clouds as an essential element for growth and employment and trust in cloud computing services and providers and for ensuring a high level of personal data protection;

54. Reiterates its serious concerns about 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, and about direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

55. Regrets the fact that such access is usually attained by means of direct enforcement by

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

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;

56. Calls on the Commission and the Member States to speed up the work of establishing a European Cloud Partnership;

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

Transatlantic Trade and Investment Partnership Agreement (TTIP)

58. 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 and for the ability of both the EU and the US to set future global regulatory standards;

59. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that the European Parliament will only consent to the final TTIP agreement provided the agreement fully respects fundamental rights recognised by the EU Charter, and that the protection of the privacy of individuals in relation to the processing and dissemination of personal data must continue to be governed by Article XIV of the GATS;

Democratic oversight of intelligence services

60. 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 an adequate technical capability and expertise, the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

61. Invites, as it has done in the case of Echelon, 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 national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means to be able to effectively control intelligence services;

62. Calls for the setting up of a high-level group to strengthen cooperation in the field of intelligence at EU level, combined with a proper oversight mechanism ensuring both democratic legitimacy and adequate technical capacity; stresses that the high-level group should cooperate closely with national parliaments in order to propose further steps to be taken for increased oversight collaboration in the EU;

63. Calls on this high-level group to define minimum European standards or guidelines on the (ex ante and ex post) oversight of intelligence services on the basis of existing best practices and recommendations by international bodies (UN, Council of Europe);

64. Calls on the high-level group to set strict limits on the duration of any surveillance

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

ordered unless its continuation is duly justified by the authorising/oversight authority;

65. Calls on the high-level group to develop criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'[1];

66. Intends to organise a conference with national oversight bodies, whether parliamentary or independent, by the end of 2014;

67. 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;

68. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);

69. Urges the Commission to present, by September 2014, a proposal for a legal basis for the activities of the EU Intelligence Analysis Centre (IntCen), as well as a proper oversight mechanism adapted to its activities, including regular reporting to the European Parliament;

70. Calls on the Commission to present, by September 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;

Kommentar [B13]: Aufbauend auf welchen Erkenntnissen? Die EU hat diesbezüglich keine eigene Kompetenzen

71. Recalls the provisions of 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 that should be used to improve oversight at EU level;

EU agencies

72. 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 has been lawfully acquired by national authorities, particularly if the information or data was initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data;

Kommentar [B14]: Hierfür hat Europol keine Kompetenz

73. Calls on Europol to ask the competent authorities of the Member States, in line with its competences, to initiate investigations with regard to possible cybercrimes and cyber attacks committed by governments or private actors in the course of the

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

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

activities under scrutiny;

Freedom of expression

74. Expresses deep concern about the developing 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';

75. Considers that the detention of Mr Miranda and the seizure of the material in his possession under Schedule 7 of the Terrorism Act 2000 (and also the request to *The Guardian* to destroy or hand over the material) constitutes an interference with the right of freedom of expression as recognised by Article 10 of the ECHR and Article 11 of the EU Charter;

76. Calls on the Commission to put forward a proposal for a comprehensive framework for the protection of whistleblowers in the EU, with particular attention to the specificities of whistleblowing in the field of intelligence, for which provisions relating to whistleblowing in the financial field may prove insufficient, and including strong guarantees of immunity;

EU IT security

77. 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; notes that these attacks require such financial and human resources that they are likely to originate from state entities acting on behalf of foreign governments or even from certain EU national governments that support them; in this context, regards the case of the hacking or tapping of the telecommunications company Belgacom as a worrying example of an attack against the EU's IT capacity;

78. 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 an autonomous IT key-resource capability for the mid term; 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;

79. Is highly concerned by indications that foreign intelligence services sought to lower IT security standards and to install backdoors in a broad range of IT systems;

80. Calls on all the Members States, the Commission, the Council and the European Council to address the EU's dangerous lack of autonomy in terms of IT tools, companies and providers (hardware, software, services and network), and encryption and cryptographic capabilities;

81. Calls on the Commission, standardisation bodies and ENISA to develop, by September 2014, minimum security and privacy standards and guidelines for IT

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data; believes that such standards should be set in an open and democratic process, not 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;

82. Points out that both telecom companies and the EU and national telecom regulators 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 encryption of communications;

83. Supports the EU cyber strategy but considers that it does not cover all possible threats and should be extended to cover malicious state behaviours;

84. Calls on the Commission, by January 2015 at the latest, to present an Action Plan to develop more 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);

85. Calls on the Commission, in the framework of the next Work Programme of the Horizon 2020 Programme, to assess whether more resources should be directed towards boosting European research, development, innovation and training in the field of IT technologies, in particular privacy-enhancing technologies and infrastructures, cryptology, secure computing, open-source security solutions and the Information Society;

86. Asks the Commission to map out current responsibilities and to review, by June 2014 at the latest, the need for a broader mandate, better coordination and/or additional resources and technical capabilities for Europol's CyberCrime Centre, ENISA, CERT-EU and the EDPS in order to enable them to be more effective in investigating major IT breaches in the EU and in performing (or assisting Member States and EU bodies to perform) on-site technical investigations regarding major IT breaches;

87. Deems it necessary for the EU to be supported by an EU IT Academy that brings together the best European experts in all related fields, tasked with providing all relevant EU Institutions and bodies with scientific advice on IT technologies, including security-related strategies; as a first step asks the Commission to set up an independent scientific expert panel;

88. Calls on the European Parliament's Secretariat to carry out, by September 2014 at the latest, a thorough review and assessment of the European 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 the EP's IT systems; believes that such an assessment should at the least

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

provide information analysis and recommendations on:

- the need for regular, rigorous, 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 specific IT security/privacy requirements, including the possibility of a requirement for Open Source Software as a condition of purchase;
- the list of US companies under contract with the European Parliament in the IT and telecom fields, taking into account revelations about NSA contracts with a company such as RSA, whose products the European Parliament is using to supposedly protect remote access to their data by its Members and staff;
- the reliability and resilience of third-party 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;
- the use of more open-source systems and fewer off-the-shelf commercial systems;
- the impact of the increased use of mobile tools (smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;
- the security of the communications between different workplaces of the European Parliament and of the IT systems used at the European Parliament;
- the use and location of servers and IT centres for the EP'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 storage by the EP, including what kind of data is stored on the cloud, how the content and access to it is protected and where the cloud is located, clarifying the applicable data protection legal regime;
- 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 signature in email;
- an analysis of the benefits of using the GNU Privacy Guard as a default encryption standard for emails which would at the same time allow for the use of digital signatures;

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

- the possibility of setting up a secure Instant Messaging service within the European Parliament allowing secure communication, with the server only seeing encrypted content;

89. Calls on all the EU Institutions and agencies to perform a similar exercise, by December 2014 at the latest, in particular the European Council, the Council, the 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;

90. 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;

91. 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, should be developed and operated in such a way as to ensure that data is not compromised as a result of US requests under the Patriot Act; asks eu-LISA to report back to Parliament on the reliability of the systems in place by the end of 2014;

92. 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 (such as Brazil), and 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;

93. Calls for the overall architecture of the internet in terms of data flows and storage to be reconsidered, striving for more data minimisation and transparency and less centralised mass storage of raw data, as well as avoiding unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy;

94. Calls on the Member States, in cooperation with ENISA, Europol's CyberCrime Centre, CERTs and national data protection authorities and cybercrime units, to start 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 'digital hygiene', encryption and safe cloud computing, making full use of the public interest information platform provided for in the Universal Service Directive;

95. Calls on the Commission, by September 2014, to evaluate the possibilities of encouraging software and hardware manufacturers to introduce more security and privacy through default features in their products, including the possibility of introducing legal liability on the part of manufacturers for unpatched known vulnerabilities or the installation of secret backdoors, and disincentives for the undue and disproportionate collection of mass personal data, and if appropriate to come forward with legislative proposals;

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

Rebuilding trust

96. Believes that the inquiry has shown the need for the US to restore trust with its partners, as US intelligence agencies' activities are primarily at stake;

97. 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 the rule of law and the credibility of democratic safeguards in a digital society;

Between the EU and the US

98. 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;

99. 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;

100. 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; insists, however, that clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership;

101. Is ready actively 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 privacy rights of EU citizens are addressed, equal information rights and privacy protection in US courts guaranteed and the current discrimination not perpetuated;

102. Insists that necessary reforms be undertaken and effective guarantees given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is limited by clearly specified conditions and related to reasonable suspicion or probable cause of terrorist or criminal activity; stresses that this purpose must be subject to transparent judicial oversight;

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

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

104. Urges the EU 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;

105. 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 among the transatlantic allies;

106. 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

107. Also believes that that the involvement and activities of EU Members States has led to a loss of trust; is of the opinion that only full clarity as to purposes and means of surveillance, public debate and, ultimately, revision of legislation, including a strengthening of the system of judicial and parliamentary oversight, will be able to re-establish the trust lost;

108. Is aware that some EU Member States are pursuing bilateral communication with the US authorities on spying allegations, and that some of them have concluded (United Kingdom) or envisage concluding (Germany, France) so-called 'anti-spying' arrangements; underlines that these Member States need to observe fully the interests of the EU as a whole;

Kommentar [B15]: Nein, DEU muss bei den Verhandlungen mit den USA keine EU Interessen vertreten

109. Considers that such arrangements should not breach European Treaties, especially the principle of sincere cooperation (under Article 4 paragraph 3 TEU), or undermine EU policies in general and, more specifically, the internal market, fair competition and economic, industrial and social development; reserves its right to activate Treaty procedures in the event of such arrangements being proved to contradict the Union's cohesion or the fundamental principles on which it is based;

Kommentar [B16]: Der Absatz sollte gestrichen werden, es ist nicht ersichtlich wie ein bilaterales no spy Abkommen bestehende EU Politiken behindern oder bestehende Kompetenzen der EU verletzen könnte

Internationally

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

111. 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 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'; asks the High Representative/Vice-President of the Commission and the External Action Service to

Kommentar [B17]: Diese Idee ist überholt; auch VN Vertreter wollen kein Zusatzprotokoll zu Art. 17; AA hat die Initiative fallen gelassen.

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

take a proactive stance;

112. Calls on the Member States to develop a coherent and strong strategy within the United Nations, supporting in particular the resolution on 'The right to privacy in the digital age' initiated by Brazil and Germany, as adopted by the third UN General Assembly Committee (Human Rights Committee) on 27 November 2013;

Priority Plan: A European Digital Habeas Corpus

113. Decides to submit to EU citizens, Institutions and Member States the abovementioned recommendations as a Priority Plan for the next legislature;

114. Decides to launch A European Digital Habeas Corpus for protecting privacy based on the following 7 actions with a European Parliament watchdog:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella Agreement ensuring proper redress mechanisms for EU citizens 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 have been properly addressed;

Action 5: Protect the rule of law and the fundamental rights of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 6: Develop a European strategy for IT independence (at national and EU level);

Action 7: Develop the EU as a reference player for a democratic and neutral governance of the internet;

115. Calls on the EU Institutions and the Member States to support and promote the European Digital Habeas Corpus; undertakes to act as the EU citizens' rights watchdog, with the following timetable to monitor implementation:

- April-July 2014: a monitoring group based on the LIBE inquiry team responsible for monitoring any new revelations in the media concerning the inquiry's mandate and scrutinising the implementation of this resolution;
- July 2014 onwards: a standing oversight mechanism for data transfers and

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

judicial remedies within the competent committee;

- Spring 2014: a formal call on the European Council to include the European Digital Habeas Corpus in the guidelines to be adopted under Article 68 TFEU;
- Autumn 2014: a commitment that the European Digital Habeas Corpus and related recommendations will serve as key criteria for the approval of the next Commission;
- 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;
- 2015: 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;

116. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the parliaments and governments of the Member States, 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, the Government and the Parliament of the Federative Republic of Brazil, and the United Nations Secretary-General.

EXPLANATORY STATEMENT

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

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

Methodology

From July 2013, the LIBE Committee of Inquiry was responsible for the extremely challenging task of fulfilling the mandate[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

[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).

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

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

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

Reactions to mass surveillance and a public debate

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

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

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

The two types of reactions outlined above are based on a set of reasons which, if followed, may lead to quite opposed decisions as to how the EU should or should not react.

5 reasons not to act

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

– The "Intelligence/national security argument": no EU competence

Edward Snowden's revelations relate to US and some Member State's 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.

[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".

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

5 reasons to act

– The "mass surveillance argument": in which society do we want to live?

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

– The "fundamental rights argument":

Mass and indiscriminate surveillance threaten citizen's 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.

Kommentar [B18]: Nach dem jetzigen Stand des Unionsrechts schon. Es ist ein großer Unterschied zwischen Kooperation im Rahmen der EU und Kompetenz der EU

– 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.

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

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:

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

A European Digital Habeas corpus for protecting privacy based on 7 actions:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella agreement ensuring proper redress mechanisms for EU citizens in case of data transfers from the EU to the US for law-enforcement purposes;

Action 3: Suspend Safe Harbour until a full review is 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 EU highest standards;

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

Action 5: Protect the rule of law and the fundamental rights of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 6: Develop a European strategy for IT independence (at national and EU level);

Action 7: Develop the EU as a reference player for a democratic and neutral governance of Internet;

After the conclusion of the Inquiry the European Parliament should continue acting as EU citizens' rights watchdog 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 in the media concerning the Inquiries 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 in the guidelines to be adopted under Article 68 TFEU;
- Autumn 2014: a commitment that the European Digital Habeas Corpus and related recommendations will serve as key criteria for the approval of the next Commission;
- 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;

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

- 2014-2015: a conference with European intelligence oversight bodies of European national parliaments;

- 2015: a conference gathering high-level European experts in the various fields conducive to IT security (including mathematics, cryptography, privacy enhancing technologies, …) to help foster an EU IT strategy for the next legislature;

ANNEX I: LIST OF WORKING DOCUMENTS

LIBE Committee Inquiry

Rapporteur & Shadows as co-authors	Issues	EP resolution of 4 July2013 (see paragraphs 15-16)
Mr Moraes (S&D)	US and EU Member Surveillance programmes and their impact on EU citizens fundamental rights	16 (a) (b) (c) (d)
Mr Voss (EPP)	US surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation	16 (a) (b) (c)
Mrs. In't Veld (ALDE) & Mrs. Ernst (GUE)	Democratic oversight of Member State intelligence services and of EU intelligence bodies.	15, 16 (a) (c) (e)
Mr Albrecht (GREENS/EFA)	The relation between the surveillance practices in the EU and the US and the EU data protection provisions	16 (c) (e) (f)
Mr Kirkhope (ECR)	Scope of International, European and national security in the EU perspective	16 (a) (b)
AFET 3 Members	Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens	16 (a) (b) (f)

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

ANNEX II: LIST OF HEARINGS AND EXPERTS

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

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

Date	Subject	Experts
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 • Jacob APPELBAUM, investigative journalist, software developer and computer security researcher with the Tor Project • 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 • Gerhard SCHMID (former MEP and Rapporteur of the ECHELON report 2001) • Duncan CAMPBELL, investigative journalist and author of the STOA report "Interception Capabilities 2000"
12th September 2013 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	• Darius ŽILYS, Council Presidency, Director International Law Department, Lithuanian Ministry of Justice

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

	and cooperation with the LIBE Committee Inquiry (In camera)	(co-chair of the EU-US ad hoc working group on data protection) • Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection) • 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) **With AFET**	- Allegations of NSA tapping into the SWIFT data used in the TFTP programme	• Cecilia MALMSTRÖM, Member of the European Commission • Rob WAINWRIGHT, Director of Europol • 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) • Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection) • 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) • Greg NOJEIM, Senior Counsel and Director of Project on Freedom, Security &

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

		Technology, Center for Democracy & Technology (CDT) (via videoconference)
	- Effectiveness of surveillance in fighting crime and terrorism in Europe - Presentation of the study on the US surveillance programmes and their impact on EU citizens' privacy	• Dr Reinhard KREISSL, Coordinator, Increasing Resilience in Surveillance Societies (IRISS) (via videoconference) • 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) **With AFET**	- Exchange of views with US Civil Society (Part II) - Whistleblowers' activities in the field of surveillance and their legal protection	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU) Statements by whistleblowers: • Thomas DRAKE, ex-NSA Senior Executive • J. Kirk WIEBE, ex-NSA Senior analyst • Annie MACHON, ex-MI5 Intelligence officer Statements by NGOs on legal protection of whistleblowers: • Jesselyn RADACK, lawyer and representative of 6 whistleblowers, Government Accountability Project • John DEVITT, Transparency International Ireland
3rd October 2013 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. • Mr Dirk LYBAERT, Secretary General, BELGACOM S.A. • Mr Frank ROBBEN, Commission de la Protection de

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

		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 - impact of us surveillance programmes on other instruments for international transfers (contractual clauses, binding corporate rules)	• Dr. Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (GERMANY) • Christopher CONNOLLY – Galexia • Peter HUSTINX, European Data Protection Supervisor (EDPS) • Ms. Isabelle FALQUE-PIERROTIN, President of CNIL (FRANCE)
14th October 2013 15.00 - 18.30 (BXL)	- Electronic Mass Surveillance of EU Citizens and International, Council of Europe and EU Law - Court cases on Surveillance Programmes	• 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" • Judge Bostjan ZUPANČIČ, Judge at the ECHR (via videoconference) • Douwe KORFF, Professor of Law, London Metropolitan University • Dominique GUIBERT, Vice-Président of the "Ligue des Droits de l'Homme" (LDH) • Nick PICKLES, Director of Big Brother Watch • Constanze KURZ, Computer Scientist, Project Leader at Forschungszentrum für Kultur und Informatik
7th November 2013 9.00 – 11.30 and 15.00 -	- The role of EU IntCen in EU Intelligence activity (in Camera)	• Mr Ilkka SALMI, Director of EU Intelligence Analysis Centre (IntCen)

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

18h30 (BXL)	- 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 • 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) (Venice Commission) (UK)	• Mr Iain CAMERON, Member of the European Commission for Democracy through Law - "Venice Commission" • Mr Ian LEIGH, Professor of Law, Durham University • Mr David BICKFORD, Former Legal Director of the Security and intelligence agencies MI5 and MI6 • Mr Gus HOSEIN, Executive Director, Privacy International
	- EU-US transatlantic experts group	• Mr Paul NEMITZ, Director - Fundamental Rights and Citizenship, DG JUST, European Commission • Mr Reinhard PRIEBE, Director - Crisis Management and Internal Security, DG Home, European Commission
11th November 2013 15h-18.30 (BXL)	- US surveillance programmes and their impact on EU citizens' privacy (statement by Mr Jim SENSENBRENNER, Member of the US Congress)	• Mr Jim SENSENBRENNER, US House of Representatives, (Member of the Committee on the Judiciary and Chairman of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations)
	- 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) • Mr A.H. VAN DELDEN, Chair of the Dutch independent Review Committee on the Intelligence and Security Services (CTIVD

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

	- 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) • Mr Nicklas LUNDBLAD, Director, Public Policy and Government Relations, Google • Mr Richard ALLAN, Director EMEA Public Policy, Facebook
14th November 2013 15.00 – 18.30 (BXL) **With AFET**	- IT Security of EU institutions (Part I) (EP, COM (CERT-EU), (eu-LISA)	• Mr Giancarlo VILELLA, Director General, DG ITEC, European Parliament • Mr Ronald PRINS, Director and co-founder of Fox-IT • Mr Freddy DEZEURE, head of task force CERT-EU, DG DIGIT, European Commission • Mr Luca ZAMPAGLIONE, Security Officer, eu-LISA
	- The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part III)(BE, DA)	• Mr Armand DE DECKER, Vice-Chair of the Belgian Senate, Member of the Monitoring Committee of the Intelligence Services Oversight Committee • Mr Guy RAPAILLE, Chair of the Intelligence Services Oversight Committee (Comité R) • 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)	• Mr Olivier BURGERSDIJK, Head of Strategy, European Cybercrime Centre, EUROPOL

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

	- The impact of mass surveillance on confidentiality of lawyer-client relations	• Prof. Udo HELMBRECHT, Executive Director of ENISA • Mr Florian WALTHER, Independent IT-Security consultant • Mr Jonathan GOLDSMITH, Secretary General, Council of Bars and Law Societies of Europe (CCBE)
9th December 2013 (STR)	- Rebuilding Trust on EU-US Data flows	• Ms Viviane REDING, Vice President of the European Commission
	- Council of Europe Resolution 1954 (2013) on "National security and access to information"	• 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 • 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 • Mr Stephan LECHNER, Director, Institute for the Protection and Security of the Citizen (IPSC), - Joint Research Centre(JRC), European Commission • Dr. Christopher SOGHOIAN, Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union • Christian HORCHERT, IT-Security Consultant, Germany
	Exchange of views with the	• Mr Glenn GREENWALD,

Gelöscht: PE526.085v01-00

Gelöscht: PR\1013353EN.doc

	journalist having made public the facts (Part II) (Videoconference)	Author and columnist with a focus on national security and civil liberties, formerly of the Guardian

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

1. Experts who declined the LIBE Chair's Invitation

US

- Mr Keith Alexander, General US Army, Director NSA[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

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, Manager Public Policy, Amazon Senior

EU Telecommunication Companies

[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.

