EUROPA-PARLAMENTET 2009 - 2014

*Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender*

**2013/2188(INI)**

8.1.2014

# UDKAST TIL BETÆNKNING

om USA's NSA-overvågningsprogram, overvågningsorganer i forskellige medlemsstater og deres indvirkning på EU-borgeres grundlæggende rettigheder samt om det transatlantiske samarbejde inden for retlige og indre anliggender

(2013/2188(INI))

Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender

Ordfører: Claude Moraes

PR_INI

## INDHOLD

**Side**

## FORSLAG TIL EUROPA-PARLAMENTETS BESLUTNING

om USA's NSA-overvågningsprogram, overvågningsorganer i forskellige medlemsstater og deres indvirkning på EU-borgeres grundlæggende rettigheder samt om det transatlantiske samarbejde inden for retlige og indre anliggender
**(2013/2188(INI))**

*Europa-Parlamentet,*

– der henviser til traktaten om Den Europæiske Union (TEU), særlig artikel 2, 3, 4, 6, 7, 10, 11 og 21,

– der henviser til traktaten om Den Europæiske Unions funktionsmåde (TEUF), særlig artikel 15, 16 og 218 samt kapitel V,

– der henviser til protokol nr. 36 om overgangsbestemmelser og artikel 10 deri og til erklæring nr. 50 om denne protokol,

– der henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 og 52,

– der henviser til den europæiske menneskerettighedskonvention, særlig artikel 6, 8, 9, 10 og 13 og de tilhørende protokoller,

– der henviser til FN's universelle menneskerettighedserklæring, særlig artikel 7, 8, 10, 11, 12 og 14[1],

– der henviser til den internationale konvention om borgerlige og politiske rettigheder, særlig artikel 14, 17 og 19,

– der henviser til Europarådets konvention om databeskyttelse (ETS nr. 108) og tillægsprotokollen af 8. november 2001 til konventionen om beskyttelse af individet i forbindelse med automatisk behandling af personoplysninger, hvad angår tilsynsmyndigheder og grænseoverskridende datastrømme (ETS nr. 181),

– der henviser til Europarådets konvention om it-kriminalitet (ETS nr. 185),

– der henviser til den rapport, som FN's særlige rapportør om fremme og beskyttelse af menneskerettighederne og de grundlæggende frihedsrettigheder i forbindelse med terrorbekæmpelse fremsatte den 17. maj 2010[2],

– der henviser til den rapport, som FN's særlige rapportør for fremme og beskyttelse af menings- og ytringsfriheden fremsatte den 17. april 2013[3],

– der henviser til retningslinjerne om menneskerettigheder og bekæmpelse af terrorisme

[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.

som vedtaget af Europarådets Ministerkomité den 11. juli 2002,

– der henviser til Bruxelleserklæringen af 1. oktober 2010 fra den sjette konference i parlamentsudvalget for overvågning af EU-medlemsstaternes sikkerheds- og efterretningstjenester,

– der henviser til Europarådets Parlamentariske Forsamlings erklæring nr. 1954 (2013) om national sikkerhed og adgang til oplysninger,

– der henviser til rapporten om demokratisk kontrol med sikkerhedstjenester som vedtaget af Venedigkommissionen den 11. juni 2007[1], og som med stor interesse imødeser ajourføringen heraf, som er planlagt til foråret 2014,

– der henviser til vidneforklaringerne fra repræsentanterne i efterretningstilsynsudvalgene i Belgien, Nederlandene, Danmark og Norge,

– der henviser til de sager, der er indgivet for den franske[2], polske og britiske[3] domstol samt for Den Europæiske Menneskerettighedsdomstol[4], hvad angår masseovervågningssystemer,

– der henviser til Rådets konvention i henhold til artikel 34 i traktaten om Den Europæiske Union om gensidig retshjælp i straffesager mellem Den Europæiske Unions medlemsstater, særlig kapitel III[5],

– der henviser til Kommissionens beslutning nr. 520/2000 af 26. juli 2000 om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af Safe Harbour-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium,

– der henviser til Kommissionens evalueringsrapporter om gennemførelsen af Safe Harbour-principperne af 13. februar 2002 (SEK(2002)196) og af 20. oktober 2004 (SEK(2004)1323),