Gelöscht: PE526.085v01-00
Gelöscht: PR\1013353EN.doc

- 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

Germany

- Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Netherlands

- Ms Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, Nederland
- Mr Rob Bertholee, Directeur Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Sweden

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

Gelöscht: PR\1013353EN.doc

Gelöscht: PE526.085v01-00

000186

EUROPEAN PARLIAMENT

2009 - 2014

Plenary sitting

A7-0139/2014

21.2.2014

L.Vg. 603-84.10 NR2

REPORT

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

(2013/2188(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION 3

EXPLANATORY STATEMENT 44

ANNEX I: LIST OF WORKING DOCUMENTS 51

ANNEX II: LIST OF HEARINGS AND EXPERTS 52

ANNEX III: LIST OF EXPERTS WHO DECLINED PARTICIPATING IN THE LIBE INQUIRY PUBLIC HEARINGS 60

RESULT OF FINAL VOTE IN COMMITTEE 62

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

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

The European Parliament,

– having regard to the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10, 11 and 21 thereof,

– having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 15, 16 and 218 and Title V thereof,

– having regard to Protocol 36 on transitional provisions and Article 10 thereof and to Declaration 50 concerning this protocol,

– having regard to the Charter on Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof,

– having regard to the European Convention on Human Rights, notably Articles 6, 8, 9, 10 and 13 thereof, and the protocols thereto,

– having regard to the Universal Declaration of Human Rights, notably Articles 7, 8, 10,11,12 and 14 thereof[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 report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted on 17 April

[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

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, and in particular to Title III thereof[6],

– having regard to Commission Decision 520/2000 of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour privacy principles and the related frequently asked questions (FAQs) issued by the US Department of Commerce,

– having regard to the Commission's assessment reports on the implementation of the Safe Harbour privacy principles of 13 February 2002 (SEC(2002)0196) and of 20 October 2004 (SEC(2004)1323),

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

– having regard to its resolution of 5 July 2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour privacy principles and

---

[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.

related frequently asked questions issued by the US Department of Commerce, which took the view that the adequacy of the system could not be confirmed[1], 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 and 7 November 2002 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),

– having regard to its resolution of 21 May 2013 on the EU Charter: standard settings for media freedom across the EU[2],

– 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, whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter[3],

---

[1] Council document 16987/13.
[2] Texts adopted, P7_TA(2013)0203.
[3] 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 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[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 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;

C. whereas cooperation between the US and the European Union and its Member States in counter-terrorism remains vital for the security and safety of both partners;

---

[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 mutual trust and understanding are key factors in the transatlantic dialogue and partnership;

E. whereas following 11 September 2001, the fight against terrorism became one of the top priorities of most governments; whereas the revelations based on documents leaked by the former NSA contractor Edward Snowden put political leaders under the obligation to address the challenges of overseeing and controlling intelligence agencies in surveillance activities and assessing the impact of their activities on fundamental rights and the rule of law in a democratic society;

F. whereas the revelations since June 2013 have caused numerous concerns within the EU as to:

- the extent of the surveillance systems revealed both in the US and in EU Member States;
- the violation of EU legal standards, fundamental rights and data protection standards;
- the degree of trust between the EU and the US as transatlantic partners;
- the degree of cooperation and involvement of certain EU Member States with US surveillance programmes or equivalent programmes at national level as unveiled by the media;
- the lack of control and effective oversight by the US political authorities and certain EU Member States over their intelligence communities;
- the possibility of these mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense, for example economic and industrial espionage or profiling on political grounds;
- the undermining of press freedom and of communications of members of professions with a confidentiality privilege, including lawyers and doctors;
- the respective roles and degree of involvement of intelligence agencies and private IT and telecom companies;
- the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect and being subject to surveillance;
- the threats to privacy in a digital era;

G. whereas the unprecedented magnitude of the espionage revealed requires full investigation by the US authorities, the European institutions and Member States' governments, national parliaments and judicial authorities;

H. whereas the US authorities have denied some of the information revealed but have not contested the vast majority of it; whereas the public debate has developed on a large scale in the US and in certain EU Member States; whereas EU governments and parliaments too often remain silent and fail to launch adequate investigations;

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

J. whereas in comparison to actions taken both by EU institutions and by certain EU Member States, the European Parliament has taken very seriously its obligation to shed light on the revelations on the indiscriminate practices of mass surveillance of EU citizens and, by means of its resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens, instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter;

K. whereas it is the duty of the European institutions to ensure that EU law is fully implemented for the benefit of European citizens and that the legal force of the EU Treaties is not undermined by a dismissive acceptance of extraterritorial effects of third countries' standards or actions;

Developments in the US on reform of intelligence

L. whereas the District Court for the District of Columbia, in its Decision of 16 December 2013, has ruled that the bulk collection of metadata by the NSA is in breach of the Fourth Amendment to the US Constitution[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;

M. whereas a Decision of the District Court for the Eastern District of Michigan has ruled that the Fourth Amendment requires reasonableness in all searches, prior warrants for any reasonable search, warrants based upon prior-existing probable cause, as well as particularity as to persons, place and things and the interposition of a neutral magistrate between executive branch enforcement officers and citizens[2];

N. whereas in its report of 12 December 2013, the President's Review Group on Intelligence and Communication Technology proposes 46 recommendations to the President of the United States; whereas the recommendations stress the need simultaneously to protect national security and personal privacy and civil liberties; whereas in this regard it invites the US Government: to end bulk collection of phone records of US persons under Section 215 of the USA PATRIOT Act as soon as practicable; to undertake a thorough review of the NSA and the US intelligence legal framework in order to ensure respect for the right to privacy; to end efforts to subvert or make vulnerable commercial software (backdoors and malware); to increase the use of encryption, particularly in the case of data in transit, and not to undermine efforts to create encryption standards; to create a Public Interest Advocate to represent privacy and civil liberties before the Foreign Intelligence Surveillance Court; to confer on the Privacy and Civil Liberties Oversight Board the power to oversee Intelligence Community activities for foreign intelligence purposes, and not only for counterterrorism purposes; and to receive whistleblowers' complaints, to use Mutual Legal Assistance Treaties to obtain electronic communications, and not to use surveillance to steal industry or trade secrets;

---

[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.

O. whereas, according to an open memorandum submitted to President Obama by Former NSA Senior Executives/Veteran Intelligence Professionals for Sanity (VIPS) on 7 January 2014,[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;

P. whereas in respect of intelligence activities concerning non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental principle of respect for privacy and human dignity as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; whereas they do not recommend granting non-US persons the same rights and protections as US persons;

Q. whereas in his Presidential Policy Directive on Signals Intelligence Activities of 17 January 2014 and the related speech, US President Barack Obama stated that mass electronic surveillance is necessary for the United States to protect its national security, its citizens and the citizens of US allies and partners, as well as to advance its foreign policy interests; whereas this policy directive contains certain principles regarding the collection, use and sharing of signals intelligence and extends certain safeguards to non-US persons, partly providing for treatment equivalent to that enjoyed by US citizens, including safeguards for the personal information of all individuals regardless of their nationality or residence; whereas, however, President Obama did not call for any concrete proposals, particularly regarding the prohibition of mass surveillance activities and the introduction of administrative and judicial redress for non-US persons;

Legal framework

Fundamental rights

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

S. whereas fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, as enshrined in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy; whereas mass surveillance of human beings is incompatible with these cornerstones;

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

T. whereas in all Member States the law protects from disclosure information communicated in confidence between lawyer and client, a principle which has been recognised by the European Court of Justice[1];

U. whereas in its resolution of 23 October 2013 on organised crime, corruption and money laundering Parliament called on the Commission to submit a legislative proposal establishing an effective and comprehensive European whistleblower protection programme in order to protect EU financial interests and furthermore conduct an examination on whether such future legislation should also cover other fields of Union competence;

Union competences in the field of security

V. whereas according to Article 67(3) TFEU the EU 'shall endeavour to ensure a high level of security'; whereas the provisions of the Treaty (in particular Article 4(2) TEU, Article 72 TFEU and Article 73 TFEU) imply that the EU possesses certain competences on matters relating to the collective external security of the Union; whereas the EU has competence in matters of internal security (Article 4(j) TFEU) and has exercised this competence by deciding on a number of legislative instruments and concluding international agreements (PNR, TFTP) aimed at fighting serious crime and terrorism, and by setting up an internal security strategy and agencies working in this field;

W. whereas the Treaty on the Functioning of the European Union states that 'it shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security' (Article 73 TFEU);

X. whereas Article 276 TFEU states that 'in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security';

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

Z. whereas the European Treaties confer on the European Commission the role of the 'Guardian of the Treaties', and it is therefore the legal responsibility of the Commission to investigate any potential breaches of EU law;

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

issued by the US Department of Commerce for personal data transferred from the Union to organisations established in the US that have joined the Safe Harbour;

AH. whereas in its resolution of 5 July 2000 Parliament expressed doubts and concerns as to the adequacy of the Safe Harbour, and called on the Commission to review the decision in good time, in the light of experience and of any legislative developments;

AI. whereas in Parliament's working document 4 on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation of 12 December 2013, the rapporteurs expressed doubts and concerns as to the adequacy of Safe Harbour and called on the Commission to repeal the decision on the adequacy of Safe Harbour and to find new legal solutions;

AJ. whereas Commission Decision 520/2000 stipulates that the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Safe Harbour principles, in order to protect individuals with regard to the processing of their personal data in cases where there is a substantial likelihood that the Safe Harbour principles are being violated or that the continuing transfer would create an imminent risk of grave harm to data subjects;

AK. whereas Commission Decision 520/2000 also states that where evidence has been provided that anybody responsible for ensuring compliance with the principles is not effectively fulfilling their role, the Commission must inform the US Department of Commerce and, if necessary, present measures with a view to reversing or suspending the Decision or limiting its scope;

AL. whereas in its first two reports on the implementation of the Safe Harbour, published in 2002 and 2004, the Commission identified several deficiencies as regards the proper implementation of the Safe Harbour and made a number of recommendations to the US authorities with a view to rectifying those deficiencies;

AM. whereas in its third implementation report, of 27 November 2013, nine years after the second report and without any of the deficiencies recognised in that report having been rectified, the Commission identified further wide-ranging weaknesses and shortcomings in the Safe Harbour and concluded that the current implementation could not be maintained; whereas the Commission has stressed that wide-ranging access by US intelligence agencies to data transferred to the US by Safe Harbour-certified entities raises additional serious questions as to the continuity of protection of the data of EU data subjects; whereas the Commission addressed 13 recommendations to the US authorities and undertook to identify by summer 2014, together with the US authorities, remedies to be implemented as soon as possible, forming the basis for a full review of the functioning of the Safe Harbour principles;

AN. whereas on 28-31 October 2013 a delegation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) met in Washington D.C. with the US Department of Commerce and the US Federal Trade Commission; whereas the Department of Commerce acknowledged the existence of organisations having self-certified adherence to Safe Harbour Principles but clearly showing a 'not-current status', meaning that the company does not fulfil Safe Harbour requirements

although continuing to receive personal data from the EU; whereas the Federal Trade Commission admitted that the Safe Harbour should be reviewed in order to improve it, particularly with regard to complaints and alternative dispute resolution systems;

AO. whereas Safe Harbour Principles may be limited 'to the extent necessary to meet national security, public interest, or law enforcement requirements'; whereas, as an exception to a fundamental right, such an exception must always be interpreted restrictively and be limited to what is necessary and proportionate in a democratic society, and the law must clearly establish the conditions and safeguards to make this limitation legitimate; whereas the scope of application of such exception should have been clarified by the US and the EU, notably by the Commission, to avoid any interpretation or implementation that nullifies in substance the fundamental right to privacy and data protection, among others; whereas, consequently, such an exception should not be used in a way that undermines or nullifies the protection afforded by Charter of Fundamental Rights, the ECHR, the EU data protection law and the Safe Harbour principles; insists that if the national security exception is invoked, it must be specified under which national law;

AP. whereas large-scale access by US intelligence agencies has seriously eroded transatlantic trust and negatively impacted on trust as regards US organisations acting in the EU; whereas this is further exacerbated by the lack of judicial and administrative redress for EU citizens under US law, particularly in cases of surveillance activities for intelligence purposes;

Transfers to third countries with the adequacy decision

AQ. whereas according to the information revealed and to the findings of the inquiry conducted by the LIBE Committee, the national security agencies of New Zealand, Canada and Australia have been involved on a large scale in mass surveillance of electronic communications and have actively cooperated with the US under the so-called 'Five Eyes' programme, and may have exchanged with each other personal data of EU citizens transferred from the EU;

AR. whereas Commission Decisions 2013/65[1] and 2/2002 of 20 December 2001[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

AS. whereas Directive 95/46/EC provides that international transfers to a third country may also take place by means of specific instruments whereby the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights;

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

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

AU. whereas Directive 95/46/EC empowers the Commission to decide that specific standard contractual clauses offer sufficient safeguards required by the Directive, and whereas on this basis the Commission has adopted three models of standard contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;

AV. whereas the Commission Decisions establishing the standard contractual clauses stipulate that the competent authorities in Member States may exercise their existing powers to suspend data flows where it is established that the law to which the data importer or a sub-processor is subject imposes upon them requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC, where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or where there is a substantial likelihood that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects;

AW. whereas national data protection authorities have developed binding corporate rules (BCRs) in order to facilitate international transfers within a multinational corporation with adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; whereas before being used, BCRs need to be authorised by the Member States' competent authorities after the latter have assessed compliance with Union data protection law; whereas BCRs for data processors have been rejected in the LIBE Committee report on the General Data Protection Regulation, as they would leave the data controller and the data subject without any control over the jurisdiction in which their data is processed;

AX. whereas the European Parliament, given its competence stipulated by Article 218 TFEU, has the responsibility to continuously monitor the value of international agreements it has given its consent to;

Transfers based on TFTP and PNR agreements

AY. whereas in its resolution of 23 October 2013 Parliament expressed serious concerns over the revelations concerning the NSA's activities as regards direct access to financial payments messages and related data, which would constitute a clear breach of the TFTP Agreement, and in particular Article 1 thereof;

AZ. whereas terrorist finance tracking is an essential tool in the fight against terrorism financing and serious crime, allowing counterterrorism investigators to discover links between targets of investigation and other potential suspects connected with wider terrorist networks suspected of financing terrorism;

BA. whereas Parliament asked the Commission to suspend the Agreement and requested that all relevant information and documents be made available immediately for Parliament's deliberations; whereas the Commission has done neither;

BB. whereas following the allegations published by the media, the Commission decided to open consultations with the US pursuant to Article 19 of the TFTP Agreement; whereas on 27 November 2013 Commissioner Malmström informed the LIBE Committee that, after meeting US authorities and in view of the replies given by the US authorities in their letters and during their meetings, the Commission had decided not to pursue the consultations on the grounds that there were no elements showing that the US Government has acted in a manner contrary to the provisions of the Agreement, and that the US has provided written assurance that no direct data collection has taken place contrary to the provisions of the TFTP agreement; whereas it is not clear whether the US authorities have circumvented the Agreement by accessing such data through other means, as indicated in the letter of 18 September 2013 from the US authorities[1];

BC. whereas during its visit to Washington of 28-31 October 2013 the LIBE delegation met with the US Department of the Treasury; whereas the US Treasury stated that since the entry into force of the TFTP Agreement it had not had access to data from SWIFT in the EU except within the framework of the TFTP; whereas the US Treasury refused to comment on whether SWIFT data would have been accessed outside TFTP by any other US government body or department or whether the US administration was aware of NSA mass surveillance activities; whereas on 18 December 2013 Mr Glenn Greenwald stated before the inquiry held by the LIBE Committee that the NSA and GCHQ had targeted SWIFT networks;

BD. whereas the Belgian and Netherlands data protection authorities decided on 13 November 2013 to conduct a joint investigation into the security of SWIFT's payment networks in order to ascertain whether third parties could gain unauthorised or unlawful access to European citizens' bank data[2];

BE. whereas according to the Joint Review of the EU-US PNR agreement, the US Department of Homeland Security (DHS) made 23 disclosures of PNR data to the NSA on a case-by-case basis in support of counterterrorism cases, in a manner consistent with the specific terms of the Agreement;

BF. whereas the Joint Review fails to mention the fact that in the case of processing of personal data for intelligence purposes, under US law, non-US citizens do not enjoy any judicial or administrative avenue to protect their rights, and constitutional protections are only granted to US persons; whereas this lack of judicial or administrative rights nullifies the protections for EU citizens laid down in the existing PNR agreement;

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

BG. whereas the EU-US Agreement on mutual legal assistance in criminal matters of

---

[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

6 June 2003[1] entered into force on 1 February 2010 and is intended to facilitate cooperation between the EU and the US to combat crime in a more effective way, having due regard for the rights of individuals and the rule of law;

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

BH. whereas the purpose of this general agreement is to establish the legal framework for all transfers of personal data between the EU and US for the sole purposes of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters; whereas negotiations were authorised by the Council on 2 December 2010; whereas this agreement is of the utmost importance and would act as the basis to facilitate data transfer in the context of police and judicial cooperation and in criminal matters;

BI. whereas this agreement should provide for clear and precise and legally binding data-processing principles, and should in particular recognise EU citizens' right to judicial access to and rectification and erasure of their personal data in the US, as well as the right to an efficient administrative and judicial redress mechanism for EU citizens in the US and independent oversight of the data-processing activities;

BJ. whereas in its communication of 27 November 2013 the Commission indicated that the 'umbrella agreement' should result in a high level of protection for citizens on both sides of the Atlantic and should strengthen the trust of Europeans in EU-US data exchanges, providing a basis on which to develop EU-US security cooperation and partnership further;

BK. whereas negotiations on the agreement have not progressed because of the US Government's persistent position of refusing recognition of effective rights of administrative and judicial redress to EU citizens and because of the intention of providing broad derogations to the data protection principles contained in the agreement, such as purpose limitation, data retention or onward transfers either domestically or abroad;

Data protection reform

BL. whereas the EU data protection legal framework is currently being reviewed in order to establish a comprehensive, consistent, modern and robust system for all data-processing activities in the Union; whereas in January 2012 the Commission presented a package of legislative proposals: a General Data Protection Regulation[2], which will replace Directive 95/46/EC and establish a uniform law throughout the EU, and a Directive[3] which will lay down a harmonised framework for all data processing activities by law enforcement authorities for law enforcement purposes and will reduce the current divergences among national laws;

BM. whereas on 21 October 2013 the LIBE Committee adopted its legislative reports on

[1] OJ L 181, 19.7.2003, p. 25.
[2] COM(2012)0011, 25.1.2012.
[3] COM(2012)0010, 25.1.2012.

the two proposals and a decision on the opening of negotiations with the Council with a view to having the legal instruments adopted during this legislative term;

BN. whereas, although the European Council of 24/25 October 2013 called for the timely adoption of a strong EU General Data Protection framework in order to foster the trust of citizens and businesses in the digital economy, after two years of deliberations the Council has still been unable to arrive at a general approach on the General Data Protection Regulation and the Directive[1];

IT security and cloud computing

BO. whereas Parliament's resolution of 10 December 2013[2] emphasises the economic potential of 'cloud computing' business for growth and employment; whereas the overall economic value of the cloud market is forecast to be worth USD 207 billion a year by 2016, or twice its value in 2012;

BP. whereas the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context; whereas Union data protection law, since it is technologically neutral, already applies fully to cloud computing services operating in the EU;

BQ. whereas mass surveillance activities give intelligence agencies access to personal data stored or otherwise processed by EU individuals under cloud services agreements with major US cloud providers; whereas the US intelligence authorities have accessed personal data stored or otherwise processed in servers located on EU soil by tapping into the internal networks of Yahoo and Google; whereas such activities constitute a violation of international obligations and of European fundamental rights standards including the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, freedom of assembly and association and the freedom to conduct business; whereas it is not excluded that information stored in cloud services by Member States' public authorities or undertakings and institutions has also been accessed by intelligence authorities;

BR. whereas US intelligence agencies have a policy of systematically undermining cryptographic protocols and products in order to be able to intercept even encrypted communication; whereas the US National Security Agency has collected vast numbers of so called 'zero-day exploits' – IT security vulnerabilities that are not yet known to the public or the product vendor; whereas such activities massively undermine global efforts to improve IT security;

BS. whereas the fact that intelligence agencies have accessed personal data of users of online services has severely distorted the trust of citizens in such services, and therefore has an adverse effect on businesses investing in the development of new services using 'Big Data' and new applications such as the 'Internet of Things';

BT. whereas IT vendors often deliver products that have not been properly tested for IT

[1] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[2] A7-0353/2013 - PE506.114v2.00.

security or that even sometimes have backdoors implanted purposefully by the vendor; whereas the lack of liability rules for software vendors has led to such a situation, which is in turn exploited by intelligence agencies but also leaves open the risk of attacks by other entities;

BU. whereas it is essential for companies providing such new services and applications to respect the data protection rules and privacy of the data subjects whose data are collected, processed and analysed, in order to maintain a high level of trust among citizens;

Democratic oversight of intelligence services

BV. whereas intelligence services in democratic societies are given special powers and capabilities to protect fundamental rights, democracy and the rule of law, citizens' rights and the State against internal and external threats, and are subject to democratic accountability and judicial oversight; whereas they are given special powers and capabilities only to this end; whereas these powers should be used within the legal limits imposed by fundamental rights, democracy and the rule of law and their application should be strictly scrutinised, as otherwise they lose legitimacy and risk undermining democracy;

BW. whereas the fact that a certain level of secrecy is conceded to intelligence services in order to avoid endangering ongoing operations, revealing modi operandi or putting at risk the lives of agents, such secrecy cannot override or exclude rules on democratic and judicial scrutiny and examination of their activities, as well as on transparency, notably in relation to the respect of fundamental rights and the rule of law, all of which are cornerstones in a democratic society;

BX. whereas most of the existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid political and technological developments over the last decade that have led to increased international intelligence cooperation, also through the large scale exchange of personal data, and often blurring the line between intelligence and law enforcement activities;

BY. whereas democratic oversight of intelligence activities is still only conducted at national level, despite the increase in exchange of information between EU Member States and between Member States and third countries; whereas there is an increasing gap between the level of international cooperation on the one hand and oversight capacities limited to the national level on the other, which results in insufficient and ineffective democratic scrutiny;

BZ. whereas national oversight bodies often do not have full access to intelligence received from a foreign intelligence agency, which can lead to gaps in which international information exchanges can take place without adequate review; whereas this problem is further aggravated by the so-called 'third party rule' or the principle of 'originator control', which has been designed to enable originators to maintain control over the further dissemination of their sensitive information, but is unfortunately often interpreted as applying also to the recipient services' oversight;

CA. whereas private and public transparency reform initiatives are key to ensuring public trust in the activities of intelligence agencies; whereas legal systems should not prevent companies from disclosing to the public information about how they handle all types of government requests and court orders for access to user data, including the possibility of disclosing aggregate information on the number of requests and orders approved and rejected;

Main findings

1. Considers that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, admissions by authorities, and the insufficient response to these allegations, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner;

2. Points specifically to US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted 'man-in-the-middle attacks' on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme);

3. Notes the allegations of 'hacking' or tapping into the Belgacom systems by the UK intelligence agency GCHQ; notes the statements by Belgacom that it could neither confirm nor deny that EU institutions were targeted or affected, and that the malware used was extremely complex and its development and use would require extensive financial and staffing resources that would not be available to private entities or hackers;

4. Emphasises that trust has been profoundly shaken: trust between the two transatlantic partners, trust between citizens and their governments, trust in the functioning of democratic institutions on both sides of the Atlantic, trust in the respect of the rule of law, and trust in the security of IT services and communication; believes that in order to rebuild trust in all these dimensions, an immediate and comprehensive response plan comprising a series of actions which are subject to public scrutiny is needed;

5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society;

6. Recalls the EU's firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection;

7. Considers that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled;

8. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Titles I and VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4(3) of the Treaty on European Union, as well as the principle that Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';

9. Notes that international treaties and EU and US legislation, as well as national oversight mechanisms, have failed to provide for the necessary checks and balances or for democratic accountability;

10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws;

11. Considers it crucial that the professional confidentiality privilege of lawyers, journalists, doctors and other regulated professions is safeguarded against mass surveillance activities; stresses, in particular, that any uncertainty about the confidentiality of communications between lawyers and their clients could negatively impact on EU citizens' right of access to legal advice and access to justice and the right to a fair trial;

12. Sees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in this regard the decision of the German Federal Constitutional

Court[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 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'[2]; recalls further that the protection of the privacy of all EU citizens is at stake, as are the security and reliability of all EU communication networks; believes, therefore, that discussion and action at EU level are not only legitimate, but also a matter of EU autonomy;

17. Commends the current discussions, inquiries and reviews concerning the subject of this inquiry in several parts of the world, including through the support of civil society; points to the Global Government Surveillance Reform signed up to by the world's leading technology companies calling for sweeping changes to national surveillance laws, including an international ban on bulk collection of data, to help preserve the public's trust in the internet and in their businesses; points to the calls

[1] No 1 BvR 518/02 of 4 April 2006.
[2] Judgement in Case C-300/11, ZZ v Secretary of State for the Home Department, 4 June 2013.

made by hundreds of leading academics[1], civil society organisations[2] and 562 international authors, including five Nobel laureates, for an end to mass surveillance; notes with great interest the recommendations published recently by the US President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court[3]; strongly urges governments to take these calls and recommendations fully into account and to overhaul their national frameworks for their intelligence services in order to implement appropriate safeguards and oversight;

18. Commends the institutions and experts who have contributed to this Inquiry; 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;

19. Is aware that in such a limited timeframe it has been possible to conduct only a preliminary investigation of all the issues at stake since July 2013; recognises both the scale of the revelations involved and their ongoing nature; adopts, therefore, a forward-planning approach consisting in a set of specific proposals and a mechanism for follow-up action in the next parliamentary term, ensuring the findings remain high on the EU political agenda;

20. Intends to request strong political undertakings from the new Commission which will be designated after the May 2014 European elections to the effect that it will implement the proposals and recommendations of this Inquiry; expects an appropriate level of commitment from the candidates in the upcoming parliamentary hearings for the new Commissioners;

Recommendations

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

22. Calls on the EU Member States, and in particular those participating in the so-called '9-eyes' and '14-eyes' programmes[4], to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny, that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency, including by reference to the UN compilation of good practices and the recommendations of the Venice Commission, and that they are in line with the standards of the European Convention on Human Rights and comply with Member States' fundamental rights obligations, in particular as regards data protection, privacy, and the presumption of innocence;

[1] www.academicsagainstsurveillance.net.
[2] www.stopspyingonus.com and www.en.necessaryandproportionate.org.
[3] http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.
[4] 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.