– der henviser til Kommissionens meddelelse af 27. november 2013 (COM(2013)0847) om Safe Harbour-princippernes funktionsmåde ud fra EU-borgernes og -virksomhedernes synspunkt og Kommissionens meddelelse af 27. november 2013 om genopretning af tilliden til datastrømmen mellem EU og USA (COM(2013)0846),

– der henviser til Europa-Parlamentets beslutning af 5. juli 2000 om Kommissionens forslag til beslutning om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af Safe Harbour-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium, som fandt, at systemets

[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 i Paris.
[3] Sager fra Privacy International og Liberty for Investigatory Powers Tribunal.
[4] Fælles anvendelse i henhold til artikel 34 i Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (fordringshavere) vs. Det Forenede Kongerige (skyldner).
[5] EFT L 197 af 12.7.2000, s. 1.

tilstrækkelighed ikke kunne bekræftes[1], og til Artikel 29-Gruppens udtalelser, særlig udtalelse nr. 4/2000 af 16. maj 2000[2],

– der henviser til aftalerne mellem Amerikas Forenede Stater og Den Europæiske Union om anvendelse og overførsel af passagerlisteoplysninger af 2004, 2007[3] og 2012[4],

– der henviser til den fælles gennemgang af gennemførelsen af aftalen mellem EU og USA om behandling og overførsel af passagerlisteoplysninger til United States Department of Homeland Security, som ledsager Kommissionens rapport til Europa-Parlamentet og Rådet om den fælles gennemgang (COM(2013)0844),

– der henviser til generaladvokat Cruz Villalóns udtalelse om, at direktiv 2006/24/EF om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet som helhed er uforeneligt med artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder, og at artikel 6 heri er uforenelig med chartrets artikel 7 og 52, stk. 1[5],

– der henviser til Rådets afgørelse 2010/412/EU af 13. juli 2010 om indgåelse af aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om behandling og overførsel af finansielle betalingsdata fra Den Europæiske Union til USA til brug for programmet til sporing af finansiering af terrorisme[6] og de tilhørende erklæringer fra Kommissionen og Rådet,

– der henviser til aftalen om gensidig retshjælp mellem Den Europæiske Union og Amerikas Forenede Stater[7],

– der henviser til de igangværende forhandlinger om en rammeaftale mellem EU og USA om beskyttelse af personoplysninger, når de overføres og behandles med henblik på at forebygge, undersøge, afsløre eller retsforfølge strafferetlige overtrædelser, herunder terrorisme, inden for rammerne af politisamarbejdet og det retlige samarbejde i straffesager ("paraplyaftalen"),

– der henviser til Rådets forordning (EF) nr. 2271/96 af 22. november 1996 om beskyttelse mod virkningerne af den ekstraterritoriale anvendelse af lovgivning vedtaget af et tredjeland og af foranstaltninger, som er baseret herpå eller er en følge heraf[8],

– der henviser til redegørelsen fra Den Føderative Republik Brasiliens præsident ved åbningen af FN's Generalforsamlings 68. samling den 24. september 2013 og arbejdet udført af det parlamentariske undersøgelsesudvalg om spionage som oprettet af det

[1] EFT L 121 af 24.4.2001, s. 152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32da.pdf.
[3] EUT L 204 af 4.8.2007, s. 18.
[4] EUT L 215 af 11.8.2012, s. 5.
[5] Generaladvokaten Cruz Villalóns udtalelse af 12. december 2013, sag C-293/12.
[6] EUT L 195 af 27.7.2010, s. 3.
[7] EUT L 181 af 19.7.2003, s. 34.
[8] EFT L 309 af 29.11.1996, s. 1.

føderale senat i Brasilien,

– der henviser til den amerikanske lov Patriot Act som underskrevet af præsident George W. Bush den 26. oktober 2001,

– der henviser til den amerikanske lov Foreign Intelligence Surveillance Act (FISA) af 1978 og ændringerne til FISA-loven af 2008,

– der henviser til dekret nr. 12333 som udstedt af den amerikanske præsident i 1981 og ændret i 2008,

– der henviser til de lovgivningsmæssige forslag, der i øjeblikket er ved at blive undersøgt i den amerikanske kongres, særlig udkastet til den amerikanske lov Freedom Act,