23. Calls on all EU Member States and in particular, with regard to its Resolution of 4 July 2013 and Inquiry Hearings, the United Kingdom, France, Germany, Sweden, the Netherlands and Poland to ensure that their current or future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies are in line with the standards of the European Convention on Human Rights and European Union data protection legislation; calls on these Member States to clarify the allegations of mass surveillance activities, including mass surveillance of cross border telecommunications, untargeted surveillance on cable-bound communications, potential agreements between intelligence services and telecommunication companies as regards access and exchange of personal data and access to transatlantic cables, US intelligence personnel and equipment on EU territory without oversight on surveillance operations, and their compatibility with EU legislation; invites the national parliaments of those countries to intensify cooperation of their intelligence oversight bodies at European level;

24. Calls on the United Kingdom, in particular, given the extensive media reports referring to mass surveillance by the intelligence service GCHQ, to revise its current legal framework, which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000;

25. Takes note of the review of the Dutch Intelligence and Security Act 2002 (report by the Dessens Commission of 2 December 2013); supports those recommendations of the review commission which aim to strengthen the transparency, control and oversight of the Dutch intelligence services; calls on the Netherlands to refrain from extending the powers of the intelligence services in such a way as to enable untargeted and large-scale surveillance also to be performed on cable-bound communications of innocent citizens, especially given the fact that one of the biggest Internet Exchange Points in the world is located in Amsterdam (AMS-IX); calls for caution in defining the mandate and capabilities of the new Joint Sigint Cyber Unit, as well as for caution regarding the presence and operation of US intelligence personnel on Dutch territory;

26. Calls on the Member States, including when represented by their intelligence agencies, to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including the protection of human rights under the TEU, the ECHR and the EU Charter of Fundamental Rights;

27. Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law;

28. Invites the Secretary-General of the Council of Europe to launch the Article 52 procedure according to which 'on receipt of a request from the Secretary-General of the Council of Europe any High Contracting Party shall furnish an explanation of the

manner in which its internal law ensures the effective implementation of any of the provisions of the Convention';

29. Calls on Member States to take appropriate action immediately, including court action, against the breach of their sovereignty, and thereby the violation of general public international law, perpetrated through the mass surveillance programmes; calls further on Member States to make use of all available international measures to defend EU citizens' fundamental rights, notably by triggering the inter-state complaint procedure under Article 41 of the International Covenant on Civil and Political Rights (ICCPR);

30. Calls on the US to revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens, to put rights of EU citizens on an equal footing with rights of US citizens, and to sign the Optional Protocol allowing for complaints by individuals under the ICCPR;

31. Welcomes, in this regard, the remarks made and the Presidential Policy Directive issued by US President Obama on 17 January 2014, as a step towards limiting authorisation of the use of surveillance and data processing to national security purposes and towards equal treatment of all individuals' personal information, regardless of their nationality or residence, by the US intelligence community; awaits, however, in the context of the EU-US relationship, further specific steps which will, most importantly, strengthen trust in transatlantic data transfers and provide for binding guarantees for enforceable privacy rights of EU citizens, as outlined in detail in this report;

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

33. Calls on the Commission to carry out, before July 2014, an assessment of the applicability of Regulation (EC) No 2271/96 to cases of conflict of laws on transfers of personal data;

34. Calls on the Fundamental Rights Agency to undertake in-depth research on the protection of fundamental rights in the context of surveillance, and in particular on the current legal situation of EU citizens with regard to the judicial remedies available to them in relation to those practices;

International transfers of data

US data protection legal framework and US Safe Harbour

35. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by the US NSA are companies that have self-certified their adherence to the Safe Harbour, and that the Safe Harbour is the legal instrument used for the transfer of EU personal data to the US (examples being Google, Microsoft, Yahoo!, Facebook, Apple and LinkedIn); expresses its concerns that these organisations have not encrypted information and communications flowing between their data centres, thereby enabling intelligence services to intercept information; welcomes the subsequent statements by some US companies that they will accelerate plans to implement encryption of data flows between their global data centres;

36. Considers that large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not meet the criteria for derogation under 'national security';

37. Takes the view that, as under the current circumstances the Safe Harbour principles do not provide adequate protection for EU citizens, these transfers should be carried out under other instruments, such as contractual clauses or BCRs, provided these instruments set out specific safeguards and protections and are not circumvented by other legal frameworks;

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

39. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles, and of the related FAQs issued by the US Department of Commerce; calls on the US authorities, therefore, to put forward a proposal for a new framework for transfers of personal data from the EU to the US which meets Union law data protection requirements and provides for the required adequate level of protection;

40. Calls on Member States' competent authorities, in particular the data protection authorities, to make use of their existing powers and immediately suspend data flows to any organisation that has self-certified its adherence to the US Safe Harbour Principles, and to require that such data flows are only carried out under other instruments and provided they contain the necessary safeguards and guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals;

41. Calls on the Commission to present, by December 2014, a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities, and concrete recommendations based on the absence of a general data protection law in the US; encourages the Commission to engage with the US administration in order to establish a legal framework providing for a high level of protection of individuals with regard to the protection of their personal data when transferred to the US and ensure the equivalence of EU and US privacy frameworks;

Transfers to other third countries with adequacy decision

42. Recalls that Directive 95/46/EC stipulates that transfers of personal data to a third country may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection, the purpose of this provision being to ensure the continuity of the protection afforded by EU data protection law where personal data are transferred outside the EU;

43. Recalls that Directive 95/46/EC also provides that the adequacy of the level of protection afforded by a third country is to be assessed in the light of all the circumstances surrounding a data transfer operation or set of such operations; recalls likewise that the said Directive also equips the Commission with implementing powers to declare that a third country ensures an adequate level of protection in the light of the criteria laid down by Directive 95/46/EC; recalls that Directive 95/46/EC also empowers the Commission to declare that a third country does not ensure an adequate level of protection;

44. Recalls that in the latter case Member States must take the measures necessary to prevent any transfer of data of the same type to the third country in question, and that the Commission should enter into negotiations with a view to remedying the situation;

45. Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New Zealand Privacy Act and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by Commission Decisions 2013/65 and 2/2002 of 20 December 2001, has been affected by the involvement of those countries' national intelligence agencies in the mass surveillance of EU citizens, and, if necessary, to take appropriate measures to suspend or reverse the adequacy decisions; also calls on the Commission to assess the situation for other countries that have received an adequacy rating; expects the Commission to report to Parliament on its findings on the above-mentioned countries by December 2014 at the latest;

Transfers based on contractual clauses and other instruments

46. Recalls that national data protection authorities have indicated that neither standard contractual clauses nor BCRs were formulated with situations of access to personal data for mass surveillance purposes in mind, and that such access would not be in line with the derogation clauses of the contractual clauses or BCRs which refer to exceptional derogations for a legitimate interest in a democratic society and where necessary and proportionate;

47. Calls on the Member States to prohibit or suspend data flows to third countries based on the standard contractual clauses, contractual clauses or BCRs authorised by the national competent authorities where it is likely that the law to which data recipients are subject imposes requirements on them which go beyond the restrictions that are strictly necessary, adequate and proportionate in a democratic society and are likely to have an adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or because continuing transfer would create a risk of grave harm to the data subjects;

48. Calls on the Article 29 Working Party to issue guidelines and recommendations on the safeguards and protections that contractual instruments for international transfers of EU personal data should contain in order to ensure the protection of the privacy, fundamental rights and freedoms of individuals, taking particular account of the third-country laws on intelligence and national security and the involvement of the companies receiving the data in a third country in mass surveillance activities by a third country's intelligence agencies;

49. Calls on the Commission to examine without delay the standard contractual clauses it has established in order to assess whether they provide the necessary protection as regards access to personal data transferred under the clauses for intelligence purposes and, if appropriate, to review them;

Transfers based on the Mutual Legal Assistance Agreement

50. Calls on the Commission to conduct, before the end of 2014, an in-depth assessment of the existing Mutual Legal Assistance Agreement, pursuant to its Article 17, in order to verify its practical implementation and, in particular, whether the US has made effective use of it for obtaining information or evidence in the EU and whether the Agreement has been circumvented to acquire the information directly in the EU, and to assess the impact on the fundamental rights of individuals; such an assessment should not only refer to US official statements as a sufficient basis for the analysis but also be based on specific EU evaluations; this in-depth review should also address the consequences of the application of the Union's constitutional architecture to this instrument in order to bring it into line with Union law, taking account in particular of Protocol 36 and Article 10 thereof and Declaration 50 concerning this protocol; calls on the Council and Commission also to assess bilateral agreements between Member States and the US so as to ensure that they are consistent with the agreements that the EU follows or decides to follow with the US;

EU mutual assistance in criminal matters

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

Transfers based on the TFTP and PNR agreements

52. Takes the view that the information provided by the European Commission and the US Treasury does not clarify whether US intelligence agencies have access to SWIFT financial messages in the EU by intercepting SWIFT networks or banks' operating systems or communication networks, alone or in cooperation with EU national intelligence agencies and without having recourse to existing bilateral channels for mutual legal assistance and judicial cooperation;

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

54. Calls on the Commission to react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy;

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

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

56. Asks for an immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should put rights for EU citizens on an equal footing with rights for US citizens; stresses that, moreover, this agreement should provide effective and enforceable administrative and judicial remedies for all EU citizens in the US without any discrimination;

57. Asks the Commission and Council not to initiate any new sectorial agreements or arrangements for the transfer of personal data for law enforcement purposes with the US as long as the 'Umbrella Agreement' has not entered into force;

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

Data protection reform

59. Calls on the Council Presidency and the Member States to accelerate their work on the whole Data Protection Package to allow for its adoption in 2014, so that EU citizens will be able to enjoy a high level of data protection in the very near future; stresses that strong engagement and full support on the part of the Council are a necessary condition to demonstrate credibility and assertiveness towards third countries;

60. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals, and that the two must therefore be treated as a package to be adopted simultaneously, in order to ensure that all data-processing activities in the EU provide a high level of protection in all circumstances; stresses that it will only adopt further law enforcement cooperation measures once the Council has entered into negotiations with Parliament and the Commission on the Data Protection Package;

61. Recalls that the concepts of 'privacy by design' and 'privacy by default' are a strengthening of data protection and should have the status of guidelines for all products, services and systems offered on the internet;

62. Considers higher transparency and safety standards for online and telecommunication as a necessary principle with a view to a better data protection regime; calls, therefore, on the Commission to put forward a legislative proposal on standardised general terms and conditions for online and telecommunications services, and to mandate a supervisory body to monitor compliance with the general terms and conditions;

Cloud computing

63. Notes that trust in US cloud computing and cloud providers has been negatively affected by the above-mentioned practices; emphasises, therefore, the development of European clouds and IT solutions as an essential element for growth and employment and for trust in cloud computing services and providers, as well as for ensuring a high level of personal data protection;

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

65. Reiterates its serious concern regarding the compulsory direct disclosure of EU personal data and information processed under cloud agreements to third-country authorities by cloud providers subject to third-country laws or using storage servers located in third countries, as also regarding direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

66. Deplores the fact that such access is usually attained by means of direct enforcement by third-country authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;

67. Calls on the Commission and the Member States to speed up the work of establishing a European Cloud Partnership while fully including civil society and the technical community, such as the Internet Engineering Task Force (IETF), and incorporating data protection aspects;

68. Urges the Commission, when negotiating international agreements that involve the processing of personal data, to take particular note of the risks and challenges that cloud computing□poses to fundamental rights, in particular – but not exclusively – the right to private life and to the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; urges the Commission, furthermore, to take note of the negotiating partner's domestic rules governing the access of law enforcement and intelligence agencies to personal data processed through cloud computing services, in particular by demanding that such access be granted only if there is full respect for due process of law and on an unambiguous legal basis, as well as the requirement that the exact conditions of access, the purpose of gaining such access, the security measures put in place when handing over data and the rights of the individual, as well as the rules for supervision and for an effective redress mechanism, be specified;

69. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches, and underlines the importance of having effective, proportionate and dissuasive administrative sanctions in place that can be imposed on 'cloud computing' service providers who do not comply with EU data protection standards;

70. Calls on the Commission and the competent authorities of the Member States to evaluate the extent to which EU rules on privacy and data protection have been

violated through the cooperation of EU legal entities with secret services or through the acceptance of court warrants of third-country authorities requesting personal data of EU citizens contrary to EU data protection legislation;

71. Calls on businesses providing new services using 'Big Data' and new applications such as the 'Internet of Things' to build in data protection measures already at the development stage, in order to maintain a high level of trust among citizens;

Transatlantic Trade and Investment Partnership Agreement (TTIP)

72. Recognises that the EU and the US are pursuing negotiations for a Transatlantic Trade and Investment Partnership, which is of major strategic importance for creating further economic growth;

73. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that the consent of the European Parliament to the final TTIP agreement could be endangered as long as the blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not completely abandoned and an adequate solution is found for the data privacy rights of EU citizens, including administrative and judicial redress; stresses that Parliament may only consent to the final TTIP agreement provided the agreement fully respects, inter alia, the fundamental rights recognised by the EU Charter, and provided the protection of the privacy of individuals in relation to the processing and dissemination of personal data remain governed by Article XIV of the GATS; stresses that EU data protection legislation cannot be deemed an 'arbitrary or unjustifiable discrimination' in the application of Article XIV of the GATS;

Democratic oversight of intelligence services

74. Stresses that, despite the fact that oversight of intelligence services' activities should be based on both democratic legitimacy (strong legal framework, ex ante authorisation and ex post verification) and adequate technical capability and expertise, the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

75. Calls, as it did in the case of Echelon, on all national parliaments which have not yet done so to install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate; calls on the national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means, including the right to conduct on-site visits, to be able to effectively control intelligence services;

76. Calls for the setting up of a High-Level Group to propose, in a transparent manner and in collaboration with parliaments, recommendations and further steps to be taken for enhanced democratic oversight, including parliamentary oversight, of intelligence services and increased oversight collaboration in the EU, in particular as regards its cross-border dimension;

77. Considers this High-Level group should:

- define minimum European standards or guidelines on the (ex ante and ex post) oversight of intelligence services on the basis of existing best practices and recommendations by international bodies (UN, Council of Europe), including the issue of oversight bodies being considered as a third party under the 'third party rule', or the principle of 'originator control', on the oversight and accountability of intelligence from foreign countries;

- set strict limits on the duration and scope of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority; recalls that the duration of any surveillance ordered should be proportionate and limited to its purpose;

- develop criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'[1];

78. Intends to organise a conference with national oversight bodies, whether parliamentary or independent, by the end of 2014;

79. Calls on the Member States to draw on best practices so as to improve access by their oversight bodies to information on intelligence activities (including classified information and information from other services) and establish the power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments;

80. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);

81. Urges the Commission and the HR/VP to present, by December 2014, a proposal for a legal basis for the activities of the EU Intelligence Analysis Centre (IntCen), together with an adequate oversight mechanism; urges the HR/VP to regularly account for the activities of IntCen to the responsible bodies of Parliament, including its full compliance with fundamental rights and applicable EU data privacy rules, and to specifically clarify its existing oversight mechanism with Parliament;

82. Calls on the Commission to present, by December 2014, a proposal for an EU security clearance procedure for all EU office holders, as the current system, which relies on the security clearance undertaken by the Member State of citizenship, provides for different requirements and lengths of procedures within national systems, thus leading to differing treatment of Members of Parliament and their staff depending on their nationality;

83. Recalls the provisions of the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, which should be used to improve oversight at EU level;

EU agencies

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

84. Calls on the Europol Joint Supervisory Body, together with national data protection authorities, to conduct a joint inspection before the end of 2014 in order to ascertain whether information and personal data shared with Europol have been lawfully acquired by national authorities, particularly if the information or data were initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data; considers that Europol should not process any information or data which were obtained in violation of fundamental rights which would be protected under the Charter of Fundamental Rights;

85. Calls on Europol to make full use of its mandate to request the competent authorities of the Member States to initiate criminal investigations with regards to major cyberattacks and IT breaches with potential cross-border impact; believes that Europol's mandate should be enhanced in order to allow it to initiate its own investigation following suspicion of a malicious attack on the network and information systems of two or more Member States or Union bodies[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;

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

89. Calls on the Member States to ensure that their legislation, notably in the field of national security, provides a safe alternative to silence for disclosing or reporting of wrongdoing, including corruption, criminal offences, breaches of legal obligation, miscarriages of justice and abuse of authority, which is also in line with the provisions of different international (UN and Council of Europe) instruments against corruption, the principles laid out in the PACE Resolution 1729 (2010), the Tshwane principles, etc;

EU IT security

90. Points out that recent incidents clearly demonstrate the acute vulnerability of the EU, and in particular the EU institutions, national governments and parliaments, major European companies, European IT infrastructures and networks, to sophisticated attacks using complex software and malware; notes that these attacks require financial and human resources on a scale such that they are likely to originate from state entities acting on behalf of foreign governments; in this context, regards the case of the hacking or tapping of the telecommunications company Belgacom as a worrying example of an attack on the EU's IT capacity; underlines that boosting EU IT capacity and security also reduces the vulnerability of the EU towards serious cyberattacks originating from large criminal organisations or terrorist groups;

91. Takes the view that the mass surveillance revelations that have initiated this crisis can be used as an opportunity for Europe to take the initiative and build up, as a strategic priority measure, a strong and autonomous IT key-resource capability; stresses that in order to regain trust, such a European IT capability should be based, as much as possible, on open standards and open-source software and if possible hardware, making the whole supply chain from processor design to application layer transparent and reviewable; points out that in order to regain competitiveness in the strategic sector of IT services, a 'digital new deal' is needed, with joint and large-scale efforts by EU institutions, Member States, research institutions, industry and civil society; calls on the Commission and the Member States to use public procurement as leverage to support such resource capability in the EU by making EU security and privacy standards a key requirement in the public procurement of IT goods and services; urges the Commission, therefore, to review the current public procurement practices with regard to data processing in order to consider restricting tender procedures to certified companies, and possibly to EU companies, where security or other vital interests are involved;

92. Strongly condemns the fact that intelligence services sought to lower IT security standards and to install backdoors in a wide range of IT systems; asks the Commission to present draft legislation to ban the use of backdoors by law enforcement agencies; recommends, consequently, the use of open-source software in all environments where IT security is a concern;

93. Calls on all the Member States, the Commission, the Council and the European Council to give their fullest support, including through funding in the field of research and development, to the development of European innovative and technological capability in IT tools, companies and providers (hardware, software, services and network), including for purposes of cybersecurity and encryption and cryptographic

capabilities;

94. Calls on the Commission, standardisation bodies and ENISA to develop, by December 2014, minimum security and privacy standards and guidelines for IT systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data and the integrity of all IT systems; believes that such standards could become the benchmark for new global standards and should be set in an open and democratic process, rather than being driven by a single country, entity or multinational company; takes the view that, while legitimate law enforcement and intelligence concerns need to be taken into account in order to support the fight against terrorism, they should not lead to a general undermining of the dependability of all IT systems; expresses support for the recent decisions by the Internet Engineering Task Force (IETF) to include governments in the threat model for internet security;

95. Points out that EU and national telecom regulators, and in certain cases also telecom companies, have clearly neglected the IT security of their users and clients; calls on the Commission to make full use of its existing powers under the ePrivacy and Telecommunication Framework Directive to strengthen the protection of confidentiality of communication by adopting measures to ensure that terminal equipment is compatible with the right of users to control and protect their personal data, and to ensure a high level of security of telecommunication networks and services, including by way of requiring state-of-the-art end-to-end encryption of communications;

96. Supports the EU cyber strategy, but considers that it does not cover all possible threats and should be extended to cover malicious state behaviour; underlines the need for more robust IT security and resilience of IT systems;

97. Calls on the Commission, by January 2015 at the latest, to present an Action Plan to develop greater EU independence in the IT sector, including a more coherent approach to boosting European IT technological capabilities (including IT systems, equipment, services, cloud computing, encryption and anonymisation) and to the protection of critical IT infrastructure (including in terms of ownership and vulnerability);

98. Calls on the Commission, in the framework of the next Work Programme of the Horizon 2020 Programme, to direct more resources towards boosting European research, development, innovation and training in the field of IT, in particular privacy-enhancing technologies and infrastructures, cryptology, secure computing, the best possible security solutions including open-source security, and other information society services, and also to promote the internal market in European software, hardware, and encrypted means of communication and communication infrastructures, including by developing a comprehensive EU industrial strategy for the IT industry; considers that small and medium enterprises play a particular role in research; stresses that no EU funding should be granted to projects having the sole purpose of developing tools for gaining illegal access into IT systems;

99. Asks the Commission to map out current responsibilities and to review, by December 2014 at the latest, the need for a broader mandate, better coordination and/or additional resources and technical capabilities for ENISA, Europol's Cyber Crime Centre and other Union centres of specialised expertise, CERT-EU and the EDPS, in

order to enable them to play a key role in securing European communication systems, be more effective in preventing and investigating major IT breaches in the EU and performing (or assisting Member States and EU bodies to perform) on-site technical investigations regarding major IT breaches; in particular, calls on the Commission to consider strengthening ENISA's role in defending the internal systems within the EU institutions and to establish within ENISA's structure a Computer Emergency Response Team (CERT) for the EU and its Member States;

100. Requests the Commission to assess the need for an EU IT Academy that brings together the best independent European and international experts in all related fields, tasked with providing all relevant EU institutions and bodies with scientific advice on IT technologies, including security-related strategies;

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

- the need for regular, rigorous and independent security audits and penetration tests, with the selection of outside security experts ensuring transparency and guarantees of their credentials vis-à-vis third countries or any types of vested interest;

- the inclusion in tender procedures for new IT systems of best-practice specific IT security/privacy requirements, including the possibility of a requirement for open-source software as a condition of purchase or a requirement that trusted European companies should take part in the tender when sensitive, security-related areas are concerned;

- the list of companies under contract with Parliament in the IT and telecom fields, taking into account any information that has come to light about their cooperation with intelligence agencies (such as revelations about NSA contracts with a company such as RSA, whose products Parliament is using to supposedly protect remote access to their data by its Members and staff), including the feasibility of providing the same services by other, preferably European, companies;

- the reliability and resilience of the software, and especially off-the-shelf commercial software, used by the EU institutions in their IT systems with regard to penetrations and intrusions by EU or third-country law enforcement and intelligence authorities, taking also into account relevant international standards, best-practice security risk management principles, and adherence to EU Network Information Security standards on security breaches;

- the use of more open-source systems;