– der henviser til evalueringerne gennemført af det amerikanske råd for tilsyn med privatlivets fred og borgerlige rettigheder, det amerikanske nationale sikkerhedsråd og præsidentens undersøgelsesudvalg om efterretnings- og kommunikationsteknologi, særlig sidstnævntes rapport af 12. december 2013 med titlen "Liberty and Security in a Changing World" (frihed og sikkerhed i en verden i forandring),

– der henviser til afgørelsen truffet af Amerikas Forenede Staters distriktsdomstol for distriktet Columbia, Klayman et al. vs. Obama et al., det civile søgsmål nr. 13-0851 af 16. december 2013,

– der henviser til rapporten om resultaterne fra de europæiske medformænd for arbejdsgruppen mellem EU og USA om databeskyttelse af 27. november 2013[1],

– der henviser til sine beslutninger af 5. september 2001 og 7. november 2002 om eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet),

– der henviser til sin beslutning af 21. maj 2013 om EU-chartret: standarder for mediefrihed i EU[2],

– der henviser til sin beslutning af 4. juli 2013 om det amerikanske nationale sikkerhedsagenturs overvågningsprogram, tilsynsorganerne i forskellige medlemsstater og konsekvenserne for EU-borgerne, i henhold til hvilken Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender blev pålagt at gennemføre en dybdegående undersøgelse af sagen[3],

– der henviser til sin beslutning af 23. oktober 2013 om organiseret kriminalitet, korruption og hvidvaskning af penge: henstillinger om foranstaltninger og initiativer[4],

– der henviser til sin beslutning af 23. oktober 2013 om suspensionen af TFTP-aftalen

[1] Rådsdokument 16987/13.
[2] Vedtagne tekster, P7_TA(2013)0203.
[3] Vedtagne tekster, P7_TA(2013)0322.
[4] Vedtagne tekster, P7_TA(2013)0444.

som følge af det amerikanske sikkerhedsagenturs overvågning[1],

– der henviser til sin beslutning af 10. december 2013 om udnyttelse af potentialet ved cloud computing[2],

– der henviser til den interinstitutionelle aftale mellem Europa-Parlamentet og Rådet om fremsendelse til Europa-Parlamentet og dettes behandling af Rådets klassificerede informationer på andre områder end dem, der er omfattet af den fælles udenrigs- og sikkerhedspolitik[3],

– der henviser til forretningsordenens bilag VIII,

– der henviser til forretningsordenens artikel 48,

– der henviser til betænkning fra Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender (A70000/2013),

***Konsekvenserne af masseovervågning***

A. der henviser til, at båndene mellem Europa og Amerikas Forenede Stater tager udgangspunkt i demokratiets, frihedens, retfærdighedens og solidaritetens ånd og principper;

B. der henviser til, at gensidig tillid og forståelse er nøglefaktorer i den transatlantiske dialog;

C. der henviser til, at verden i september 2001 gik ind i en ny fase, som førte til, at de fleste regeringer fastsatte bekæmpelsen af terrorisme som sin hovedprioritet; der henviser til, at afsløringerne med udgangspunkt i lækkede dokumenter fra Edward Snowden, tidligere medarbejder i det amerikanske nationale sikkerhedsagentur, forpligtede demokratisk valgte ledere til at imødegå udfordringerne med efterretningsagenturernes øgede kapaciteter inden for overvågningsaktiviteter og konsekvenserne heraf for retsstatsprincippet i et demokratisk samfund;

D. der henviser til, at de afsløringer, der er kommet frem siden juni 2013, har medført utallige bekymringer i EU, hvad angår:

- omfanget af overvågningssystemerne som afsløret i både USA og i EU-medlemsstater;
- den høje risiko for at overtræde EU's juridiske standarder, grundlæggende rettigheder og databeskyttelsesstandarder;
- graden af tillid mellem EU og de amerikanske transatlantiske partnere;
- graden af samarbejde og inddragelse af visse EU-medlemsstater i USA's

[1] Vedtagne tekster, P7_TA(2013)0449.
[2] Vedtagne tekster, P7_TA(2013)0535.
[3] EUT C 353 E af 3.12.2013, s.156-167.