- steps and measures to take in order to address the increased use of mobile tools (e.g. smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;

- the security of the communications between the different workplaces of the Parliament and of the IT systems used in Parliament;

- the use and location of servers and IT centres for Parliament's IT systems and the implications for the security and integrity of the systems;

- the implementation in reality of the existing rules on security breaches and prompt notification of the competent authorities by the providers of publicly available telecommunication networks;

- the use of cloud computing and storage services by Parliament, including the nature of the data stored in the cloud, how the content and access to it is protected and where the cloud-servers are located, clarifying the applicable data protection and intelligence legal framework, as well as assessing the possibilities of solely using cloud servers that are based on EU territory;

- a plan allowing for the use of more cryptographic technologies, in particular end-to-end authenticated encryption for all IT and communications services such as cloud computing, email, instant messaging and telephony;

- the use of electronic signatures in email;

- a plan for using a default encryption standard, such as the GNU Privacy Guard, for emails that would at the same time allow for the use of digital signatures;

- the possibility of setting up a secure instant messaging service within Parliament allowing secure communication, with the server only seeing encrypted content;

102. Calls for all the EU institutions and agencies to perform a similar exercise in cooperation with ENISA, Europol and the CERTs, by December 2014 at the latest, in particular the European Council, the Council, the European External Action Service (including EU delegations), the Commission, the Court of Justice and the European Central Bank; invites the Member States to conduct similar assessments;

103. Stresses that as far as the external action of the EU is concerned, assessments of related budgetary needs should be carried out and first measures taken without delay in the case of the European External Action Service (EEAS) and that appropriate funds need to be allocated in the 2015 draft budget;

104. Takes the view that the large-scale IT systems used in the area of freedom, security and justice, such as the Schengen Information System II, the Visa Information System, Eurodac and possible future systems such as EU-ESTA, should be developed and operated in such a way as to ensure that data are not compromised as a result of requests by authorities from third countries; asks eu-LISA to report back to Parliament on the reliability of the systems in place by the end of 2014;

105. Calls on the Commission and the EEAS to take action at the international level, with the UN in particular, and in cooperation with interested partners to implement an EU strategy for democratic governance of the internet in order to prevent undue influence over ICANN's and IANA's activities by any individual entity, company or country by ensuring appropriate representation of all interested parties in these bodies, while avoiding the facilitation of state control or censorship or the balkanisation and fragmentation of the internet;

106. Calls for the EU to take the lead in reshaping the architecture and governance of the internet in order to address the risks related to data flows and storage, striving for more data minimisation and transparency and less centralised mass storage of raw data, as well as for rerouting of Internet traffic or full end-to-end encryption of all Internet traffic so as to avoid the current risks associated with unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy ;

107. Calls for the promotion of

- EU search engines and EU social networks as a valuable step in the direction of IT independence for the EU;

- European IT service providers;

- encrypting communication in general, including email and SMS communication;

- European IT key elements, for instance solutions for client-server operating systems, using open-source standards, developing European elements for grid coupling, e.g. routers;

108. Calls on the Member States, in cooperation with ENISA, Europol's CyberCrime Centre, CERTs and national data protection authorities and cybercrime units, to develop a culture of security and to launch an education and awareness-raising campaign in order to enable citizens to make a more informed choice regarding what personal data to put on-line and how better to protect them, including through encryption and safe cloud computing, making full use of the public interest information platform provided for in the Universal Service Directive;

109. Calls on the Commission, by December 2014, to put forward legislative proposals to encourage software and hardware manufacturers to introduce more security and privacy by design and by default features in their products, including by introducing disincentives for the undue and disproportionate collection of mass personal data and legal liability on the part of manufacturers for unpatched known vulnerabilities, faulty or insecure products or the installation of secret backdoors enabling unauthorised access to and processing of data; in this respect, calls on the Commission to evaluate the possibility of setting up a certification or validation scheme for IT hardware including testing procedures at EU level to ensure the integrity and security of the products;

Rebuilding trust

110. Believes that, beyond the need for legislative change, the inquiry has shown the need for the US to restore trust with its EU partners, as it is the US intelligence agencies' activities that are primarily at stake;

111. Points out that the crisis of confidence generated extends to:

– the spirit of cooperation within the EU, as some national intelligence activities may jeopardise the attainment of the Union's objectives;

– citizens, who realise that not only third countries or multinational companies but also their own government may be spying on them;

– respect for fundamental rights, democracy and the rule of law, as well as the credibility of democratic, judicial and parliamentary safeguards and oversight in a digital society;

Between the EU and the US

112. Recalls the important historical and strategic partnership between the EU Member States and the US, based on a common belief in democracy, the rule of law and fundamental rights;

113. Believes that the mass surveillance of citizens and the spying on political leaders by the US have caused serious damage to relations between the EU and the US and negatively impacted on trust in US organisations acting in the EU; this is further exacerbated by the lack of judicial and administrative remedies for redress under US law for EU citizens, particularly in cases of surveillance activities for intelligence purposes;

114. Recognises, in light of the global challenges facing the EU and the US, that the transatlantic partnership needs to be further strengthened, and that it is vital that transatlantic cooperation in counter-terrorism continues on a new basis of trust based on true common respect for the rule of law and the rejection of all indiscriminate practices of mass surveillance; insists, therefore, that clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership;

115. Is ready to engage in a dialogue with US counterparts so that, in the ongoing American public and congressional debate on reforming surveillance and reviewing intelligence oversight, the right to privacy and other rights of EU citizens, residents or other persons protected by EU law and equivalent information rights and privacy protection in US courts, including legal redress, are guaranteed through, for example, a revision of the Privacy Act and the Electronic Communications Privacy Act and by ratifying the First Optional Protocol to the International Covenant on Civil and Political Rights (ICCPR), so that the current discrimination is not perpetuated;

116. Insists that necessary reforms be undertaken and effective guarantees be given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is proportional, limited by clearly specified conditions, and related to reasonable suspicion and probable cause of terrorist activity; stresses that

this purpose must be subject to transparent judicial oversight;

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

118. Urges the Commission and the US Administration to address, in the context of the ongoing negotiations on an EU-US Umbrella Agreement on data transfer for law enforcement purposes, the information and judicial redress rights of EU citizens, and to conclude these negotiations, in line with the commitment made at the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013, before summer 2014;

119. Encourages the US to accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as it acceded to the 2001 Convention on Cybercrime, thus strengthening the shared legal basis between the transatlantic allies;

120. Calls on the EU institutions to explore the possibilities for establishing with the US a code of conduct which would guarantee that no US espionage is pursued against EU institutions and facilities;

Within the European Union

121. Also believes that the involvement and activities of EU Member States have led to a loss of trust, including among Member States and between EU citizens and their national authorities; is of the opinion that only full clarity as to purposes and means of surveillance, public debate and, ultimately, revision of legislation, including an end to mass surveillance activities and strengthening the system of judicial and parliamentary oversight, will it be possible to re-establish the trust lost; reiterates the difficulties involved in developing comprehensive EU security policies with such mass surveillance activities in operation, and stresses that the EU principle of sincere cooperation requires that Member States refrain from conducting intelligence activities in other Member States' territory;

122. Notes that some Member States are pursuing bilateral communication with the US authorities on spying allegations, and that some of them have concluded (the UK) or envisage concluding (Germany, France) so-called 'anti-spying' arrangements; stresses that these Member States need to observe fully the interests and the legislative framework of the EU as a whole; deems such bilateral arrangements to be counterproductive and irrelevant, given the need for a European approach to this problem; asks the Council to inform Parliament on developments by Member States on an EU-wide mutual no-spy arrangement;

123. Considers that such arrangements should not breach the Union Treaties, especially the principle of sincere cooperation (under Article 4(3) TEU), or undermine EU policies in general and, more specifically, the internal market, fair competition, and economic, industrial and social development; decides to review any such arrangements for their compatibility with European law, and reserves the right to activate Treaty procedures in the event of such arrangements being proven to contradict the Union's cohesion or the fundamental principles on which it is based;

124. Calls on the Member States to make every effort to ensure better cooperation with a view to providing safeguards against espionage, in cooperation with the relevant EU bodies and agencies, for the protection of EU citizens and institutions, European companies, EU industry, and IT infrastructure and networks, as well as European research; considers the active involvement of EU stakeholders to be a precondition for an effective exchange of information; points out that security threats have become more international, diffuse and complex, thereby requiring an enhanced European cooperation; believes that this development should be better reflected in the Treaties, and therefore calls for a revision of the Treaties in order to reinforce the notion of sincere cooperation between the Member States and the Union as regards the objective of achieving an area of security and to prevent mutual espionage between Member States within the Union;

125. Considers tap-proof communication structures (email and telecommunications, including landlines and cell phones) and tap-proof meeting rooms within all relevant EU institutions and EU delegations to be absolutely necessary; therefore calls for the establishment of an encrypted internal EU email system;

126. Calls on the Council and Commission to consent without further delay to the proposal adopted by the European Parliament on 23 May 2012 for a regulation of the European Parliament on the detailed provisions governing the exercise of the European Parliament's right of inquiry and repealing Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission presented on the basis of Article 226 TFEU; calls for a revision of the Treaty in order to extend such inquiry powers to cover, without restrictions or exceptions, all fields of Union competence or activity and to include the possibility of questioning under oath;

Internationally

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

128. Calls on the Member States to follow the call of the 35th International Conference of Data Protection and Privacy Commissioners 'to advocate the adoption of an additional protocol to 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;

129. Calls on the Member States to develop a coherent and strong strategy within the UN, supporting in particular the resolution on 'the right to privacy in the digital age' initiated by Brazil and Germany, as adopted by the Third Committee of the UN General Assembly Committee (Human Rights Committee) on 27 November 2013, as well as taking further action for the defence of the fundamental right to privacy and

data protection at an international level while avoiding any facilitation of state control or censorship or the fragmentation of the internet, including an initiative for an international treaty prohibiting mass surveillance activities and an agency for its oversight;

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

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

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

Action 1: Adopt the Data Protection Package in 2014;

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

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

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

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

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

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

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

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

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

133. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the parliaments and governments of the Member States, the national data protection authorities, the EDPS, eu-LISA, ENISA, the Fundamental Rights Agency, the Article 29 Working Party, the Council of Europe, the Congress of the United States of America, the US Administration, the President, Government and Parliament of the Federative Republic of Brazil, and the UN Secretary-General.

EXPLANATORY STATEMENT

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

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

Methodology

From July 2013, the LIBE Committee of Inquiry was responsible for the extremely challenging task of fulfilling the mandate[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

[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).

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

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

Reactions to mass surveillance and a public debate

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

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

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

The two types of reactions outlined above are based on a set of reasons which, if followed, may lead to quite opposed decisions as to how the EU should or should not react.

5 reasons not to act

– The 'Intelligence/national security argument': no EU competence

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

– The 'Terrorism argument': danger of the whistleblower

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

– The 'Treason argument: no legitimacy for the whistleblower

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

– The 'realism argument': general strategic interests

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

– The 'Good government argument': trust your government

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

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

[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'.

5 reasons to act

– The 'mass surveillance argument': in which society do we want to live?

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

– The 'fundamental rights argument':

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

– The 'EU internal security argument':

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

– The 'deficient oversight argument'

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

– The 'chilling effect on media' and the protection of whistleblowers

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

ANNEX I: LIST OF WORKING DOCUMENTS

LIBE Committee Inquiry

Rapporteur & Shadows as co-authors	Issues	EP resolution of 4 July2013 (see paragraphs 15-16)
Mr Moraes (S&D)	US and EU Member Surveillance programmes and their impact on EU citizens fundamental rights	16 (a) (b) (c) (d)
Mr Voss (EPP)	US surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation	16 (a) (b) (c)
Mrs In't Veld (ALDE) & Mrs Ernst (GUE)	Democratic oversight of Member State intelligence services and of EU intelligence bodies.	15, 16 (a) (c) (e)
Mr Albrecht (GREENS/EFA)	The relation between the surveillance practices in the EU and the US and the EU data protection provisions	16 (c) (e) (f)
Mr Kirkhope (ECR)	Scope of International, European and national security in the EU perspective[1]	16 (a) (b)
AFET 3 Members	Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens	16 (a) (b) (f)

[1] Not delivered.

ANNEX II: LIST OF HEARINGS AND EXPERTS

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

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

Date	Subject	Experts
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 • Jacob APPELBAUM, investigative journalist, software developer and computer security researcher with the Tor Project • 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 • Gerhard SCHMID (former MEP and Rapporteur of the ECHELON report 2001) • Duncan CAMPBELL, investigative journalist and author of the STOA report 'Interception Capabilities 2000'
12th September 2013 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	• Darius ŽILYS, Council Presidency, Director International Law Department, Lithuanian Ministry of Justice

	and cooperation with the LIBE Committee Inquiry (In camera)	(co-chair of the EU-US ad hoc working group on data protection) • Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection) • 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) **With AFET**	- Allegations of NSA tapping into the SWIFT data used in the TFTP programme	• Cecilia MALMSTRÖM, Member of the European Commission • Rob WAINWRIGHT, Director of Europol • 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) • Paul NEMITZ, Director DG JUST, European Commission (co-chair of the EU-US ad hoc working group on data protection) • 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) • Greg NOJEIM, Senior Counsel and Director of Project on Freedom, Security &

	- Effectiveness of surveillance in fighting crime and terrorism in Europe - Presentation of the study on the US surveillance programmes and their impact on EU citizens' privacy	Technology, Center for Democracy & Technology (CDT) (via videoconference) • Dr Reinhard KREISSL, Coordinator, Increasing Resilience in Surveillance Societies (IRISS) (via videoconference) • 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) **With AFET**	- Exchange of views with US Civil Society (Part II) - Whistleblowers' activities in the field of surveillance and their legal protection	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU) Statements by whistleblowers: • Thomas DRAKE, ex-NSA Senior Executive • J. Kirk WIEBE, ex-NSA Senior analyst • Annie MACHON, ex-MI5 Intelligence officer Statements by NGOs on legal protection of whistleblowers: • Jesselyn RADACK, lawyer and representative of 6 whistleblowers, Government Accountability Project • John DEVITT, Transparency International Ireland
3rd October 2013 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. • Mr Dirk LYBAERT, Secretary General, BELGACOM S.A. • 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 - impact of us surveillance programmes on other instruments for international transfers (contractual clauses, binding corporate rules)	• Dr Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (GERMANY) • Christopher CONNOLLY – Galexia • Peter HUSTINX, European Data Protection Supervisor (EDPS) • Ms Isabelle FALQUE-PIERROTIN, President of CNIL (FRANCE)
14th October 2013 15.00 - 18.30 (BXL)	- Electronic Mass Surveillance of EU Citizens and International, Council of Europe and EU Law - Court cases on Surveillance Programmes	• 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' • Judge Bostjan ZUPANČIČ, Judge at the ECHR (via videoconference) • Douwe KORFF, Professor of Law, London Metropolitan University • Dominique GUIBERT, Vice-Président of the 'Ligue des Droits de l'Homme' (LDH) • Nick PICKLES, Director of Big Brother Watch • 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 • 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)[1] (Venice Commission) (UK)	• Mr Iain CAMERON, Member of the European Commission for Democracy through Law - 'Venice Commission' • Mr Ian LEIGH, Professor of Law, Durham University • Mr David BICKFORD, Former Legal Director of the Security and intelligence agencies MI5 and MI6 • Mr Gus HOSEIN, Executive Director, Privacy International
	- EU-US transatlantic experts group	• Mr Paul NEMITZ, Director - Fundamental Rights and Citizenship, DG JUST, European Commission • Mr Reinhard PRIEBE, Director - Crisis Management and Internal Security, DG Home, European Commission
11th November 2013 15h-18.30 (BXL)	- US surveillance programmes and their impact on EU citizens' privacy (statement by Mr Jim SENSENBRENNER, Member of the US Congress)	• Mr Jim SENSENBRENNER, US House of Representatives, (Member of the Committee on the Judiciary and Chairman of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations)
	- 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) • Mr A.H. VAN DELDEN, Chair

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

		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) • Mr Nicklas LUNDBLAD, Director, Public Policy and Government Relations, Google • Mr Richard ALLAN, Director EMEA Public Policy, Facebook
14th November 2013 15.00 – 18.30 (BXL) **With AFET**	- IT Security of EU institutions (Part I) (EP, COM (CERT-EU), (eu-LISA)	• Mr Giancarlo VILELLA, Director General, DG ITEC, European Parliament • Mr Ronald PRINS, Director and co-founder of Fox-IT • Mr Freddy DEZEURE, head of task force CERT-EU, DG DIGIT, European Commission • Mr Luca ZAMPAGLIONE, Security Officer, eu-LISA
	- The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance (Part III)(BE, DA)	• Mr Armand DE DECKER, Vice-Chair of the Belgian Senate, Member of the Monitoring Committee of the Intelligence Services Oversight Committee • Mr Guy RAPAILLE, Chair of the Intelligence Services Oversight Committee (Comité R) • 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) - The impact of mass surveillance on confidentiality of lawyer-client relations	• Mr Olivier BURGERSDIJK, Head of Strategy, European Cybercrime Centre, EUROPOL • Prof. Udo HELMBRECHT, Executive Director of ENISA • Mr Florian WALTHER, Independent IT-Security consultant • Mr Jonathan GOLDSMITH, Secretary General, Council of Bars and Law Societies of Europe (CCBE)
9th December 2013 (STR)	- Rebuilding Trust on EU-US Data flows - Council of Europe Resolution 1954 (2013) on 'National security and access to information'	• Ms Viviane REDING, Vice President of the European Commission • 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) IT means of protecting privacy	• Ms Vanessa GRAZZIOTIN, Chair of the Parliamentary Committee of Inquiry on Espionage • Mr Ricardo DE REZENDE FERRAÇO, Rapporteur of the Parliamentary Committee of Inquiry on Espionage • Mr Bart PRENEEL, Professor in Computer Security and Industrial Cryptography in the University KU Leuven, Belgium • Mr Stephan LECHNER, Director, Institute for the Protection and Security of the Citizen (IPSC), - Joint Research Centre(JRC), European Commission • Dr Christopher SOGHOIAN, Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union

	Exchange of views with the journalist having made public the facts (Part II) (Videoconference)	• Christian HORCHERT, IT-Security Consultant, Germany • 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

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

1. Experts who declined the LIBE Chair's Invitation

US

- Mr Keith Alexander, General US Army, Director NSA[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

---

[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.

- Dr Saskia Horsch, Senior Manager Public Policy, Amazon

EU Telecommunication Companies

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

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

Netherlands

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

Sweden

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

RESULT OF FINAL VOTE IN COMMITTEE

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

Neist, Dennis

Von: Rensmann, Michael
Gesendet: Dienstag, 21. Januar 2014 15:24
An: Neist, Dennis
Cc: ref603; ref601; Bartodziej, Peter; Schmidt, Matthias
Betreff: WG: Bitte um Ergänzung und Mitzeichnung - Vorlage Leiter Büro ChBK zum LIBE-Report - heute, 16:00 Uhr

Anlagen: 20140121_Vorlage_BueroLChBK_LIBE.doc

Lieber Herr Neist,

mit den eingefügten Änderungen und Kürzungen für 132 mitgezeichnet.

Viele Grüße
Michael Rensmann

Von: Neist, Dennis
Gesendet: Dienstag, 21. Januar 2014 14:59
An: ref601; ref132
Cc: ref603
Betreff: Bitte um Ergänzung und Mitzeichnung - Vorlage Leiter Büro ChBK zum LIBE-Report - heute, 16:00 Uhr

Liebe Kolleginnen und Kollegen,

Ich bitte um Mitzeichnung der neuerlich modifizierten Vorlage zum LIBE-Bericht, in welcher nun auch die Stellungnahme BMI Eingang gefunden hat.



20140121_Vorlage_
BueroLChBK_LI...

Referat 132 bitte ich in der Vorlage insbesondere zu den angemerkten Punkten DatSchGrdVO und "Moratorium Transatlantisches Freihandelsabkommen" zu ergänzen.

Über eine Mitzeichnung bis heute, 16:00 Uhr, wäre ich Ihnen dankbar. Ich bitte die kurze Fristsetzung zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Neist, Dennis

Von: Polzin, Christina
Gesendet: Dienstag, 21. Januar 2014 15:53
An: Neist, Dennis; ref601; ref132
Cc: ref603
Betreff: AW: Bitte um Ergänzung und Mitzeichnung - Vorlage Leiter Büro ChBK zum LIBE-Report - heute, 16:00 Uhr

Lieber Herr Neist, 601 zeichnet mit. Gruß,

Christina Polzin
Bundeskanzleramt
Referatsleiterin 601
Willy-Brandt-Straße 1
10557 Berlin
Tel: +49 (0) 30 18 400 -2612
Fax.:+49-(0) 30 18 10 400-2612
E-Mail: christina.polzin@bk.bund.de

2 k 9

Von: Neist, Dennis
Gesendet: Dienstag, 21. Januar 2014 14:59
An: ref601; ref132
Cc: ref603
Betreff: Bitte um Ergänzung und Mitzeichnung - Vorlage Leiter Büro ChBK zum LIBE-Report - heute, 16:00 Uhr

Liebe Kolleginnen und Kollegen,

Ich bitte um Mitzeichnung der neuerlich modifizierten Vorlage zum LIBE-Bericht, in welcher nun auch die Stellungnahme BMI Eingang gefunden hat.

< Datei: 20140121_Vorlage_BueroLChBK_LIBE.doc >>

Referat 132 bitte ich in der Vorlage insbesondere zu den angemerkten Punkten DatSchGrdVO und "Moratorium Transatlantisches Freihandelsabkommen" zu ergänzen.

Über eine Mitzeichnung bis heute, 16:00 Uhr, wäre ich Ihnen dankbar. Ich bitte die kurze Fristsetzung zu entschuldigen.

Mit freundlichen Grüßen
Auftrag

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Referat 603

603 - 151 00 – Bu 10/14 NA 2 VS-NfD

ORR Neist

Berlin, 21. Januar 2014

Hausruf: 2662

Über

Herrn Referatsleiter 603 21/1

Herrn Ständigen Vertreter AL 6 21.1.

Herrn Abteilungsleiter 6 21.1.

Herrn Staatssekretär

1. Vorlage hat Herrn BL ChBK elektronisch vorgelegen.
2. Herrn AL 6 zum Rücklauf.

Herrn Büroleiter ChBK

1. Hr. BL ChBK hat mich unterrichtet die Änderungswünsche im BMI/DEP Voss vorgetragen zu haben. Sie wurden von dort kommuniziert
2. Hr. GL 6 ist informiert.
3. Z.K. 603 z.K.
4. z.d.A.

Betr.: Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) zum NSA Überwachungsprogramm
hier: Stellungnahme und Einbringung von Änderungsvorschlägen

Anlage: 1.) Änderungswünsche BMI per E-Mail an MdEP Voss vom 20. Januar 2014
2.) Stellungnahme BND vom 20. Januar 2014
3.) Schreiben Pr BND an LIBE-Ausschuss vom 16. Januar 2014

28/1 27.1.