overvågningsprogrammer eller lignende programmer på nationalt plan som afsløret i medierne;

- USA's politiske myndigheders og visse EU-medlemsstaters grad af kontrol af og effektive tilsyn med deres efterretningsorganer;

- muligheden for, at disse masseovervågningsaktiviteter har andre formål end national sikkerhed og skærpet bekæmpelse af terrorisme, eksempelvis økonomisk og industriel spionage eller politisk motiveret profilering;

- efterretningsagenturernes og private it- og telekommunikationsvirksomheders roller og inddragelsesgrad;

- de stadig mere udflydende grænser mellem retshåndhævelse og efterretningsaktiviteter, hvilket medfører, at alle borgere behandles som mistænkte;

- truslerne mod privatlivets fred i en digital tidsalder;

E. der henviser til, at det hidtil usete omfang af den afslørede spionage nødvendiggør en fuld undersøgelse ved de amerikanske myndigheder, EU-institutionerne og medlemsstaternes regeringer og nationale parlamenter;

F. der henviser til, at de amerikanske myndigheder har nægtet nogle af de afslørede oplysninger, men ikke anfægtet størsteparten deraf; der henviser til, at der har været en omfattende offentlig debat i USA, mens denne har været begrænset i EU-medlemsstaterne; der henviser til, at EU's regeringer alt for ofte forholder sig tavse og afholder sig fra at gennemføre passende undersøgelser;

G. der henviser til, at EU-institutionerne har ansvar for at sikre en fuld gennemførelse af EU-lovgivningen til fordel for EU-borgerne, og at EU-traktaternes retskraft ikke undermineres af en afvisning af de ekstraterritoriale virkninger af tredjelandes standarder eller aktiviteter;

***Udviklinger i USA, hvad angår en efterretningsreform***

H. der henviser til distriktsdomstolen for distriktet Columbia, som i sin afgørelse af 16. december 2013 har bestemt, at det amerikanske nationale efterretningsagenturs masseindsamling af metadata er en overtrædelse af fjerde ændring til den amerikanske forfatning[1];

I. der henviser til en afgørelse truffet af distriktsdomstolen for det østlige distrikt i Michigan, som har bestemt, at der ifølge den fjerde ændring kræves rimelighed i alle søgninger, forudgående varsler for rimelige søgninger af enhver art, arrestordrer med udgangspunkt i en eksisterende sandsynlig årsag og hensyntagen til personer, sted og sager samt inddragelse af en neutral dommer mellem det retshåndhævende personale

[1] Klayman et al. vs. Obama et al., civilt søgsmål nr. 13-0851, 16. december 2013.

for den udøvende magt og borgerne[1];

J. der henviser til, at præsidents undersøgelsesudvalg om efterretnings- og kommunikationsteknologi i sin rapport af 12. december 2013 kommer med 45 anbefalinger til den amerikanske præsident; der henviser til, at anbefalingerne understreger behovet for en beskyttelse af den nationale sikkerhed samtidig med privatlivets fred og borgerrettighederne; der i den forbindelse henviser til, at den amerikanske regering opfordres til så snart som muligt at indstille sin masseindsamling af telefonaflytninger af amerikanske borgere i henhold til afsnit 215 i den amerikanske lov Patriot Act, at gennemføre en dybdegående undersøgelse af det amerikanske nationale sikkerhedsagentur og den lovmæssige ramme for den amerikanske efterretning med henblik på at sikre respekten for retten til privatlivets fred, at indstille aktiviteter, som undergraver kommerciel software (bagdøre og malware) og gør denne sårbar, at øge brugen af kryptering, særlig i sager med data under overførsel, og ikke at underminere bestræbelserne på at udvikle krypteringsstandarder, at oprette en advokat for de offentlige interesser, som skal repræsentere privatlivets fred og borgerrettighederne ved den amerikanske domstol for udenlandsk efterretningsovervågning, at bemyndige det amerikanske råd for tilsyn med privatlivets fred og borgerlige rettigheder til at føre tilsyn med efterretningsorganernes aktiviteter af udenlandske efterretningshensyn og ikke blot med henblik på bekæmpelsen af terrorisme og at modtage klager fra whistleblowers, at gøre brug af traktaterne om gensidig retshjælp til indhentning af elektroniske meddelelser og ikke at gøre brug af overvågning for at stjæle industrielle eller handelshemmeligheder;

K. der henviser til, at anbefalingerne til den amerikanske præsident i forbindelse med efterretningsaktiviteterne vedrørende ikkeamerikanske borgere i henhold til afsnit 702 i FISA anerkender det grundlæggende spørgsmål vedrørende respekten af privatlivets fred og den menneskelige værdighed i henhold til artikel 12 i FN's verdenserklæring om menneskerettigheder og artikel 17 i den internationale konvention om borgerlige og politiske rettigheder; der henviser til, at de ikke anbefaler, at ikkeamerikanske borgere tillægges de samme rettigheder og den samme beskyttelse som amerikanske borgere;

***Lovgivningsramme***

*Grundlæggende rettigheder*

L. der henviser til, at rapporten om resultaterne fra de europæiske medformænd for arbejdsgruppen mellem EU og USA om databeskyttelse giver et overblik over den lovmæssige situation i USA, men ikke i tilstrækkelig grad har bidraget til klarlægningen af fakta omkring USA's efterretningsprogrammer; der henviser til, at der ikke er blevet offentliggjort oplysninger om den såkaldte "spor nummer to"-arbejdsgruppe, i hvilken medlemsstaterne bilateralt diskuterer sager vedrørende den nationale sikkerhed med de amerikanske myndigheder;

M. der henviser til, at de grundlæggende rettigheder, navnlig ytringsfriheden,

[1] ACLU vs. NSA nr. 06-CV-10204, 17. august 2006.

pressefriheden, tankefriheden, samvittighedsfriheden, religionsfriheden og forsamlingsfriheden, privatlivets fred, databeskyttelse samt retten til adgang til effektive retsmidler, uskyldsformodningen og retten til retfærdig rettergang og ikkeforskelsbehandling i henhold til Den Europæiske Unions charter om grundlæggende rettigheder er hjørnesten i demokratiet;

*Unionens kompetencer på sikkerhedsområdet*

N. der henviser til, at EU i henhold til artikel 67, stk. 3, i TEUF "bestræber sig på at sikre et højt sikkerhedsniveau"; der henviser til, at EU i henhold til bestemmelserne i traktaten (særlig artikel 4, stk. 2, i TEU, artikel 72 i TEUF og artikel 73 i TEUF) råder over specifikke kompetencer i anliggender i forbindelse med EU's fælles sikkerhed; der henviser til, at EU har udøvet sin kompetence i forbindelse med national sikkerhed ved at fastlægge en række lovgivningsinstrumenter og indgå internationale aftaler (PNR, TFTP), som har til formål at bekæmpe alvorlig kriminalitet og terrorisme, og ved at fastlægge en intern sikkerhedsstrategi og agenturer, der arbejder på dette område;

O. der henviser til, at der eksisterer en overlapning mellem koncepterne "national sikkerhed", "indre sikkerhed", "indre sikkerhed i EU" og "international sikkerhed"; der henviser til, at Wienerkonventionen om traktatretten, princippet om loyalt samarbejde mellem EU-medlemsstaterne og det generelle menneskerettighedsprincip om at fortolke undtagelser af enhver art snævert peger mod en restriktiv fortolkning af begrebet "national sikkerhed" og betyder, at medlemsstaterne skal afholde sig fra at gribe ind i EU's kompetencer;

P. der henviser til, at medlemsstaternes agenturer og selv private aktører med aktiviteter på området for den nationale sikkerhed i henhold til den europæiske menneskerettighedskonvention ligeledes skal respektere rettighederne i konventionen, både over for deres egne borgere og andre staters borgere; der henviser til, at dette ligeledes gælder for samarbejde med andre staters myndigheder på området for den nationale sikkerhed;