I. Votum

- Telefonische Kontaktaufnahme durch Büroleiter ChBK zu MdEP Voss
- Unterstreichung der bereits übermittelten Anpassungsvorschläge des BMI
- Einbringung der Änderungsvorschläge des BND

II. Sachverhalt

Im Zuge des Bekanntwerdens der globalen Aufklärungsaktivitäten der NSA hat das Europäische Parlament per Entschließungsantrag am 04. Juli 2013 eine Arbeitsgruppe im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet und damit beauftragt, zur großflächigen

...

elektronischen Aufklärung gegen EU Bürger und Einrichtungen durch die amerikanischen Nachrichtendienste zu berichten. Hierzu hat der Ausschuss auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht verfasst. Dieser kommt zu dem Schluss, die NSA führe (teilweise gemeinsam mit Behörden aus dem Vereinigten Königreich, Kanada und Neuseeland) eine massenhafte Überwachung der elektronischen Kommunikation durch und verletze dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten. In Anbetracht dieser Feststellung wird im Bericht ein breites Maßnahmenbündel vorgeschlagen, welches u.a. der Überprüfung und Anpassung von Abkommen mit den USA, die Stärkung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), dem Europol-Cybercrime-Center (EC3) und des Europäischen Datenschutzbeauftragten (EDPS) sowie diversen Appellen an die Kommission und die Mitgliedstaaten vorsieht.

BMI (Büro PSt Schröder) hat hierzu folgende Änderungswünsche sowie weiterführende Erläuterungen am 20. Januar 2014 per E-Mail an MdEP Voss übermittelt (im Einzelnen siehe Anlage 1). Diese betreffen u.a.

- die Vermutung ähnlicher Programme in DEU
- die Aufforderung an DEU, seine Gesetzgebung zu überprüfen bzw. zu überarbeiten oder
- die Aufforderung an alle MS, die unterstellten Verletzungen ihrer Souveränität auch gerichtlich geltend zu machen.

Auch der BND geht in seiner Stellungnahme (Anlage 2) auf die Behauptung ein, DEU betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu sei festzustellen, dass für einen solchen Vergleich die Grundlage fehle. Für den Bundesnachrichtendienst sei festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetze.

Im Weiteren teilte der BND mit, dass der Präsident des Bundesnachrichten-dienstes am 16. Januar 2014 ein Schreiben an den Vorsitzenden des LIBE-

...

Ausschuss gerichtet habe, in welchem um Berichtigung der unzutreffenden Feststellung gebeten werde, der Präsident des BND habe sich nicht auf die Einladung zur Anhörung vor dem LIBE-Ausschuss zurückgemeldet (Anlage 3). Diese Rückmeldung sei nach Angaben des BND mit Schreiben vom 20. November 2013 erfolgt.

III. Bewertung und Änderungsvorschläge

In einer telefonischen Erörterung mit Herrn MdEP Voss sollten die Änderungsvorschläge des BMI ausdrücklich unterstützt werden. Die Frist zur Einbringung von Änderungsvorschlägen endet am 22. Januar 2014.
Ferner sollte beim Punkt DatSchGrdVO darauf hingewiesen werden, dass der Oktober-ER die Verabschiedung im Rahmen der Vollendung des digitalen Binnenmarkts bis 2015 als Ziel vorgegeben hat.

Ggf. könnte auch noch auf den sehr bedenklichen Punkt „Moratorium Transatlantisches Freihandelsabkommen“ hingewiesen werden.

Des Weiteren sollte möglichst auf folgende Änderungen mit Bezug zum BND hingewirkt werden:

1.)

S.16 (Main findings Nr.2 - Analog zum Vorschlag des BMI)::

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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill); believes that the existence of programmes of a similar nature, even if on a more limited scale, is likely in other EU countries such as France (DGSE), ***Germany (BND)*** *and Sweden (FRA);*

Streiche: , Germany (BND)

...

Begründung: Unzutreffende Feststellung, da die deutschen Sicherheitsbehörden ihre Arbeit unter Achtung der EU-Menschenrechtskonvention, der Einhaltung der nationalen gesetzlichen Regelungen sowie der Kontrolle durch das deutsche Parlament durchführen

2.)

S. 51-52 (Annex III – List of experts who declined participating in the LIBE Inquiry public hearings):

Streiche:

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

Germany: Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Setze:

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

Germany: Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Begründung: Der Präsident des Bundesnachrichtendienst, Herr Gerhard Schindler, teilte dem Vorsitzenden des LIBE-Ausschusses, Herrn Juan Fernando López Aguilar, in Schreiben vom 20. November 2013 mit, dass der Einladung nicht Folge geleistet werden könne. Er hat also gekniffen!

Referate 132, 413 und 601 haben mitgezeichnet.

(Dennis Neist)

Referat 603

Berlin, 21. Januar 2014

603 - 151 00 – Bu 10/14 NA 2 VS-NfD

ORR Neist

Hausruf: 2662

1. Vfg.

Über
Herrn Referatsleiter 603 21/1
Herrn Ständigen Vertreter AL 6 21.1.
Herrn Abteilungsleiter 6 21.1.
Herrn Staatssekretär ab am 22.1. Fli.

Herrn Büroleiter ChBK

Betr.: Berichtsentwurf des EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) zum NSA Überwachungsprogramm
hier: Stellungnahme und Einbringung von Änderungsvorschlägen

Anlage: 1.) Änderungswünsche BMI per E-Mail an MdEP Voss vom 20. Januar 2014
2.) Stellungnahme BND vom 20. Januar 2014
3.) Schreiben Pr BND an LIBE-Ausschuss vom 16. Januar 2014

I. Votum

- Telefonische Kontaktaufnahme durch Büroleiter ChBK zu MdEP Voss
- Unterstreichung der bereits übermittelten Anpassungsvorschläge des BMI
- Einbringung der Änderungsvorschläge des BND

II. Sachverhalt

Im Zuge des Bekanntwerdens der globalen Aufklärungsaktivitäten der NSA hat das Europäische Parlament per Entschließungsantrag am 04. Juli 2013 eine Arbeitsgruppe im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz

...

und Inneres (LIBE) eingerichtet und damit beauftragt, zur großflächigen elektronischen Aufklärung gegen EU Bürger und Einrichtungen durch die amerikanischen Nachrichtendienste zu berichten. Hierzu hat der Ausschuss auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht verfasst. Dieser kommt zu dem Schluss, die NSA führe (teilweise gemeinsam mit Behörden aus dem Vereinigten Königreich, Kanada und Neuseeland) eine massenhafte Überwachung der elektronischen Kommunikation durch und verletze dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten. In Anbetracht dieser Feststellung wird im Bericht ein breites Maßnahmenbündel vorgeschlagen, welches u.a. der Überprüfung und Anpassung von Abkommen mit den USA, die Stärkung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), dem Europol-Cybercrime-Center (EC3) und des Europäischen Datenschutzbeauftragten (EDPS) sowie diversen Appellen an die Kommission und die Mitgliedstaaten vorsieht.

BMI (Büro PSt Schröder) hat hierzu folgende Änderungswünsche sowie weiterführende Erläuterungen am 20. Januar 2014 per E-Mail an MdEP Voss übermittelt (im Einzelnen siehe Anlage 1). Diese betreffen u.a.

- die Vermutung ähnlicher Programme in DEU
- die Aufforderung an DEU, seine Gesetzgebung zu überprüfen bzw. zu überarbeiten oder
- die Aufforderung an alle MS, die unterstellten Verletzungen ihrer Souveränität auch gerichtlich geltend zu machen.

Auch der BND geht in seiner Stellungnahme (Anlage 2) auf die Behauptung eine, DEU betreibe ein dem "Überwachungsprogramm" der NSA vergleichbares Programm. Hierzu sei festzustellen, dass für einen solchen Vergleich die Grundlage fehle. Für den Bundesnachrichtendienst sei festzuhalten, dass er Mittel der technischen Fernmeldeaufklärung im vorgegebenen gesetzlichen Rahmen und ausschließlich zur Verfolgung ihm zugewiesener Aufgaben einsetze.

...

Im Weiteren teilte der BND mit, dass der Präsident des Bundesnachrichtendienstes am 16. Januar 2014 ein Schreiben an den Vorsitzenden des LIBE-Ausschuss gerichtet habe, in welchem um Berichtigung der unzutreffenden Feststellung gebeten werde, der Präsident des BND habe sich nicht auf die Einladung zur Anhörung vor dem LIBE-Ausschuss zurückgemeldet (Anlage 3). Diese Rückmeldung sei nach Angaben des BND mit Schreiben vom 20. November 2013 erfolgt.

III. Bewertung und Änderungsvorschläge

In einer telefonischen Erörterung mit Herrn MdEP Voss sollten die Änderungsvorschläge des BMI ausdrücklich unterstützt werden. Die Frist zur Einbringung von Änderungsvorschlägen endet am 22. Januar 2014.
Ferner sollte beim Punkt DatSchGrdVO darauf hingewiesen werden, dass der Oktober-ER die Verabschiedung im Rahmen der Vollendung des digitalen Binnenmarkts bis 2015 als Ziel vorgegeben hat.

Ggf. könnte auch noch auf den sehr bedenklichen Punkt „Moratorium Transatlantisches Freihandelsabkommen" hingewiesen werden.

Des Weiteren sollte möglichst auf folgende Änderungen mit Bezug zum BND hingewirkt werden:

1.)

S.16 (Main findings Nr.2 - Analog zum Vorschlag des BMI)::

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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill); believes that the existence of programmes of a similar nature, even if on a more limited scale, is likely in other EU countries such as France (DGSE), ***Germany (BND)*** *and Sweden (FRA);*

...

Streiche: , Germany (BND)

Begründung: Unzutreffende Feststellung, da die deutschen Sicherheits behörden ihre Arbeit unter Achtung der EU-Menschenrechtskonvention, der Einhaltung der nationalen gesetzlichen Regelungen sowie der Kontrolle durch das deutsche Parlament durchführen

2.)

S. 51-52 (Annex III – List of experts who declined participating in the LIBE Inquiry public hearings):

Streiche:

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

Germany: Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Setze:

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

Germany: Mr Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Begründung: Der Präsident des Bundesnachrichtendienst, Herr Gerhard Schindler, teilte dem Vorsitzenden des LIBE-Ausschusses, Herrn Juan Fernando López Aguilar, in Schreiben vom 20. November 2013 mit, dass der Einladung nicht Folge geleistet werden könne.

Referate 132, 413 und 601 haben mitgezeichnet.

(Dennis Neist)

2. 601 m.d.B. um Ergänzung und Mitzeichnung
3. 132 m.d.B. um Ergänzung und Mitzeichnung
4. 413 m.d.B. um Ergänzung und Mitzeichnung

} Mitzeichnung erfolgte per Mail Ne 27.2.14

4. ab
5. WV 603

000257

EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2013/2188(INI)

24.1.2014

AMENDMENTS
1 - 265

Draft report
Claude Moraes
(PE526.085v02-00)

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))

Motion for a resolution	*Amendment*
1. Considers that recent revelations in the press ***by whistleblowers and journalists***, together with the expert evidence given during this inquiry, 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 and location data and metadata of all citizens around the world on an unprecedented scale and in an indiscriminate and non-suspicion-based manner;	1. Considers that recent revelations in the press, together with the expert evidence given during this inquiry, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems to collect, store and analyse communication and location data and metadata of all citizens around the world on an unprecedented scale and in an indiscriminate and non-suspicion-based manner; ***recalls the importance of strengthening the existing structures in the Member States against mass surveillance; therefore considers of utmost importance a decentralised structure for the purpose of data retention;***

Or. en

Amendment 125
Timothy Kirkhope
on behalf of the ECR Group
Motion for a resolution
Paragraph 2

Motion for a resolution	*Amendment*
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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill); believes that the existence of programmes of a similar nature, even if	***deleted***

on a more limited scale, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA);

Or. en

Amendment 126
Jan Philipp Albrecht, Judith Sargentini, Jean Lambert, Hélène Flautre, Rui Tavares, Raül Romeva i Rueda
Motion for a resolution
Paragraph 2

Motion for a resolution	*Amendment*
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 ***its*** upstream surveillance activity (Tempora programme) and decryption programme (Edgehill); ***believes*** that the existence of programmes of a similar nature, even if on a more limited ***scale***, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA);	2. Points ***out*** 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) and ***the*** decryption programme (Edgehill); ***the targeted man-in-the-middle attacks on information systems (Quantumtheory and Foxacid programmes); the collection and retention of 200 million SMS text messages per day (Dishfire programme); considers*** that the existence of programmes of a similar nature, even if on a more limited ***dimension***, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA);

Or. en

Amendment 127
Axel Voss, Anna Maria Corazza Bildt, Véronique Mathieu Houillon, Agustín Díaz de Mera García Consuegra, Teresa Jiménez-Becerril Barrio, Arnaud Danjean, Salvador Sedó i Alabart

Motion for a resolution
Paragraph 2

Motion for a resolution	*Amendment*
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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill); ***believes that the existence of programmes of a similar nature, even if on a more limited scale, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA);***	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 its upstream surveillance activity (Tempora programme) and decryption programme (Edgehill);

Or. en

Amendment 128
Anna Maria Corazza Bildt
Motion for a resolution
Paragraph 2 a (new)

Motion for a resolution	*Amendment*
	2a. Welcomes the recent declarations by President Obama to reform the NSA and its programmes, with a view to improve data protection safeguards also for non-US citizens;

Or. en

Amendment 129
Timothy Kirkhope
on behalf of the ECR Group
Motion for a resolution
Paragraph 3

000261

Kleidt, Christian

Von: Karl, Albert
Gesendet: Dienstag, 25. Februar 2014 13:08
An: ref603
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA
Anlagen: NSA Bericht_Konsolidierter Text.doc
Friederike bitte R

L.Vg 603 · Bu 10 NA 2

Von: Schäper, Hans-Jörg
Gesendet: Dienstag, 25. Februar 2014 12:09
An: Karl, Albert
Cc: Heiß, Günter
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Lieber Albert,

anliegende E-Mail sowie den beigefügten Bericht leite ich Dir mit der Bitte um Prüfung zu.

Vielen Dank und beste Grüße
Hans-Jörg

Von: Semmler, Jörg
Gesendet: Dienstag, 25. Februar 2014 10:04
An: Maas, Carsten; Schäper, Hans-Jörg
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Lieber Carsten, lieber Herr Schäper,

anliegenden Bericht zur Kenntnis und kritischen Durchsicht.

Dank und Gruß,

J. Semmler

Von: TOPORAN Selma [mailto:selma.toporan@europarl.europa.eu]
Gesendet: Montag, 24. Februar 2014 19:54
An: Semmler, Jörg
Betreff: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,
im Namen von Herrn Voss danke Ich Ihnen zunächst für die sehr gute Kooperation, Ihre Unterstützung und qualitativ hochwertige Expertise, die Sie uns im Vorfeld unsrer Frist für Änderungsanträge zum Beicht von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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" zur Verfügung gestellt haben.
Anbei sende ich Ihnen im Auftrag von Herrn Voss den konsolidierten Bericht zum Überwachungsprogramm der US-amerikanischen NSA mit der Bitte um Weiterleitung an Herrn BM Peter Altmaier.
Der Bericht stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Über die 521 Änderungsanträge und 74 Kompromisse wurden im Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) am 12.Februar abgestimmt. Das Europäische Parlament entscheidet in einer Plenarabstimmung am 12. März über den konsolidierten Text.
Die wichtigsten Ergebnisse sind ab Seite 20 und die Empfehlungen ab Seite 24 dargestellt. Leider liegt der

konsolidierte Text bislang nur in Englisch vor.
Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist höchstwahrscheinlich der 5. März.
Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.
Mit freundlichen Grüßen,
Selma Toporan

Selma Toporan
(Parlamentarische Referentin)
Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel
Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: TOPORAN Selma
Sent: 30 January 2014 19:41
To: 'Semmler, Jörg'
Subject: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,
vielen Dank für Ihre Email. Ich habe den Brief entsprechend weitergeleitet und mir wurde mündlich zugesichert, dass die Änderung im Endbericht vollzogen werden soll. Der Endbericht, der im März im Plenum des Europäischen Parlaments zur Abstimmung steht, soll dann rechtmäßig BND -Präsidenten Herrn Gerhard Schinlder im Annex unter der Kategorie "Sachverständige, die die Einladung des LIBE-Vorsitzes abgelehnt haben" geführt werden.

Vielen Dank für Ihre Kooperation.
Beste Grüße nach Berlin,
Selma Toporan

Selma Toporan
(Parlamentarische Referentin)
Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel
Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: Semmler, Jörg [mailto:Joerg.Semmler@bk.bund.de]
Sent: 30 January 2014 19:08
To: TOPORAN Selma
Subject: AW: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrte Frau Toporan,
anbei eine Kopie des Absage-Schreibens des BND-Präsidenten.
Besten Dank und Gruß,

Dr. Jörg Semmler
Leiter des Büros des Chefs des Bundeskanzleramtes
Willy-Brandt-Str. 1
10557 Berlin

Tel.: 030 -18 400 2072
Fax: 030 -18 400 2359
E-Mail: joerg.semmler@bk.bund.de

Von: TOPORAN Selma [mailto:selma.toporan@europarl.europa.eu]
Gesendet: Montag, 27. Januar 2014 18:49
An: Semmler, Jörg
Betreff: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,
ich danke Ihnen noch einmal vielmals für das ausgiebige Telefonat vergangene Woche zum Thema Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA. Das Gespräch war wirklich sehr hilfreich und hat zur Erarbeitung der Änderungsanträge beigetragen.
Wie ich Ihnen bereits telefonisch gesagt habe, lassen sich die Annexe nicht verändern. Im Rahmen eines internen Treffens, habe ich Ihren Kritikpunkt angesprochen und gefordert, dass der Annex entsprechen geändert wird, da Herr Gerhard Schindler seine Teilnahme schriftlich abgesagt hat und es somit eine Antwort gab hingegen der Darstellung im Annex. Um diese Argumentation fortzuführen und das Sekretariat zu bitten, diese Änderung vorzunehmen, wäre es hilfreich, wenn Sie uns einen Scan des Antwortbriefs von Herrn Schindler zukommen lassen könnten, sofern möglich.
Falls Sie noch Fragen haben oder Informationen benötigen, können Sie sich gerne bei mir melden.
Mit freundlichen Grüßen,
Selma Toporan

Selma Toporan
(Parlamentarische Referentin)
Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel
Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: VOSS Axel
Sent: 10 January 2014 18:16
To: 'joerg.semmler@bk.bund.de'
Subject: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA
Sehr geehrter Herr Dr. Semmler,
anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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" mit der Bitte um Weiterleitung an Herrn BM Peter Altmaier.
Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

MAT A BK-1-4s.pdf, Blatt 277

Herr Voss hat mich vor allem darum gebeten, Herrn MB Altmaier auf folgende Absätze hinzuweisen: Absatz 2 (Seite 16); Absatz 10 (Seite 17); Absatz 20 (Seite19). Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.
Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.
Mit freundlichen Grüßen,
Selma Toporan

Selma Toporan
(Parlamentarische Referentin)
Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel
Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

MAT A BK-1-4s.pdf, Blatt 278

Neist, Dennis

Von: Karl, Albert
Gesendet: Dienstag, 28. Januar 2014 14:30
An: ref603
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

DENNIS bitte übernehmen

Von: Polzin, Christina
Gesendet: Dienstag, 28. Januar 2014 13:47
An: Karl, Albert
Cc: Schäper, Hans-Jörg
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Lieber Albert, das Schreiben von Herrn Schinidler habt ihr, ne ? Schickst du es Herrn Semmler ?

Gruß, Christina

Christina Polzin
Bundeskanzleramt
Referatsleiterin 601
Willy-Brandt-Straße 1
10557 Berlin
Tel: +49 (0) 30 18 400 -2612
Fax.:+49-(0) 30 18 10 400-2612
E-Mail: christina.polzin@bk.bund.de

Von: Schäper, Hans-Jörg
Gesendet: Dienstag, 28. Januar 2014 13:02
An: Polzin, Christina
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Liebe Frau Polzin,

bitte seien Sie so freundlich, Herrn Semmler das gescannte Schreiben des BND-Präsidenten zuzuleiten. Er wird es an das Büro MdEP Voss übersenden.

Vielen Dank und beste Grüße
Hans-Jörg Schäper

Von: Semmler, Jörg
Gesendet: Dienstag, 28. Januar 2014 12:29
An: Schäper, Hans-Jörg
Cc: Maas, Carsten
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Lieber Herr Schäper,

lassen Sie mich wissen, wie wir weiter verfahren wollen.

Dank und Gruß,

MAT A BK-1-4s.pdf, Blatt 279

J. Semmler

Von: TOPORAN Selma [mailto:selma.toporan@europarl.europa.eu]
Gesendet: Montag, 27. Januar 2014 18:49
An: Semmler, Jörg
Betreff: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

ich danke Ihnen noch einmal vielmals für das ausgiebige Telefonat vergangene Woche zum Thema Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA. Das Gespräch war wirklich sehr hilfreich und hat zur Erarbeitung der Änderungsanträge beigetragen.

Wie ich Ihnen bereits telefonisch gesagt habe, lassen sich die Annexe nicht verändern. Im Rahmen eines internen Treffens, habe ich Ihren Kritikpunkt angesprochen und gefordert, dass der Annex entsprechen geändert wird, da Herr Gerhard Schindler seine Teilnahme schriftlich abgesagt hat und es somit eine Antwort gab hingegen der Darstellung im Annex. Um diese Argumentation fortzuführen und das Sekretariat zu bitten, diese Änderung vorzunehmen, wäre es hilfreich, wenn Sie uns einen Scan des Antwortbriefs von Herrn Schindler zukommen lassen könnten, sofern möglich.

Falls Sie noch Fragen haben oder Informationen benötigen, können Sie sich gerne bei mir melden.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: VOSS Axel
Sent: 10 January 2014 18:16
To: 'joerg.semmler@bk.bund.de'
Subject: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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" mit der Bitte um Weiterleitung an Herrn BM Peter Altmaier.

Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Herr Voss hat mich vor allem darum gebeten, Herrn MB Altmaier auf folgende Absätze hinzuweisen: Absatz 2 (Seite 16); Absatz 10 (Seite 17); Absatz 20 (Seite19).

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

MAT A BK-1-4s.pdf, Blatt 281

Neist, Dennis

Von: Neist, Dennis
Gesendet: Dienstag, 28. Januar 2014 14:50
An: Semmler, Jörg
Cc: ref603; ref601; Schäper, Hans-Jörg; Heiß, Günter; Maas, Carsten
Betreff: AW: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA
Anlagen: 20131120_Schreiben_PrBND_LIBE-Ausschuss_Absage.pdf

Sehr geehrter Herr Dr. Semmler,

anbei erhalten Sie wie erbeten eine digitale Kopie des angefragten Antwortbriefs vom Präsidenten des Bundesnachrichtendiensts, Herrn Schindler, an den Vorsitzenden des LIBE-Ausschusses, Herr Juan Fernandez López Aguilar, vom 20. November 2013.

Mit freundlichen Grüßen
Im Auftrag

2/g 603 - 84 10 NAL

Dennis Neist
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: dennis.neist@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Semmler, Jörg
Gesendet: Dienstag, 28. Januar 2014 12:29
An: Schäper, Hans-Jörg
Cc: Maas, Carsten
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Lieber Herr Schäper,

lassen Sie mich wissen, wie wir weiter verfahren wollen.

Dank und Gruß,

J. Semmler

Von: TOPORAN Selma [mailto:selma.toporan@europarl.europa.eu]
Gesendet: Montag, 27. Januar 2014 18:49
An: Semmler, Jörg
Betreff: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

ich danke Ihnen noch einmal vielmals für das ausgiebige Telefonat vergangene Woche zum Thema Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA. Das Gespräch war wirklich sehr hilfreich und hat zur Erarbeitung der Änderungsanträge beigetragen.