*Ekstraterritorialitet*

Q. der henviser til, at et tredjelands ekstraterritoriale anvendelse af sine love, bestemmelser og andre lovgivningsmæssige retsakter eller gennemførelsesretsakter i situationer, som henhører under EU's eller EU-medlemsstaternes jurisdiktion, kan påvirke den etablerede lovlige orden og retsstatsprincippet eller endda være i strid med international eller EU-lovgivning, herunder fysiske og juridiske personers rettigheder, idet der tages højde for omfanget af og det erklærede eller reelle mål med en sådan anvendelse; der henviser til, at der i disse særlige tilfælde er brug for handling på EU-niveau for at sikre respekten af retsstatsprincippet og fysiske og juridiske personers rettigheder i EU, navnlig ved at fjerne, neutralisere, blokere eller på anden vis bekæmpe konsekvenserne af den pågældende udenlandske lovgivning;

***International dataoverførsel***

R. der henviser til, at EU-institutionernes, -kontorernes eller -agenturernes eller

medlemsstaternes overførsel af personlige oplysninger til USA af hensyn til retshåndhævelsen uden tilstrækkelige sikkerhedsforanstaltninger og tilstrækkelig beskyttelse af respekten af EU-borgernes grundlæggende rettigheder, navnlig retten til privatliv og beskyttelsen af personlige oplysninger, i henhold til artikel 340 i TEUF eller EU-Domstolens etablerede retspraksis gør den pågældende EU-institution, -kontor eller -agentur ansvarlig for overtrædelsen af EU-lovgivningen – herunder enhver overtrædelse af de grundlæggende rettigheder i henhold til EU-chartret;

*Overførsler til USA med udgangspunkt i de amerikanske Safe Harbour-principper*

S. der henviser til, at den amerikanske lovgivningsmæssige ramme om databeskyttelse ikke sikrer EU-borgerne et tilstrækkeligt beskyttelsesniveau;

T. der henviser til, at Kommissionen i sin beslutning nr. 520/2000 med henblik på at sikre, at EU's registeransvarlige kan overføre personlige oplysninger til et organ i USA, har erklæret, at beskyttelsen af de personlige oplysninger, der overføres fra EU til organisationer i Amerikas Forenede Stater, som har tiltrådt Safe Harbour-principperne, i henhold til Safe Harbour-principperne om privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium er tilstrækkelig;

U. der henviser til, at Europa-Parlamentet i sin beslutning af 5. juli 2000 tvivlede på og udtrykte bekymring, hvad angår Safe Harbour-princippernes tilstrækkelighed, og opfordrede Kommissionen til rettidigt at revidere sin beslutning i lyset af erfaringer og lovgivningsmæssige udviklinger af enhver art;

V. der henviser til, at Kommissionens beslutning nr. 520/2000 indeholder bestemmelser om, at medlemsstaternes kompetente myndigheder kan udøve deres eksisterende beføjelser og suspendere datastrømmene til en organisation, som på grundlag af selvcertificering har tilsluttet sig de amerikanske Safe Harbour-principper, med henblik på at beskytte personer ved behandlingen af deres personlige oplysninger i tilfælde, hvor der er stor sandsynlighed for, at Safe Harbour-principperne bliver overtrådt, eller en fortløbende overførsel ville medføre en stor risiko for på betydelig vis at skade de registrerede;

W. der henviser til, at Kommissionens beslutning nr. 520/2000 ligeledes fastsætter, at Kommissionen i de tilfælde, hvor der foreligger dokumentation for, at en aktør med ansvar for at sikre overholdelsen af principperne ikke effektivt varetager denne opgave, skal informere det amerikanske handelsministerium og om nødvendigt fremlægge foranstaltninger til ophævelse eller suspension af den pågældende beslutning eller begrænse dens anvendelsesområde;

X. der henviser til, at Kommissionen i de første to rapporter om gennemførelsen af Safe Harbour-principperne fra 2002 og 2004 præsenterede en række problemstillinger, hvad angår den korrekte gennemførelse af Safe Harbour-principperne, og fremlagde en række anbefalinger for de amerikanske myndigheder med henblik på at revidere principperne;

Y. der henviser til, at Kommissionen i sin tredje gennemførelsesrapport af 27. november 2013 – ni år efter den anden rapport og uden at indeholde nogen af de mangler, der

blev fremført i denne rapport, og som er blevet afhjulpet – identificerede en række yderligere vidtrækkende svagheder og mangler i Safe Harbour-principperne og konkluderede, at den aktuelle gennemførelse ikke kunne fastholdes; der henviser til, at Kommissionen har understreget, at de amerikanske efterretningsagenturers omfattende adgang til oplysninger overført til USA af Safe Harbour-certificerede organer yderligere giver anledning til alvorlig bekymring, hvad angår den fortsatte beskyttelse af EU-registreredes oplysninger; der henviser til, at Kommissionen fremlagde 13 anbefalinger for de amerikanske myndigheder og traf foranstaltninger til inden sommeren 2014 og i samarbejde med de amerikanske myndigheder at identificere en række afhjælpende tiltag, som skal gennemføres hurtigst muligt, til udarbejdelse af grundlaget for en fuldstændig gennemgang af Safe Harbour-principperne;

Z. der henviser til, at delegationen af Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE-udvalget) den 28. til 31. oktober 2013 var i Washington D.C. for at mødes med det amerikanske handelsministerium og US Federal Trade Commission; der henviser til, at handelsministeriet anerkendte, at der findes organisationer, som på grundlag af selvcertificering har tilsluttet sig Safe Harbour-principperne, men tydeligvis har status som "not-current", hvilket betyder, at virksomheden ikke overholder Safe Harbour-kravene, på trods af at den fortsat modtager personlige oplysninger fra EU; der henviser til, at Federal Trade Commission gav tilladelse til en gennemgang af Safe Harbour-principperne med henblik på en forbedring heraf, navnlig hvad angår klager og alternative tvistbilæggelsessystemer;

AA. der henviser til, at Safe Harbour-principperne muligvis er begrænset til det omfang, der er nødvendigt for at overholde krav om national sikkerhed, offentlige interesser eller retshåndhævelse; der henviser til, at en undtagelse – forstået som undtagelse fra en grundlæggende rettighed – altid skal fortolkes restriktivt og begrænses til det, der er nødvendigt og rimeligt i et demokratisk samfund, og at loven tydeligt skal fastlægge betingelserne og sikkerhedsforanstaltningerne, således at denne begrænsning bliver legitim; der henviser til, at en sådan undtagelse ikke bør finde anvendelse på en måde, der underminerer beskyttelsen i henhold til EU's lovgivning om databeskyttelse og Safe Harbour-principperne;

AB. der henviser til, at de amerikanske efterforskningsagenturers vidtrækkende adgang i alvorlig grad har udhulet den transatlantiske tillid og på negativ vis har påvirket tilliden til amerikanske organisationer med aktiviteter i EU; der henviser til, at dette forværres ydermere af manglen på retlige og administrative klagemidler i den amerikanske lovgivning for EU's borgere, navnlig i forbindelse med overvågningsaktiviteter til efterforskningsformål;

*Overførsel til tredjelande med afgørelse om tilstrækkelighed*

AC. der henviser til, at New Zealands og Canadas nationale sikkerhedsagenturer ifølge afslørede oplysninger og resultaterne i LIBE-udvalgets undersøgelse i omfattende grad har været involveret i masseovervågning af elektroniske meddelelser og aktivt har samarbejdet med USA under det såkaldte "Five eyes"-program og muligvis har udvekslet andre personlige oplysninger om EU's borgere overført fra EU med

hinanden;

AD. der henviser til, at Kommissionens beslutning nr. 2013/65 og nr. 2/2002 af 20. december 2001 har fastlagt, at beskyttelsesniveauet i New Zealands og Canadas lovgivning om beskyttelsen af personlige oplysninger og elektroniske dokumenter er tilstrækkeligt; der henviser til, at de ovenstående afsløringer også i alvorlig grad påvirker tilliden til retssystemerne i de pågældende lande, hvad angår EU-borgernes fortsatte beskyttelse, der henviser til, at Kommissionen ikke har undersøgt dette aspekt;

*Overførsel baseret på kontraktbestemmelser og andre instrumenter*

AE. der henviser til, at direktiv 95/46/EF fastsætter, at internationale overførsler til et tredjeland ligeledes kan ske ved hjælp af specifikke instrumenter, hvorved den registeransvarlige yder passende garantier i forhold til beskyttelsen af privatlivets fred og de grundlæggende rettigheder samt personfriheder og i forhold til udøvelsen af de pågældende rettigheder;

AF. der henviser til, at disse garantier især kan fremgå af passende kontraktbestemmelser;