MAT A BK-1-4s.pdf, Blatt 282

Wie ich Ihnen bereits telefonisch gesagt habe, lassen sich die Annexe nicht verändern. Im Rahmen eines internen Treffens, habe ich Ihren Kritikpunkt angesprochen und gefordert, dass der Annex entsprechen geändert wird, da Herr Gerhard Schindler seine Teilnahme schriftlich abgesagt hat und es somit eine Antwort gab hingegen der Darstellung im Annex. Um diese Argumentation fortzuführen und das Sekretariat zu bitten, diese Änderung vorzunehmen, wäre es hilfreich, wenn Sie uns einen Scan des Antwortbriefs von Herrn Schindler zukommen lassen könnten, sofern möglich.

Falls Sie noch Fragen haben oder Informationen benötigen, können Sie sich gerne bei mir melden.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: VOSS Axel
Sent: 10 January 2014 18:16
To: 'joerg.semmler@bk.bund.de'
Subject: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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" mit der Bitte um Weiterleitung an Herrn BM Peter Altmaier.

Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Herr Voss hat mich vor allem darum gebeten, Herrn MB Altmaier auf folgende Absätze hinzuweisen:

MAT A BK-1-4s.pdf, Blatt 283

000270

Absatz 2 (Seite 16); Absatz 10 (Seite 17); Absatz 20 (Seite19).

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

Bundesnachrichtendienst

Gerhard Schindler
Präsident

20. November 2013

Herrn
Juan Fernando López Aguilar
Vorsitzender
Committee on Civil Liberties, Justice
and Home Affairs
Europäisches Parlament
Brüssel

Belgien

Sehr geehrter Herr López Aguilar,

zunächst bedanke ich mich für Ihr Schreiben vom 14. Oktober 2013, in dem sie mich zu einer Anhörung des von Ihnen geleiteten Komitees einladen.

Die Arbeit und Zielsetzung Ihres Komitees begrüße ich ausdrücklich; hierbei beziehe ich mich insbesondere auf die Wahrung der Rechte der EU – Bürgerinnen und – Bürger, die im Einklang mit der Europäischen Menschenrechtskonvention stehen. Diese wird in der Bundesrepublik Deutschland in höchstem Maße gewürdigt und selbstverständlich auch von den deutschen Nachrichtendiensten geachtet.

Die drei deutschen Nachrichtendienste sind dem deutschen Gesetz gegenüber verpflichtet und richten ihre Arbeit daran aus, dies gilt auch für den Umgang mit Informationen, die nicht selbst erhoben wurden. Das deutsche Parlament hat hierauf stets sein Augenmerk gerichtet und wird dies auch in Zukunft tun. Um dies zu gewährleisten, wurden geeignete Mechanismen entwickelt, wie Gremien zur Aufsicht, Kontrolle und Überwachung.

Auch wenn ich bedauerlicherweise Ihre Einladung nicht annehmen kann, wünsche ich Ihnen alles Gute und eine glückliche Hand für ihre Arbeit.

Mit freundlichen Grüßen

(Gerhard Schindler)

EUROPEAN PARLIAMENT

2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

LIBE(2014)0130_1

DRAFT AGENDA

Meeting

Thursday 30 January 2014, 9.00 – 12.30
Room: József Antall (6Q2)

Thursday 30 January 2014, 14.00 – 17.30
Room: Paul-Henri Spaak (3C50)

Brussels

1. **Adoption of agenda**

2. **Chair's announcements**

   PLEASE NOTE THAT ALL TIME SLOTS ARE ONLY INDICATIVE AND ARE SUBJECT TO CHANGE DURING THE MEETING!

30 January 2014, 9.00 – 9.40

3. **State of play of on-going interinstitutional negotiations in legislative procedures**
   LIBE/7/11557

4. **Amendment to Decision 2005/681/JHA establishing the European Police College (CEPOL)**
   LIBE/7/14751
   ***I 2013/0812(COD) 17043/2013 – C7-0435/2013

Rapporteur:	Kinga Gál (PPE)	PR – PE526.113v01-00
Responsible:	LIBE –	
Opinions:	BUDG –	

- Consideration of draft report
- Decision on deadline for tabling amendments
- Deadline for tabling amendments: **4 February 2014, 12.00**

30 January 2014, 9.40 – 10.00

5. Evaluation of justice in relation to criminal justice and the rule of law
LIBE/7/15038
2014/2006(INI)

Rapporteur:	Kinga Göncz (S&D)	PR – PE527.913v01-00
Responsible:	LIBE –	

- Consideration of amendments

30 January 2014, 10.00 – 11.30

**** Electronic vote ****

6. European Union Agency for Law Enforcement Cooperation and Training (Europol) and repeal of Decisions 2009/371/JHA and 2005/681/JHA
LIBE/7/12427
***I 2013/0091(COD) COM(2013)0173 – C7-0094/2013

Rapporteur:	Agustín Díaz de Mera García Consuegra (PPE)		PR – PE513.116v01-00 AM – PE519.813v01-00 AM – PE519.786v01-00 DV – PE513.126v01-00
Responsible:	LIBE –		
Opinions:	BUDG –	Jutta Haug (S&D)	AD – PE510.878v02-00 AM – PE514.688v01-00
	CONT –	Inés Ayala Sender (S&D)	AD – PE514.840v04-00 AM – PE519.545v01-00

EMPL – Decision: no opinion
JURI – Decision: no opinion

AFCO – Alexandra Thein (ADLE)

CM – PE514.704v01-00
CM – PE514.566v01-00
CM – PE514.701v01-00
AD – PE513.290v02-00
AM – PE516.853v01-00

ŏ Adoption of draft report

7. Implementation of the Treaty of Lisbon with respect to the European Parliament
LIBE/7/14097
2013/2130(INI)

Rapporteur for the opinion: Nuno Melo (PPE) — PA – PE524.605v01-00, AM – PE524.619v01-00

Responsible: AFCO – Paulo Rangel (PPE) — PR – PE526.057v01-00, DV – PE527.969v01-00

ŏ Adoption of draft opinion

8. Deployment of the eCall in-vehicle system
LIBE/7/14576
***I 2013/0165(COD) COM(2013)0316 – C7-0174/2013

Rapporteur for the opinion: Axel Voss (PPE) — PA – PE524.542v01-00, AM – PE524.689v02-00

Responsible: IMCO* – Olga Sehnalová (S&D) — PR – PE521.605v01-00, AM – PE523.081v01-00

ŏ Adoption of draft opinion

*** ***End of electronic vote*** ***

30 January 2014, 11.30 – 12.00

Joint debate

9. EU-Azerbaijan Agreement on the readmission of persons residing without authorisation
LIBE/7/14478
*** 2013/0358(NLE) COM(2013)0744

Rapporteur : Mariya Gabriel (PPE) PR – PE527.921v01-00

Responsible: LIBE –

Opinions: AFET – Anneli Jäätteenmäki (ADLE) PA – PE526.104v01-00

- Presentation by the Commission and 1st exchange of views

10. EU-Azerbaijan Agreement on the facilitation of the issuance of visas
LIBE/7/14436
*** 2013/0356(NLE) COM(2013)0742

Rapporteur : Mariya Gabriel (PPE) PR – PE527.928v01-00

Responsible: LIBE –

Opinions: AFET – Anneli Jäätteenmäki (ADLE) PA – PE526.103v01-00

- Presentation by the Commission and 1st exchange of views

30 January 2014, 12.00 – 12.30

11. European Public Prosecutor's Office
LIBE/7/13509

Rapporteur : Salvatore Iacolino (PPE)

- Consideration of amendments

30 January 2014, 14.00 – 15.00

12. The US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs
LIBE/7/13778
2013/2188(INI)

Rapporteur :	Claude Moraes (S&D)	PR – PE526.085v02-00 DT – PE524.632v01-00 DT – PE523.025v02-00 DT – PE524.799v01-00 DT – PE524.633v01-00
Responsible:	LIBE –	
Opinions:	AFET – Decision: no opinion INTA – Decision: no opinion ITRE –	

- Consideration of amendments

30 January 2014, 15.00 – 16.00

13. Communication from the Commission to the European Parliament and the Council on the work of the Task Force Mediterranean
COM(2013)0869

- Presentation by Mr Muschel, Director on Migration and Asylum, DG HOME, European Commission

30 January 2014, 16.00 – 16.30

14. Public access to documents (Rule 104(7)) for the years 2011-2013
LIBE/7/13390
2013/2155(INI)

Rapporteur :	Sophia in 't Veld (ADLE)	PR – PE524.641v01-00 AM – PE526.326v01-00
Responsible:	LIBE –	

- Consideration of amendments

15. Any other business

30 January 2014, 16.30 – 17.30

In camera

16. Modernisation of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
LIBE/7/14101

- Presentation by Françoise Le Bail, Director-General for Justice and debriefing on the negotiations with the United States on the so-called "umbrella agreement"

17. Next meeting(s)

- 3 February 2014 (Strasbourg)

- 12 February 2014, 9.00 – 12.30 and 15.00 – 18.30 (Brussels)
- 13 February 2014, 9.00 – 12.30 and 15.00 – 18.30 (Brussels)

Neist, Dennis

Von: Karl, Albert
Gesendet: Freitag, 31. Januar 2014 10:51
An: ref603
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

zV

VG
AK

z.Vg. 603-Bu 10 NAZ

Von: Schäper, Hans-Jörg
Gesendet: Freitag, 31. Januar 2014 10:39
An: Heiß, Günter
Cc: Karl, Albert
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Lieber Günter,

die Information zum aktuellen Stand sende ich auch Dir m.d.B. um Kenntnisnahme.

Beste Grüße
Hans-Jörg

Von: Semmler, Jörg
Gesendet: Freitag, 31. Januar 2014 10:31
An: Schäper, Hans-Jörg
Cc: Maas, Carsten
Betreff: WG: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

zur Kenntnis, Gruß J. Semmler

Von: TOPORAN Selma [mailto:selma.toporan@europarl.europa.eu]
Gesendet: Donnerstag, 30. Januar 2014 19:41
An: Semmler, Jörg
Betreff: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,
vielen Dank für Ihre Email. Ich habe den Brief entsprechend weitergeleitet und mir wurde mündlich zugesichert, dass die Änderung im Endbericht vollzogen werden soll. Der Endbericht, der im März im Plenum des Europäischen Parlaments zur Abstimmung steht, soll dann rechtmäßig BND -Präsidenten Herrn Gerhard Schinlder im Annex unter der Kategorie "Sachverständige, die die Einladung des LIBE-Vorsitzes abgelehnt haben" geführt werden.

Vielen Dank für Ihre Kooperation.

Beste Grüße nach Berlin,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

MAT A BK-1-4s.pdf, Blatt 292

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: Semmler, Jörg [mailto:Joerg.Semmler@bk.bund.de]
Sent: 30 January 2014 19:08
To: TOPORAN Selma
Subject: AW: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrte Frau Toporan,

anbei eine Kopie des Absage-Schreibens des BND-Präsidenten.

Besten Dank und Gruß,

Dr. Jörg Semmler
Leiter des Büros des Chefs des Bundeskanzleramtes
Willy-Brandt-Str. 1
10557 Berlin

Tel.: 030 -18 400 2072
Fax: 030 -18 400 2359
E-Mail: joerg.semmler@bk.bund.de

Von: TOPORAN Selma [mailto:selma.toporan@europarl.europa.eu]
Gesendet: Montag, 27. Januar 2014 18:49
An: Semmler, Jörg
Betreff: RE: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

ich danke Ihnen noch einmal vielmals für das ausgiebige Telefonat vergangene Woche zum Thema Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA. Das Gespräch war wirklich sehr hilfreich und hat zur Erarbeitung der Änderungsanträge beigetragen.

Wie ich Ihnen bereits telefonisch gesagt habe, lassen sich die Annexe nicht verändern. Im Rahmen eines internen Treffens, habe ich Ihren Kritikpunkt angesprochen und gefordert, dass der Annex entsprechen geändert wird, da Herr Gerhard Schindler seine Teilnahme schriftlich abgesagt hat und es somit eine Antwort gab hingegen der Darstellung im Annex. Um diese Argumentation fortzuführen und das Sekretariat zu bitten, diese Änderung vorzunehmen, wäre es hilfreich, wenn Sie uns einen Scan des Antwortbriefs von Herrn Schindler zukommen lassen könnten, sofern möglich.

MAT A BK-1-4s.pdf, Blatt 293

Falls Sie noch Fragen haben oder Informationen benötigen, können Sie sich gerne bei mir melden.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

From: VOSS Axel
Sent: 10 January 2014 18:16
To: 'joerg.semmler@bk.bund.de'
Subject: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Semmler,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "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" mit der Bitte um Weiterleitung an Herrn BM Peter Altmaier.

Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Herr Voss hat mich vor allem darum gebeten, Herrn MB Altmaier auf folgende Absätze hinzuweisen: Absatz 2 (Seite 16); Absatz 10 (Seite 17); Absatz 20 (Seite19).

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

MAT A BK-1-4s.pdf, Blatt 294

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302
Fax:+32-2-28 49302
Email: selma.toporan@europarl.europea.eu

MAT A BK-1-4s.pdf, Blatt 295

000282

Committee on Civil Liberties, Justice and Home Affairs
The Chairman

IPOL-COM-LIBE D (2014) 6682

200825 06.02.2014

Herrn
Gerhard SCHINDLER
Präsident
Bundesnachrichtendienst
Postfach 45 01 71
12171 Berlin
Germany

Sehr geehrter Herr Schindler,

Herzlichen Dank für Ihre Schreiben vom 20. November 2013 sowie vom 16. Januar 2014 und besonders auch für Ihr darin zum Ausdruck gebrachtes Interesse an der Arbeit des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres und Ihre Hinweise über die Arbeit des Bundesnachrichtendienstes.

Ich bedauere die fälschliche Erwähnung Ihres Namens im Anhang des Berichtsentwurfs in der Liste der Personen, die nicht auf meine Einladung geantwortet haben. Dies wird in der endgültigen Fassung korrigiert werden. Ihr Name wird dann nicht unter der Liste der Personen, die nicht auf meine Einladung geantwortet haben, aufgeführt werden, sondern auf der Liste derer, die meine Einladung abgelehnt haben.

Zur Erläuterung möchte ich anfügen, dass Ihr Schreiben vom 20. November dem Parlament am 30. Dezember über die Ständige Vertretung übermittelt wurde und am 3. Januar als im Parlament eingegangen registriert wurde. Zu diesem Zeitpunkt war der Berichtsentwurf bereits fertiggestellt.

Ich bedauere sehr, dass Sie meiner Einladung nicht folgen konnten, denn es war und bleibt mein Anliegen, alle Seiten und Argumente zu hören. Wenn Ihnen eine Annahme meiner Einladung zu einem späteren Zeitpunkt möglich sein sollte, so würde ich dies begrüßen.

Mit freundlichen Grüßen

Juan Fernando López Aguilar

IP-LIBE@europarl.europa.eu
B-1047 Brussels - Tel. +32 2 284 06 60 - Fax +32 2 284 49 41
F-67070 Strasbourg - Tel. +33 3 88 17 44 20 - Fax +33 3 88 17 90 40

MAT A BK-1-4s.pdf, Blatt 296

000283

Kleidt, Christian

Von: Kleidt, Christian
Gesendet: Dienstag, 11. Februar 2014 16:19
An: al6; Schäper, Hans-Jörg; Maas, Carsten
Cc: ref603
Betreff: WG: Transfer von: PLSA-HH-RECHT-SI/DAND%DAND@vsit.dand.de: Weiterleitung ans BKAmt
Anlagen: 140211_LIBE-Ausschuss-Pr_Reaktion auf Schreiben BND.pdf

Lieber Herr Heiß, lieber Herr Schäper, lieber Herr Dr. Maas,

der BND übermittelte anliegendes Schreiben des Vorsitzenden des LIBE-Ausschusses an Pr BND zK.
BL ChefBK war seinerzeit in den Vorgang involviert; seine Beteiligung rege ich an.

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: transfer@bnd.bund.de [mailto:transfer@bnd.bund.de]
Gesendet: Dienstag, 11. Februar 2014 11:14
An: ref603
Betreff: WG: Transfer von: PLSA-HH-RECHT-SI/DAND%DAND@vsit.dand.de: Weiterleitung ans BKAmt

Mit freundlichen Grüßen

IT-Leitstand

Betr.: Draft Report des LIBE-Committees (2013/2188(INI)) zum NSA-Überwachungsprogramm
hier: Übersendung eines Schreibens des LIBE-Committees
Bezug: laufender Vorgang

Sehr geehrte Damen und Herren,

in vorgenannter Angelegenheit lasse ich Ihnen anliegend ein Schreiben des LIBE-Committees (Reaktion auf die Schreiben des BND vom 20. November 2013 und 16. Januar 2014) mit der Bitte um Kenntnisnahme zukommen.

11.02.2014

(See attached file: 140211_LIBE-Ausschuss-Pr_Reaktion auf Schreiben BND.pdf)

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]

MAT A BK-1-4s.pdf, Blatt 298

Kleidt, Christian

Von: Heiß, Günter
Gesendet: Dienstag, 11. Februar 2014 18:42
An: Kleidt, Christian
Cc: Schäper, Hans-Jörg; Karl, Albert
Betreff: AW: Transfer von: PLSA-HH-RECHT-SI/DAND%DAND@vsit.dand.de: Weiterleitung ans BKAmt

Hallo Herr Kleidt,

dann müssten Sie ein Vorlage fertigen

lg gh

2 lg 603 - Bu 10 NA 2

Von: Kleidt, Christian
Gesendet: Dienstag, 11. Februar 2014 16:19
An: al6; Schäper, Hans-Jörg; Maas, Carsten
Cc: ref603
Betreff: WG: Transfer von: PLSA-HH-RECHT-SI/DAND%DAND@vsit.dand.de: Weiterleitung ans BKAmt

Lieber Herr Heiß, lieber Herr Schäper, lieber Herr Dr. Maas,

der BND übermittelte anliegendes Schreiben des Vorsitzenden des LIBE-Ausschusses an Pr BND zK.
BL ChefBK war seinerzeit in den Vorgang involviert; seine Beteiligung rege ich an.

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: transfer@bnd.bund.de [mailto:transfer@bnd.bund.de]
Gesendet: Dienstag, 11. Februar 2014 11:14
An: ref603
Betreff: WG: Transfer von: PLSA-HH-RECHT-SI/DAND%DAND@vsit.dand.de: Weiterleitung ans BKAmt

Mit freundlichen Grüßen

IT-Leitstand

Kleidt, Christian

Von: Becker-Krüger, Maike
Gesendet: Donnerstag, 13. Februar 2014 18:08
An: Kleidt, Christian
Cc: ref121; Uslar-Gleichen, Tania von; Felsheim, Georg
Betreff: AW: Anfrage Brief BND an EP/LIBE-Ausschuss
Anlagen: 140213_BL ChefBK_LIBE-Schreiben Pr BND_nÄ mbk.doc

Lieber Herr Kleidt,

in der Sache, wie ja auch schon vorher besprochen, völlig einverstanden. Würde nur die Antwort an die BT-Verwaltung wie vorgeschlagen formulieren, dass wir nicht anfangen Ping-Pong zu spielen ("Sie sagen, EUZBBG ist nicht einschlägig, warum, was steht genau drin" und schon geht der Briefwechsel los...). Dann haben wir gesagt, dass es persönliche Korrespondenz im Sinne "Danke für Einladung, kann aber nicht" ist und die WELT das aufbauscht und wir dem BT da eine Einordnung geben, warum wir zu dem Schluss kommen.

Zum Schluss frage ich mich nur, wer die Antwort denn der BT-Verwaltung geben soll? Wenn Sie das aus BND-Bezug-Gründen machen wollen, ist das fine, ansonsten sollte das BMWi machen, da die Kollegen ja auch angesprochen wurden, oder

Besten Dank, Grüße & schönen Abend

Wg 603 · Bn 10 NAL

mbk

Von: Kleidt, Christian
Gesendet: Donnerstag, 13. Februar 2014 16:48
An: ref121; Becker-Krüger, Maike
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss
Wichtigkeit: Hoch

Liebe Frau Mildenberger, liebe Frau Becker-Krüger,

in Bezug auf den u.a. Vorgang beabsichtigen wir Herrn BLChBK mit angehängter Vorlage zu unterrichten und das weitere Vorgehen vorzuschlagen. Das PDF-Dokument enthält die Anlagen, auf die Bezug genommen wird. Ich wäre Ihnen dankbar für die Prüfung auf Mitzeichnungsfähigkeit der Vorlage.
Ich wäre sehr dankbar für eine Rückmeldung bis zum 14.02.2014 um 11:00 Uhr und stehe bei Rückfragen jerderzeit zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de

E-Mail: ref603@bk.bund.de

Von: Schiffl, Franz
Gesendet: Dienstag, 11. Februar 2014 17:40
An: ref603
Cc: Schäper, Hans-Jörg
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss
Wichtigkeit: Hoch

IdA Ihrer Zuständigkeit.

Gruß

Schiffl

Von: Becker-Krüger, Maike
Gesendet: Dienstag, 11. Februar 2014 15:33
An: ref602
Cc: ref502; ref503; ref501
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss
Wichtigkeit: Hoch

Liebe Kolleginnen & Kollegen,

in der Hoffnung, dass ich bei Ihnen richtig bin, u.s. Anforderung zK sowie der Frage, wie wir hiermit umgehen sollen?

Beste Grüße

mbk

PS: Das einschlägige BND-Schreiben liegt mir nicht vor.

Maike Becker-Krüger MBA
Bundeskanzleramt
Referat 503
Koordinierung der Europapolitik der Bundesregierung;
Europäischer Rat

Willy-Brandt-Str.1
10557 Berlin
Tel.: 030 / 18 400 - 2591
Mobil: 0175 / 57 76 675
Fax: 030 / 18 10 400 - 2591
Email: Maike.Becker-Krueger@bk.bund.de

Von: Susanne.Hegels@bmwi.bund.de [mailto:Susanne.Hegels@bmwi.bund.de]
Gesendet: Freitag, 7. Februar 2014 11:49

An: Felsheim, Georg
Cc: Klaus-Peter.Leier@bmwi.bund.de; Wolf-Dieter.Plessing@bmwi.bund.de; e01-1@auswaertiges-amt.de
Betreff: AW: Anfrage Brief BND an EP/LIBE-Ausschuss

Sehr geehrter Herr Felsheim,

mit AA sind wir uns einig, dass es für eine abschließende Prüfung der Frage, ob der Bundestag die Übersendung des BND-Briefes verlangen kann, günstig wäre, den genauen Inhalt zu kennen. Liegt Ihnen der Brief vor und könnten Sie uns insoweit informieren, bitte? Wichtig wäre vor allem zu wissen, ob es tatsächlich ausschließlich um vermeintliche Verstöße gegen die EMRK geht, oder ob auch Fragen im Zusammenhang mit EU-Recht angesprochen werden.

Vielen Dank im Voraus.

Mit freundlichen Grüßen
S. Hegels

Von: Hegels, Susanne, Dr., EA1
Gesendet: Mittwoch, 5. Februar 2014 10:30
An: Felsheim, Georg
Cc: Leier, Klaus-Peter, EA1
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss

Sehr geehrter Herr Felsheim,

zur untenstehenden Anfrage von Herrn Dr. Schmidt prüfen wir gerade gemeinsam mit AA, ob insoweit das EUZBBG überhaupt einschlägig ist und der BT auf dieser Grundlage die Übersendung verlangen könnte. Über das Ergebnis werde ich Sie schnellstmöglich informieren.

Mit freundlichen Grüßen

S. Hegels

Dr. Susanne Hegels
Bundesministerium für Wirtschaft und Energie
Referat EA1 - Grundsatzfragen, Koordinierung, Weisungsgebung, EP
Scharnhorststraße 34-37
10115 Berlin
Tel. 03018 615 - 7584

Von: PE 5 EU-Dokumentation - Koordination [mailto:europabuero-koordination@bundestag.de]
Gesendet: Dienstag, 4. Februar 2014 19:05
An: Krusen, Denis, EA1
Cc: Leier, Klaus-Peter, EA1; Hegels, Susanne, Dr., EA1; Felsheim, Georg
Betreff: Anfrage Brief BND an EP/LIBE-Ausschuss

Sehr geehrter Herr Krusen,

laut WELT vom 09.01.2014 hat sich der BND am 20.11.2013 in einem Brief an den Vorsitzenden des Ausschusses für bürgerliche Freiheiten (LIBE) im Europaparlament gewandt und sich hierin gegen Vorwürfe hinsichtlich von Verstößen gegen die EMRK verwahrt. Der Brief liegt erklärtermaßen der Presse vor, nicht jedoch dem Bundestag. Wir bitten daher um Übermittlung.

MAT A BK-1-4s.pdf, Blatt 302

Vielen Dank im Voraus für Ihre Bemühungen und mit freundlichen Grüßen
i.A. F. Schmidt

--
Dr. Friedemann Schmidt
Deutscher Bundestag
Referat PE 5 Europa-Dokumentation
Platz der Republik 1
11011 Berlin

fon +49-(0)30-227.34352
fax +49-(0)30-227.36951
friedemann.schmidt@bundestag.de
europabuero-koordination@bundestag.de

Referat 603

Berlin, 13. Februar 2014

603 – 151 00 – Bu 10/14 NA 2 VS-NfD

RD Kleidt

Hausruf: 2662

Über

Herrn Referatsleiter 603

Herrn Ständigen Vertreter AL 6

Herrn Abteilungsleiter 6

Herrn Staatssekretär

Herrn Büroleiter ChBK

Betr.: Bericht des LIBE-Committee des EP zum NSA-Überwachungsprogramm
hier: Schreiben des Vorsitzenden an BND Pr Schindler vom 06. Februar 2014 sowie Bitte um Beteiligung am Vorgang durch BT-Verwaltung

Anlage: Schreiben an Pr BND

I. Votum

Kenntnisnahme und Billigung des Vorgehens unter 2.

II. Sachverhalt

1. Der BND übermittelte in dem Ihnen bekannten Vorgang ein Schreiben des Vorsitzenden des LIBE-Committee Lopéz Aguilar an Pr BND (Anlage). Der Vorsitzende bedauert darin die irrtümliche Nennung Pr BND auf der Liste der Personen, die auf die Einladung des Committee nicht reagierten und sagt entsprechende Berichtigung in der Endfassung des Berichts zu. Das Schreiben von Pr BND habe ihn aufgrund erheblicher Verzögerungen im Postlauf über die Ständige Vertretung zu spät erreicht.

...

2. Im gleichen Vorgang wandte sich aktuell ein Mitarbeiter der BT-Verwaltung, Referat PE 5, über BMWi an BKAmt, Referat 503, und bat unter Verweis auf diesbezügliche Presseberichterstattung (Die Welt vom 10. Januar 2014) um Zurverfügungstellung des Briefes von Pr BND an das LIBE-Committee. Der BT-Verwaltung zufolge habe sich Pr BND in dem Brief gegen Vorwürfe hinsichtlich von Verstößen gegen die EMRK verwahrt.

Hiesigen Erachtens fällt der besagte Briefwechsel, der lediglich die Anzeige der Nichtteilnahme von Pr BND an der LIBE-Anhörung zum Gegenstand hat, nicht unter die Bestimmungen des Gesetzes über die Zusammenarbeit von Bundesregierung und Deutschem Bundestag in Angelegenheiten der Europäischen Union (EUZBBG), somit erscheint vor diesem Hintergrund eine Übermittlung des Briefes an den BT entbehrlich. Es ist beabsichtigt, der BT-Verwaltung dieses auf folgender Linie mitzuteilen:

„(Anrede) Der Präsident des BND dankt in dem zitierten Schreiben dem LIBE-Ausschuss-Vorsitzenden für die Einladung als Sachverständiger zu der Anhörung, unterstreicht die Beachtung der EMRK durch die deutschen Dienste und teilt dem Vorsitzenden mit, seiner Einladung nicht folgen zu können. Das genannte Schreiben ist also persönliche Korrespondenz im Sinne der Danksagung für die Einladung und einer entsprechenden Absage und keine Stellungnahme, wie der von Ihnen genannte Welt-Artikel insinuiert. Nach hiesiger Auffassung besteht somit keinerlei Bezug zum EUZBBG und daher auch kein Grund für eine Übersendung des persönlichen Absageschreibens. (Schlussformel)"

Referate 121 und 503 haben mitgezeichnet.

(Christian Kleidt)

Kommentar [M1]: Wer soll das tun? BMWi (Vorschlag aus hiesiger Sicht)? Wir (1, 5, 6?)

Gelöscht: wie folgt

Gelöscht: ist

Gelöscht: das

Gelöscht: im vorliegenden Fall nicht einschlägig. Daher erscheint eine Übermittlung des Briefes an den Deutschen Bundestag entbehrlich. Der Präsident des BND dankt in dem zitierten Schreiben dem LIBE-Vorsitzenden für die Einladung, unterstreicht die Beachtung der EMRK durch die deutschen Dienste und teilt dem Vorsitzenden mit, seiner Einladung nicht folgen zu können.

DIE WELT

13. Feb. 2014, 7:01
Diesen Artikel finden Sie online unter
http://www.welt.de/123726518

Die Welt | 10.01.14

Europaparlament rechnet mit NSA und BND ab

Von Manuel Bewarder

Lfg. 608-BK 10 NR2

Die Untersuchungsgruppe des Europaparlaments zur NSA-Affäre kritisiert den US-Nachrichtendienst in ungewohnt deutlichen Worten. Im 52-seitigen Entwurf des Abschlussberichts, der im Justizausschuss vorgelegt werden sollte, heißt es, die Enthüllungen durch Journalisten und Whistleblower sowie die Nachforschungen der Arbeitsgruppe zeigten **"eindrucksvolle Beweise für die Existenz umfassender, komplexer und technisch hoch entwickelter Systeme in den Händen der USA** (Link: http://www.welt.de/themen/usa-reisen/) **und der Nachrichtendienste einiger EU-Mitgliedsstaaten"** . Die Spähmaßnahmen in beispiellosem Ausmaß würden sich gegen Menschen überall auf der Welt richten. Berichterstatter ist der britische Labour-Abgeordnete Claude Moraes.

Schwere Vorwürfe erhebt der Berichterstatter auch gegen den Bundesnachrichtendienst (BND). Er hebt zwar die NSA und den britischen Nachrichtendienst GCHQ hervor. Allerdings nehme man an, dass auch der BND ähnliche Programme besitze, wenn auch mit deutlich weniger Umfang. Der Berichterstatter empfiehlt, die Ausspähaktivitäten mit Blick auf die EU-Menschenrechtskonvention zu überprüfen.

Der BND wehrt sich gegen die Darstellung von Moraes. In einem der "Welt" vorliegenden Brief vom 20. November 2013 an den Vorsitzenden des Ausschusses für bürgerliche Freiheiten, Juan Fernando López Aguilar, schreibt Präsident Gerhard Schindler, man achte die Menschenrechtskonvention und begrüße auch die "Arbeit und Zielsetzung" des Komitees. Zum Vorwurf, Schindler hätte auf eine Einladung zur Befragung nicht reagiert, sagte ein BND-Sprecher der "Welt", fühle man sich zunächst verpflichtet, auf nationaler Ebene bei der Aufklärung der Vorwürfe voranzukommen.

In der Bundesregierung wird trotz der Einladung von US-Präsident Barack Obama an Kanzlerin Angela Merkel nach Washington **nicht mit der raschen Unterzeichnung eines Geheimdienstabkommens gerechnet.** Noch gebe es kein abschlussreifes Verhandlungsergebnis als Konsequenz aus der NSA-Affäre und der Abhöraktion gegen das Handy Merkels, erfuhr die Deutsche Presse-Agentur aus Sicherheitskreisen. Dem Vernehmen nach will sich das Weiße Haus nicht auf eine Formulierung festlegen lassen, nach der die US-Dienste künftig alles unterlassen sollen, was deutsche Interessen verletzt.

Obama treibt indes eine **Beschränkung der Geheimdienste** voran. Am Mittwoch traf er sich mit den Geheimdienstchefs zum Stand der internen Überprüfung. Obama will voraussichtlich kommende Woche in einer Grundsatzrede seine Reformpläne erläutern.

© Axel Springer SE 2014. Alle Rechte vorbehalten

Kleidt, Christian

Von: Mildenberger, Tanja
Gesendet: Donnerstag, 13. Februar 2014 19:02
An: Kleidt, Christian
Cc: ref121; Becker-Krüger, Maike
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss
Anlagen: 140213_BL ChefBK_LIBE-Schreiben Pr BND_nÄ mbk.doc

Lieber Herr Kleidt,

ich schließe mich 503 an, rege aber, auch wenn die Anfrage uns über BMWi erreicht hat, eher eine Übermittlung des Schreibens durch Abt. 6 oder auch 503 (wegen Bündelung des Kontakts zu BT-Ref?) an; BMWi sollte nicht zu Dokumenten des BKAmtes bzw seines nachgeordneten Bereichs Auskunft geben. *

Schöne Grüße
Tanja Mildenberger

Von: Becker-Krüger, Maike
Gesendet: Donnerstag, 13. Februar 2014 18:08
An: Kleidt, Christian
Cc: ref121; Uslar-Gleichen, Tania von; Felsheim, Georg
Betreff: AW: Anfrage Brief BND an EP/LIBE-Ausschuss

Lieber Herr Kleidt,

in der Sache, wie ja auch schon vorher besprochen, völlig einverstanden. Würde nur die Antwort an die BT-Verwaltung wie vorgeschlagen formulieren, dass wir nicht anfangen Ping-Pong zu spielen ("Sie sagen, EUZBBG ist nicht einschlägig, warum, was steht genau drin" und schon geht der Briefwechsel los...). Dann haben wir gesagt, dass es persönliche Korrespondenz im Sinne "Danke für Einladung, kann aber nicht" ist und die WELT das aufbauscht und wir dem BT da eine Einordnung geben, warum wir zu dem Schluss kommen.

Zum Schluss frage ich mich nur, wer die Antwort denn der BT-Verwaltung geben soll? Wenn Sie das aus BND-Bezug-Gründen machen wollen, ist das fine, ansonsten sollte das BMWi machen, da die Kollegen ja auch angesprochen wurden, oder

Besten Dank, Grüße & schönen Abend

mbk

Von: Kleidt, Christian
Gesendet: Donnerstag, 13. Februar 2014 16:48
An: ref121; Becker-Krüger, Maike
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss
Wichtigkeit: Hoch

Liebe Frau Mildenberger, liebe Frau Becker-Krüger,

in Bezug auf den u.a. Vorgang beabsichtigen wir Herrn BLChBK mit angehängter Vorlage zu unterrichten und das weitere Vorgehen vorzuschlagen. Das PDF-Dokument enthält die Anlagen, auf die Bezug genommen wird. Ich wäre Ihnen dankbar für die Prüfung auf Mitzeichnungsfähigkeit der Vorlage.

Referat 603 Berlin, 14. Februar 2014

603 – 151 00 – Bu 10/14 NA 2 VS-NfD

RD Kleidt Hausruf: 2662

1. Vfg. T:\Abteilungen\Abt6\Ref603\Verzeichnisse neu\BV\Prism Tempora\140213_BL ChefBK_LIBE-Schreiben Pr BND.doc

Über

Herrn Referatsleiter 603

Herrn Ständigen Vertreter AL 6

Herrn Abteilungsleiter 6

Herrn Staatssekretär

Herrn Büroleiter ChBK

Betr.: Bericht des LIBE-Committee des EP zum NSA-Überwachungsprogramm
hier: Schreiben des Vorsitzenden an BND Pr Schindler vom 06. Februar 2014 sowie Bitte um Beteiligung am Vorgang durch BT-Verwaltung

Anlage: 1. Schreiben an Pr BND
2. Artikel Die Welt vom 10. Januar 2014

I. Votum

Kenntnisnahme und Billigung des Vorgehens unter 2.

II. Sachverhalt

1. Der BND übermittelte in dem Ihnen bekannten Vorgang ein Schreiben des Vorsitzenden des LIBE-Committee Lopéz Aguilar an Pr BND (Anlage). Der Vorsitzende bedauert darin die irrtümliche Nennung Pr BND auf der Liste der Personen, die auf die Einladung des Committee nicht reagierten und sagt

...

entsprechende Berichtigung in der Endfassung des Berichts zu. Das Schreiben von Pr BND habe ihn aufgrund erheblicher Verzögerungen im Postlauf über die Ständige Vertretung zu spät erreicht.

2. Im gleichen Vorgang wandte sich aktuell ein Mitarbeiter der BT-Verwaltung, Referat PE 5, über BMWi an BKAmt, Referat 503, und bat unter Verweis auf diesbezügliche Presseberichterstattung (Die Welt vom 10. Januar 2014) um Zurverfügungstellung des Briefes von Pr BND an das LIBE-Committee. Der BT-Verwaltung zufolge habe sich Pr BND in dem Brief gegen Vorwürfe hinsichtlich von Verstößen gegen die EMRK verwahrt.

Hiesigen Erachtens fällt der besagte Briefwechsel, der lediglich die Anzeige der Nichtteilnahme von Pr BND an der LIBE-Anhörung zum Gegenstand hat, nicht unter die Bestimmungen des Gesetzes über die Zusammenarbeit von Bundesregierung und Deutschem Bundestag in Angelegenheiten der Europäischen Union (EUZBBG), somit erscheint eine Übermittlung des Briefes an den BT entbehrlich. Es ist beabsichtigt, dass Referat 603 der BT-Verwaltung unter nebenabdrücklicher Beteiligung BMWi dieses wie folgt mitteilt:

„(Anrede) Der Präsident des BND dankt in dem zitierten Schreiben dem LIBE-Ausschuss-Vorsitzenden für die Einladung als Sachverständiger zu der Anhörung, unterstreicht die Beachtung der EMRK durch die deutschen Dienste und teilt dem Vorsitzenden mit, seiner Einladung nicht folgen zu können. Das genannte Schreiben ist also Korrespondenz im Sinne der Danksagung für die Einladung und einer entsprechenden Absage und keine Stellungnahme, wie der von Ihnen genannte Welt-Artikel insinuiert. Nach hiesiger Auffassung besteht somit keinerlei Bezug zum EUZBBG und daher auch kein Grund für eine Übersendung des persönlichen Absageschreibens. (Schlussformel)“

Referate 121 und 503 haben mitgezeichnet.

14/2

(Christian Kleidt)

...

1. Referate 121 und 503 m.d.B.u. Mitzeichnung / auf elektronischem Wege am 13.02.14 mit Anmerkungen/Ergänzungen erfolgt
2. ab
3. WV 603/Umlauf 603

Referat 603

Berlin, 14. Februar 2014

603 – 151 00 – Bu 10/14 NA 2 VS-NfD

RD Kleidt

Hausruf: 2662

Über

Herrn Referatsleiter 603

Herrn Ständigen Vertreter AL 6

Herrn Abteilungsleiter 6

Herrn Staatssekretär

Herrn Büroleiter ChBK

Betr.: Bericht des LIBE-Committee des EP zum NSA-Überwachungsprogramm
hier: Schreiben des Vorsitzenden an BND Pr Schindler vom 06. Februar 2014 sowie Bitte um Beteiligung am Vorgang durch BT-Verwaltung

Anlage: 1. Schreiben an Pr BND
2. Artikel Die Welt vom 10. Januar 2014

I. Votum

Kenntnisnahme und Billigung des Vorgehens unter 2.

II. Sachverhalt

1. Der BND übermittelte in dem Ihnen bekannten Vorgang ein Schreiben des Vorsitzenden des LIBE-Committee Lopéz Aguilar an Pr BND (Anlage). Der Vorsitzende bedauert darin die irrtümliche Nennung Pr BND auf der Liste der Personen, die auf die Einladung des Committee nicht reagierten und sagt entsprechende Berichtigung in der Endfassung des Berichts zu. Das Schreiben

...

von Pr BND habe ihn aufgrund erheblicher Verzögerungen im Postlauf über die Ständige Vertretung zu spät erreicht.

2. Im gleichen Vorgang wandte sich aktuell ein Mitarbeiter der BT-Verwaltung, Referat PE 5, über BMWi an BKAmt, Referat 503, und bat unter Verweis auf diesbezügliche Presseberichterstattung (Die Welt vom 10. Januar 2014) um Zurverfügungstellung des Briefes von Pr BND an das LIBE-Committee. Der BT-Verwaltung zufolge habe sich Pr BND in dem Brief gegen Vorwürfe hinsichtlich von Verstößen gegen die EMRK verwahrt.

Hiesigen Erachtens fällt der besagte Briefwechsel, der lediglich die Anzeige der Nichtteilnahme von Pr BND an der LIBE-Anhörung zum Gegenstand hat, nicht unter die Bestimmungen des Gesetzes über die Zusammenarbeit von Bundesregierung und Deutschem Bundestag in Angelegenheiten der Europäischen Union (EUZBBG), somit erscheint eine Übermittlung des Briefes an den BT entbehrlich. Es ist beabsichtigt, dass Referat 603 der BT-Verwaltung unter nebenabdrücklicher Beteiligung BMWi dieses wie folgt mitteilt:

„(Anrede) Der Präsident des BND dankt in dem zitierten Schreiben dem LIBE-Ausschuss-Vorsitzenden für die Einladung als Sachverständiger zu der Anhörung, unterstreicht die Beachtung der EMRK durch die deutschen Dienste und teilt dem Vorsitzenden mit, seiner Einladung nicht folgen zu können. Das genannte Schreiben ist also Korrespondenz im Sinne der Danksagung für die Einladung und einer entsprechenden Absage und keine Stellungnahme, wie der von Ihnen genannte Welt-Artikel insinuiert. Nach hiesiger Auffassung besteht somit keinerlei Bezug zum EUZBBG und daher auch kein Grund für eine Übersendung des persönlichen Absageschreibens. (Schlussformel)“

Referate 121 und 503 haben mitgezeichnet.

(Christian Kleidt)

MAT A BK-1-4s.pdf, Blatt 312

Kleidt, Christian

Von: Kleidt, Christian
Gesendet: Freitag, 21. Februar 2014 11:48
An: al6; Schäper, Hans-Jörg; Maas, Carsten
Cc: ref603
Betreff: WG: Anfrage Brief BND an EP/LIBE-Ausschuss
Anlagen: 131120_Brief Pr BND.pdf

zgK

Mit freundlichen Grüßen
Im Auftrag

2 Vg 603-8410 NAL

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: Kleidt, Christian
Gesendet: Freitag, 21. Februar 2014 11:47
An: 'europabuero-koordination@bundestag.de'
Cc: 'Denis.Krusen@bmwi.bund.de'; Felsheim, Georg; ref603
Betreff: AW: Anfrage Brief BND an EP/LIBE-Ausschuss

Sehr geehrter Herr Dr. Schmidt,

bezugnehmend auf Ihre u.a. Anfrage und unser Telefonat am 19.02., darf ich Ihnen in Anlage und ohne Anerkennung einer Rechtspflicht das in der Presse zitierte Schreiben zuleiten.

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Von: PE 5 EU-Dokumentation - Koordination [mailto:europabuero-koordination@bundestag.de]

21.02.2014

Gesendet: Dienstag, 4. Februar 2014 19:05
An: Krusen, Denis, EA1
Cc: Leier, Klaus-Peter, EA1; Hegels, Susanne, Dr., EA1; Felsheim, Georg
Betreff: Anfrage Brief BND an EP/LIBE-Ausschuss

Sehr geehrter Herr Krusen,

laut WELT vom 09.01.2014 hat sich der BND am 20.11.2013 in einem Brief an den Vorsitzenden des Ausschusses für bürgerliche Freiheiten (LIBE) im Europaparlament gewandt und sich hierin gegen Vorwürfe hinsichtlich von Verstößen gegen die EMRK verwahrt. Der Brief liegt erklärtermaßen der Presse vor, nicht jedoch dem Bundestag. Wir bitten daher um Übermittlung.

Vielen Dank im Voraus für Ihre Bemühungen und mit freundlichen Grüßen
i.A. F. Schmidt

--
Dr. Friedemann Schmidt
Deutscher Bundestag
Referat PE 5 Europa-Dokumentation
Platz der Republik 1
11011 Berlin

fon +49-(0)30-227.34352
fax +49-(0)30-227.36951
friedemann.schmidt@bundestag.de
europabuero-koordination@bundestag.de

Gerhard Schindler
Präsident

20. November 2013

Herrn
Juan Fernando López Aguilar
Vorsitzender
Committee on Civil Liberties, Justice
and Home Affairs
Europäisches Parlament
Brüssel

Belgien

Sehr geehrter Herr López Aguilar,

zunächst bedanke ich mich für Ihr Schreiben vom 14. Oktober 2013, in dem sie mich zu einer Anhörung des von Ihnen geleiteten Komitees einladen.

Die Arbeit und Zielsetzung Ihres Komitees begrüße ich ausdrücklich; hierbei beziehe ich mich insbesondere auf die Wahrung der Rechte der EU – Bürgerinnen und – Bürger, die im Einklang mit der Europäischen Menschenrechtskonvention stehen. Diese wird in der Bundesrepublik Deutschland in höchstem Maße gewürdigt und selbstverständlich auch von den deutschen Nachrichtendiensten geachtet.

Die drei deutschen Nachrichtendienste sind dem deutschen Gesetz gegenüber verpflichtet und richten ihre Arbeit daran aus, dies gilt auch für den Umgang mit Informationen, die nicht selbst erhoben wurden. Das deutsche Parlament hat hierauf stets sein Augenmerk gerichtet und wird dies auch in Zukunft tun. Um dies zu gewährleisten, wurden geeignete Mechanismen entwickelt, wie Gremien zur Aufsicht, Kontrolle und Überwachung.

Auch wenn ich bedauerlicherweise Ihre Einladung nicht annehmen kann, wünsche ich Ihnen alles Gute und eine glückliche Hand für ihre Arbeit.

Mit freundlichen Grüßen

(Gerhard Schindler)

Kleidt, Christian

Von: Kleidt, Christian
Gesendet: Donnerstag, 27. Februar 2014 10:59
An: 'PGNSA@bmi.bund.de'
Cc: 'OESI3AG@bmi.bund.de'; ref603; Maas, Carsten
Betreff: WG: Berichtsentwurf LIBE-Kommittee zum Überwachungsprogramm der US-amerikanischen NSA
Anlagen: NSA Bericht_Konsolidierter Text.doc

Sehr geehrter Herr Weinbrenner,

Sie hatten uns seinerzeit dankenswerter Weise an Ihren Ergebnissen der Prüfung einer Vorabfassung des Berichts des LIBE-Kommittees beteiligt. Nunmehr liegt ein konsolidierter Bericht vor, den ich Ihnen anbei zuleite mit der Bitte, diesen kurzfristig auf ggf. weiterhin bestehenden Änderungsbedarf zu prüfen. Aufgrund der kurzen hierzu bestehenden Frist bin ich Ihnen dankbar für eine Rückmeldung bis Montag, den 03. März 2014 um 15:00 Uhr. Vielen Dank!

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Telefonat mit Hrn. Weinbrenner am 28.02.2014:

1) ÖSI3AG ist „stark geneigt" auf Arbeitsebene ggü Büro TdEP Voss – wie zuvor über PSt Schröder – Einschätzung zu übermitteln. Bericht lag von dort bereits vor.

2) Ref. 603 wird an Bewertung LIBE-Bericht beteiligt

3) erneutes Telefonat Anfang 10. KW verabredet.

4) z.Vg. 603 - Bu 10 NA 2

Kleidt, Christian

Von: Kleidt, Christian
Gesendet: Donnerstag, 27. Februar 2014 11:05
An: 'leitung-grundsatz@bnd.bund.de'
Cc: ref603; Maas, Carsten
Betreff: EILT! Berichtsentwurf LIBE-Kommittee zum Überwachungsprogramm der US-amerikanischen NSA
Anlagen: NSA Bericht_Konsolidierter Text.doc

Leitungsstab
PLSA
z.Hd. Herrn S[redacted] o.V.i.A.

Az. 603 - 151 00 - Bu 10/14 NA 2 VS-NfD

Sehr geehrter Herr S[redacted]

in Anlage übersende ich Ihnen den konsolidierten Bericht des LIBE-Kommittee, verbunden mit der Bitte, diesen kurzfristig auf ggf. weiterhin bestehenden Änderungs-/Anmerkungsbedarf zu prüfen. Aufgrund der kurzen hierzu bestehenden Frist bin ich Ihnen dankbar für eine Rückmeldung bis **Montag, den 03. März 2014 um 15:00 Uhr.** Ihre Antwort kann aufgrund der knappen Frist gerne per E-Mail erfolgen.

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Kleidt, Christian

Von: transfer@bnd.bund.de
Gesendet: Montag, 3. März 2014 14:58
An: Kleidt, Christian
Betreff: WG: EILT! Berichtsentwurf LIBE-Kommittee zum Überwachungprogramm der US-amerikanischen NSA
Anlagen: NSA Bericht_Konsolidierter Text.doc

Datum: 03.03.2014 14:56
an das
Bundeskanzleramt, Herrn Christian Kleidt
E-Mail: Christian.Kleidt@bk.bund.de

L.Vg · 603 · Bu 10 NA 2

Betreff: Untersuchung des LIBE-Committee zum Überwachungsprogramm der NSA
hier: Prüfung des abschließenden Berichtsentwurfs
Bezug: E-Mail BKAmt, Az. 603 - 151 00 - Bu 10/14 NA 2 VS-NfD

Sehr geehrter Herr Kleidt,

mit Bezug baten Sie um Prüfung des konsolidierten Berichts des vorgenannten Komitees und Mitteilung ggf. bestehenden Änderungsbedarfs. Ich kann Ihnen mitteilen, dass seitens des Bundesnachrichtendienstes kein Änderungsbedarf gesehen wird. Die zwei wesentlichen Aspekte, die im Rahmen der Prüfung des Draft Reports Mitte Januar 2014 hiesigerseits angemerkt wurden, sind im aktuellen Entwurf berücksichtigt worden. Dies betraf zum einen die Nennung von Präsident Schindler unter denjenigen Experten, die auf eine Einladung des Komitees nicht reagiert hätten. Zum anderen betraf es die Darstellung in den Main Findings (dort Ziffer 2), wonach der Bundesnachrichtendienst ein technisches Überwachungsprogramm betreibe , welches eine anlasslose und massenhafte Ausspähung von Bürgerinnen und Bürgern der EU beinhalte. Dieser Aspekt spiegelt sich in dem aktuellen Entwurf in Form einer Aufforderung an Deutschland wider, entsprechende Vorwürfe klarzustellen (Recommendations, Ziffer 23). Der Bundesnachrichtendienst begrüßt diese Änderungen.

Im Übrigen finden sich im aktuellen Berichtsentwurf Anzeichen dafür, dass künftig mit einer stärkeren Einbringung der europäischen Gremien in Fragen der Ausgestaltung der Kontrolle der Nachrichtendienste in der Verantwortung der Mitgliedstaaten zu rechnen sein wird. Diesbezüglich bestehen vor dem Hintergrund der die Kontrolle des Bundesnachrichtendienstes bestimmenden Rechtslage in Deutschland keine Bedenken.

Die in den Main Findings unter Ziffer 122 zu findende Bewertung, der Abschluss eines vom Bundesnachrichtendienst angestrebten Kooperationsabkommens mit der NSA ("No-Spy-Abkommen") sei irrelevant und kontraproduktiv, ist vor dem Hintergrund, dass der Inhalt eines solchen Abkommens und dessen Zielrichtung dem LIBE-Komittee nicht bekannt sein dürfte, nicht nachzuvollziehen. Ein europäischer Ansatz - wie er aus Sicht des LIBE-Komitees offenbar anzustreben ist - dürfte in diesem Zusammenhang aus Sicht des Bundesnachrichtendienstes jedenfalls nicht erfolgversprechend und auch nicht zielführend sein.

Mit freundlichen Grüßen
Im Auftrag

M[redacted] F[redacted]
PLSA, Tel.: 8[redacted]
----- Weitergeleitet von M[redacted] F[redacted]/DAND am 03.03.2014 11:20 -----

Von: TRANSFER/DAND

03.03.2014

An: PLSA-HH-RECHT-SI/DAND@DAND
Datum: 27.02.2014 11:12
Betreff: Antwort: WG: EILT! Berichtsentwurf LIBE-Kommittee zum Überwachungsprogramm der US-amerikanischen NSA
Gesendet von: ITBA-N

Anbei eine weitergeleitete Nachricht aus dem BIZ Netz.

Freundlich grüßt Sie

Ihr ITB-Leitstand in Pullach
Tel. 8[redacted]

Von: leitung-grundsatz@bnd.bund.de
An: transfer@bnd.bund.de
Datum: 27.02.2014 11:09
Betreff: WG: EILT! Berichtsentwurf LIBE-Kommittee zum Überwachungsprogramm der US-amerikanischen NSA

Bitte an PLSA-HH-RECHT-SI weiterleiten
Danke

-----Weitergeleitet von leitung-grundsatz IVBB-BND-BIZ/BIZDOM am 27.02.2014 11:07 -----
An: "'leitung-grundsatz@bnd.bund.de'" <leitung-grundsatz@bnd.bund.de>
Von: "Kleidt, Christian" <Christian.Kleidt@bk.bund.de>
Datum: 27.02.2014 11:05
Kopie: ref603 <ref603@bk.bund.de>, "Maas, Carsten" <Carsten.Maas@bk.bund.de>
Betreff: EILT! Berichtsentwurf LIBE-Kommittee zum Überwachungsprogramm der US-amerikanischen NSA
(Siehe angehängte Datei: NSA Bericht_Konsolidierter Text.doc)

Leitungsstab
PLSA
z.Hd. Herrn S[redacted] o.V.i.A.

Az. 603 - 151 00 - Bu 10/14 NA 2 VS-NfD

Sehr geehrter Herr S[redacted],

in Anlage übersende ich Ihnen den konsolidierten Bericht des LIBE-Kommittee, verbunden mit der Bitte, diesen kurzfristig auf ggf. weiterhin bestehenden Änderungs-/Anmerkungsbedarf zu prüfen. Aufgrund der kurzen hierzu bestehenden Frist bin ich Ihnen dankbar für eine Rückmeldung bis Montag, den 03. März 2014 um 15:00 Uhr. Ihre Antwort kann aufgrund der knappen Frist gerne per E-Mail erfolgen.

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt

MAT A BK-1-4s.pdf, Blatt 319

000306

Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

(See attached file: NSA Bericht_Konsolidierter Text.doc)

MAT A BK-1-4s.pdf, Blatt 320

000307

Kleidt, Christian

z.Vg. 603 - Bu 10 Na 2

Von: Johann.Jergl@bmi.bund.de
Gesendet: Montag, 3. März 2014 15:34
An: Kleidt, Christian
Cc: Ulrich.Weinbrenner@bmi.bund.de
Betreff: Stellungnahme zum Entwurf eines konsolidierten Berichts des LIBE-Komitees zu Überwachungsprogrammen u.a. der US-amerikanischen NSA
Anlagen: vergleich.docx; 14-02-28_Stellungnahme.docx

Lieber Herr Kleidt,

beigefügt Ihnen vorab z.K. der Entwurf einer Stellungnahme zum konsolidierten Berichtsentwurf des LIBE-Komitees zu Überwachungsprogrammen u.a. der US-amerikanischen NSA (vorbehaltlich der noch ausstehenden Leitungsbilligung).

Mit freundlichen Grüßen,
Im Auftrag

Johann Jergl

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3

Alt-Moabit 101 D, 10559 Berlin
Telefon: 030 18681 1767
Fax: 030 18681 51767
E-Mail: johann.jergl@bmi.bund.de
Internet: www.bmi.bund.de

Stellungnahme BMI zum Entwurf eines konsolidierten Berichts des LIBE-Komitees zu Überwachungsprogrammen u.a. der US-amerikanischen NSA

I. „Digitaler Habeas-Corpus“

1. *Abschluss des Datenschutzpakets in 2014*
   Erscheint nicht aussichtsreich. ad Es sind noch eine Vielzahl bedeutender Fragen zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.

2. *Abschluss des EU-US-Datenschutzabkommens*
   Keine Bedenken. Zuständig ist KOM.

3. *Aussetzung von Safe-Harbour*
   Die Bundesregierung setzt sich für die Verbesserung von Safe Harbour ein. Neben der zeitnahen Umsetzung der Empfehlungen der KOM aus ihrer Safe Harbour Analyse von November 2013 im Wege der Nachverhandlung sollte in der Datenschutz-Grundverordnung ein rechtlicher Rahmen für Modelle wie Safe Harbour geschaffen werden.

4. *Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens*
   Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus unserer Sicht derzeit kein Anlass, das Abkommen auszusetzen.

5. *(neu) Evaluierung sämtlicher Abkommen oder sonstigen Austauschs mit Drittstaaten, auf deren Grundlage es zu einer Verarbeitung personenbezogener Daten kommt*
   Gegenstand der Evaluierung soll die mögliche Verletzung des Schutzes dieser Daten durch Überwachungsmaßnahmen in den Drittstaaten sein. Ein solches Vorhaben würde es aus unserer Sicht erfordern, die

Einzelheiten der Überwachungsmaßnahmen von Drittstaaten zu kennen oder diese zumindest belastbar einschätzen zu können. Nach unseren Erfahrungen ist regelmäßig nicht mit einer Bereitschaft zur Offenlegung von Maßnahmen in der hierfür notwendigen Detaillierung zu rechnen. Daher schätzen wir dieses Vorhaben nicht als aussichtsreich und gleichwohl sehr aufwändig ein.

6. *Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)*
   Keine Bedenken.

7. *Entwicklung einer Strategie für eine Europäische (stärker unabhängige) IT-Industrie („digital new deal')*
   Zustimmung; der Koalitionsvertrag beinhaltet eine vergleichbare Maßnahme:
   „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer
   Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings."

8. *EU-Politik als Referenz für demokratische und neutrale Internet-Governance*
   Keine Bedenken.

II. Weitere Punkte

In seiner Bewertung des Berichtsentwurfs vom Januar 2014 hat BMI überdies auf **aus deutscher Sicht besonders kritische Punkte** hingewiesen und deren Streichung angeregt.

Eine diesbezügliche Verbesserung kann in „Main findings“ Nr. 2 des konsolidierten Berichts festgestellt werden, wo nun nicht mehr unterstellt wird, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM.

Weiterhin enthalten ist jedoch als „Recommendation“ Nr. 22 (vorher 20) eine **Aufforderung auch an Deutschland** (als angeblicher Teil eines sog. „14-eyes“-Programms), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**. Die hier einschlägigen deutschen Vorschriften entsprechen den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP. Deswegen wird weiterhin die Streichung dieser Empfehlung für notwendig erachtet.

In Recommendation 99 ist durch neue Einfügungen u.a. die explizite Aufforderung an die KOM aufgenommen worden, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der MS im Bereich der IT-Sicherheit. Insbesondere im **operativen Bereich liegt die Zuständigkeit aber bei den Mitgliedstaaten** und auch entsprechende Aktivitäten müssen bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (…)“ und letzer Hs. ab „and to establish within ENISA’s structure a Computer Emergency response Team (CERT) for the EU and its Member States”) sollte daher eine Streichung angestrebt werden.

Kleidt, Christian

Von: Kleidt, Christian

Gesendet: Montag, 3. März 2014 15:54

An: ref601; ref132; ref413

Cc: ref603

Betreff: EILT SEHR! Bitt eum Mitprüfung Vorlage BLChefBK konsolidierter Berichtsentwurf des LIBE-Komitees

Anlagen: vergleich.docx; 14-02-28_Stellungnahme.docx; 140303_Vorlage_BLChBK_LIBE.doc

413; Dr. Schieferdecker verzichtet auf MZ, Streichung aus der Leiste

Liebe Kolleginnen und Kollegen!

Nunmehr liegt ein konsolidierter Bericht des LIBE-Ausschusses vor. Abt. 6 wurde gebeten, diesen - wie zuvor auch den Entwurf - zu prüfen. Sie hatten die entsprechende Vorlage von 603 mit Datum vom 21.01.14 mitgezeichnet. Aufgrund der knappen Fristen (Einbringung von Änderungsvorschlägen nach hiesiger Kenntnis bis 05.03.14) bitte ich um **Prüfung auf Mitzeichnungsfähigkeit bis heute um 17:00 Uhr**. Ich bitte diesbezüglich um Nachsicht.

Im Anhang finden Sie den Berichtsentwurf mit kenntlich gemachten Änderungen im Vergleich zur letzten Fassung, sowie die - soeben erhaltene, allerdings noch nicht von der BMI-Hausleitung gebilligte - Fassung der dortigen Stellungnahme.

z.Vg. 603 · Bu 10 NAL

Mit freundlichen Grüßen
Im Auftrag

Christian Kleidt
Bundeskanzleramt
Referat 603

Hausanschrift: Willy-Brandt-Str. 1, 10557 Berlin
Postanschrift: 11012 Berlin
Tel.: 030-18400-2662
E-Mail: christian.kleidt@bk.bund.de
E-Mail: ref603@bk.bund.de

Referat 603

Berlin, 03. März 2014

603 – 151 00 – Bu 10/14 NA 2 VS-NfD

RD Kleidt

Hausruf: 2662

1. Vfg.

Über
Herrn Referatsleiter 603
Herrn Ständigen Vertreter AL 6
Herrn Abteilungsleiter 6
Herrn Staatssekretär

Herrn Büroleiter ChBK

Betr.: Konsolidierter Bericht des EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) zum NSA-Überwachungsprogramm
hier: Stellungnahme

Anlage: 1.) LIBE-Bericht (Stand: 21. Februar 2014)
2.) Mailzuschrift BMI, ÖS I 3 vom 03. März 2013 mit Anmerkungsbedarf
3.) Vorlage zum LIBE-Berichtsentwurf vom 21. Januar 2014

I. Votum

Kenntnisnahme und telefonische Kontaktaufnahme zum Büro Axel Voss, MdEP

II. Sachverhalt

Mit Mailzuschrift vom 25. Februar 2014 baten Sie um Prüfung des nunmehr inoffiziell vorliegenden konsolidierten Berichts des LIBE-Ausschusses (Anlage 1). Laut Mailzuschrift Büro Voss, MdEP vom 24. Februar 2014 sei zur Einbringung von Änderungsanträgen höchstwahrscheinlich bis zum 05. März 2014

...

Gelegenheit. Der Gesamtbericht wurde in Duktus und Inhalt bei Wertungen und Empfehlungen an die Kommission und die Mitgliedstaaten verschärft.

Der BND wurde von hier um Prüfung und Stellungnahme gebeten. Die dortigen, Ihnen seinerzeit mit Bezug 1 dargelegten zwei wesentlichen Änderungswünsche wurden in der aktuellen Berichtsfassung berücksichtigt. So wird auf S. 20 unter „Main findings", Ziffer 2, DEU und der BND nicht mehr genannt als ein Land, welches ein dem der NSA vergleichbares „Überwachungsprogramm" betreibe. Auf Seite 24 wird dieser Aspekt allerdings unter „Recommendations", Ziffer 23 als Aufforderung u.a. an DEU aufgegriffen, entsprechende Vorwürfe zu klären. Im Annex auf S. 60 wird Pr BND nunmehr korrekterweise in der Rubrik „Experten, die die Einladung des LIBE-Vorsitzenden abgelehnt haben" geführt.

BMI, ÖS I 3 teilte mit, Herr Voss MdEP habe sich mit der Bitte um Prüfung des konsolidierten Berichts sowohl an PSt Dr. Ole Schröder als auch an Dr. Hans-Peter Uhl, MdB gewandt. BMI werde, wie bereits bei der Entwurfsfassung des Berichts, per E-Mail Änderungswünsche an Herrn Voss, MdEP übermitteln. Diese liegen hier bislang nur in einer noch nicht von der BMI-Hausleitung freigegebenen Form vor (s. Anlage 2):

Darin unterstreicht auch das BMI, dass im Bericht nun nicht mehr unterstellt werde, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM. Zur o.a. Aufforderung an DEU, Vorwürfe bzgl. eine Überwachungsprogramms zu klären, verweist BMI darauf, dass die hier einschlägigen deutschen Vorschriften den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts entsprechen und grundrechtskonform sind. Unabhängig davon liege die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP. Deswegen werde weiterhin die Streichung dieser Empfehlung für notwendig erachten.

Zudem verweist BMI darauf, dass in Recommendation 99 u.a. die explizite Aufforderung an die KOM neu aufgenommen worden sei, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit

...

und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der MS im Bereich der IT-Sicherheit. Insbesondere im operativen Bereich liege die Zuständigkeit jedoch bei den Mitgliedstaaten und auch entsprechende Aktivitäten müssten bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (…)" und den letzen Halbsatz ab „and to establish within ENISA's structure a Computer Emergency response Team (CERT) for the EU and its Member States") sollte daher lt. BMI eine Streichung angestrebt werden.

III. Bewertung

Es wird vorgeschlagen, dass Sie in einer telefonischen Erörterung mit Herrn Voss, MdEP, die neuerlichen Änderungsvorschläge des BMI ausdrücklich unterstützen. Zudem könnten Sie MdEP Voss für die eingebrachten und tatsächlich erfolgten Änderungen aus Sicht BKAmt, Abt. 6, sowie generell für den vertrauensvollen Austausch in dieser Angelegenheit danken.

Referate 601 und 132 haben mitgezeichnet.

3/3

(Christian Kleidt)

2. 601 m.d.B. um Mitzeichnung / elektron.
3. 132 m.d.B. um Mitzeichnung
4. ab ✓
5. WV 603 ✓ 1. Vg.

Referat 603 Berlin, 03. März 2014

603 – 151 00 – Bu 10/14 NA 2 VS-NfD

RD Kleidt Hausruf: 2662

Über

Herrn Referatsleiter 603 i.V. Kle 03/03

Herrn Ständigen Vertreter AL 6 i.V. 3.3.

Herrn Abteilungsleiter 6 4/3

Herrn Staatssekretär 3/3

Herrn Büroleiter ChBK 5/3

Büro ChBK
05. März 2014

Betr.: Konsolidierter Bericht des EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) zum NSA-Überwachungsprogramm

hier: Stellungnahme

Anlage: 1.) LIBE-Bericht (Stand: 21. Februar 2014)

2.) Mailzuschrift BMI, ÖS I 3 vom 03. März 2013 mit Anmerkungsbedarf

3.) Vorlage zum LIBE-Berichtsentwurf vom 21. Januar 2014

I. Votum

Kenntnisnahme und telefonische Kontaktaufnahme zum Büro Axel Voss, MdEP

II. Sachverhalt

Mit Mailzuschrift vom 25. Februar 2014 baten Sie um Prüfung des nunmehr inoffiziell vorliegenden konsolidierten Berichts des LIBE-Ausschusses (Anlage 1). Laut Mailzuschrift Büro Voss, MdEP vom 24. Februar 2014 sei zur Einbringung von Änderungsanträgen höchstwahrscheinlich bis zum 05. März 2014 Gelegenheit. Der Gesamtbericht wurde in Duktus und Inhalt bei Wertungen und Empfehlungen an die Kommission und die Mitgliedstaaten verschärft.

...

Der BND wurde von hier um Prüfung und Stellungnahme gebeten. Die dortigen, Ihnen seinerzeit mit Bezug 1 dargelegten zwei wesentlichen Änderungswünsche wurden in der aktuellen Berichtsfassung berücksichtigt. So wird auf S. 20 unter „Main findings", Ziffer 2, DEU und der BND nicht mehr genannt als ein Land, welches ein dem der NSA vergleichbares „Überwachungsprogramm" betreibe. Auf Seite 24 wird dieser Aspekt allerdings unter „Recommendations", Ziffer 23 als Aufforderung u.a. an DEU aufgegriffen, entsprechende Vorwürfe zu klären. Im Annex auf S. 60 wird Pr BND nunmehr korrekterweise in der Rubrik „Experten, die die Einladung des LIBE-Vorsitzenden abgelehnt haben" geführt.

BMI, ÖS I 3 teilte mit, Herr Voss MdEP habe sich mit der Bitte um Prüfung des konsolidierten Berichts sowohl an PSt Dr. Ole Schröder als auch an Dr. Hans-Peter Uhl, MdB gewandt. BMI werde, wie bereits bei der Entwurfsfassung des Berichts, per E-Mail Änderungswünsche an Herrn Voss, MdEP übermitteln. Diese liegen hier bislang nur in einer noch nicht von der BMI-Hausleitung freigegebenen Form vor (s. Anlage 2):

Darin unterstreicht auch das BMI, dass im Bericht nun nicht mehr unterstellt werde, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM. Zur o.a. Aufforderung an DEU, Vorwürfe bzgl. eines Überwachungsprogramms zu klären, verweist BMI darauf, dass die hier einschlägigen deutschen Vorschriften den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts entsprechen und grundrechtskonform sind. Unabhängig davon liege die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP. Deswegen werde weiterhin die Streichung dieser Empfehlung für notwendig erachten.

Zudem verweist BMI darauf, dass in Recommendation 99 u.a. die explizite Aufforderung an die KOM neu aufgenommen worden sei, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU

...

befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der MS im Bereich der IT-Sicherheit. Insbesondere im operativen Bereich liege die Zuständigkeit jedoch bei den Mitgliedstaaten und auch entsprechende Aktivitäten müssten bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (…)“ und den letzen Halbsatz ab „and to establish within ENISA's structure a Computer Emergency response Team (CERT) for the EU and its Member States") sollte daher lt. BMI eine Streichung angestrebt werden.

III. Bewertung

Es wird vorgeschlagen, dass Sie in einer telefonischen Erörterung mit Herrn Voss, MdEP, die neuerlichen Änderungsvorschläge des BMI ausdrücklich unterstützen. Zudem könnten Sie MdEP Voss für die eingebrachten und tatsächlich erfolgten Änderungen aus Sicht BKAmt, Abt. 6, sowie generell für den vertrauensvollen Austausch in dieser Angelegenheit danken.

erledigt

Referate 601 und 132 haben mitgezeichnet.

(Christian Kleidt)