AG. der henviser til, at Kommissionen i henhold til direktiv 95/46/EF tillægges beføjelser til at træffe beslutning om, at de specifikke kontraktbestemmelser udgør en tilstrækkelig garanti i overensstemmelse med direktivet, og henviser til, at Kommissionen på grundlag heraf har vedtaget tre modeller for standardkontraktbestemmelser for overførsler til registeransvarlige og registerførere (og underleverandører) i tredjelande;

AH. der henviser til, at Kommissionens beslutning om fastlæggelse af standardkontraktbestemmelserne fastlægger, at medlemsstaternes kompetente myndigheder kan gøre brug af deres beføjelser til at suspendere datastrømme, så snart det er blevet konkluderet, at den lovgivning, som dataimportøren eller en underleverandør er underlagt, pålægger denne krav om at afvige fra den gældende databeskyttelseslovgivning, som rækker videre end de restriktioner, som er nødvendige i et demokratisk samfund i henhold til artikel 13 i direktiv 95/46/EF, og som sandsynligvis kan have en betydelig negativ indvirkning på garantierne i henhold til den gældende databeskyttelseslovgivning og standardkontraktbestemmelserne, eller fordi der foreligger en stor sandsynlighed for, at standardkontraktbestemmelserne i bilaget ikke bliver eller ikke vil blive overholdt, eller fordi der ved fortsat overførsel er en overhængende risiko for på betydelig vis at skade de registrerede;

AI. der henviser til, at nationale databeskyttelsesmyndigheder har udarbejdet bindende virksomhedsregler for at lette internationale overførsler inden for et multinationalt samarbejde med passende sikkerhedsforanstaltninger i forhold til beskyttelsen af privatlivets fred og de grundlæggende rettigheder samt personfriheder og i forhold til udøvelsen af de pågældende rettigheder; der henviser til, at de bindende virksomhedsregler skal godkendes af medlemsstaternes kompetente myndigheder, inden de tages i brug, efter at sidstnævnte har evalueret overensstemmelsen med EU's databeskyttelseslovgivning;

*Overførsler baseret på TFTP- og PNR-aftaler*

AJ. der henviser til, at Europa-Parlamentet i sin beslutning af 23. oktober 2013 udtrykte alvorlig bekymring over afsløringerne i forbindelse med NSA's aktiviteter med hensyn til direkte adgang til meddelelser om finansielle betalinger og relaterede data, hvilket ville betyde et klart brud på aftalen, især artikel 1 heri;

AK. der henviser til, at Europa-Parlamentet har bedt Kommissionen om at suspendere aftalen og anmodet om, at alle relevante oplysninger og dokumenter omgående gøres tilgængelige med henblik på overvejelser i Parlamentet;

AL. der henviser til, at Kommissionen, efter at påstandene var blevet offentliggjort i medierne, besluttede at indlede høringer med USA i henhold til artikel 19 i TFTP-aftalen; der endvidere henviser til, at kommissær Malmström den 27. november 2013 meddelte LIBE-udvalget, at Kommissionen efter at have mødtes med myndighederne i USA og i betragtning af de svar, de amerikanske myndigheder havde givet i deres breve og under deres møder, havde besluttet ikke at fortsætte høringerne på grund af, at intet tydede på, at den amerikanske regering havde handlet i modstrid med bestemmelserne i aftalen, samt at USA har givet skriftlig garanti for, at der ikke havde fundet nogen direkte dataindsamling sted i modstrid med bestemmelserne i TFTP-aftalen;

AM. der henviser til, at LIBE's delegation til Washington i dagene 28.-31. oktober 2013 havde møder med USA's finansministerium; der endvidere henviser til, at USA's finansministerium fastslog, at det efter TFTP-aftalens ikrafttræden ikke havde haft adgang til data fra SWIFT i EU, undtagen inden for rammerne af TFTP; der henviser til, at USA's finansministerium afslog at udtale sig om, hvorvidt der kunne have været adgang til SWIFT-data uden for TFTP fra noget andet amerikansk regeringsorgans eller departements side, eller om USA's regering var vidende om NSA's masseovervågningsaktiviteter; der endvidere henviser til, at Glenn Greenwald den 18. december 2013 til LIBE-udvalgets undersøgelse udtalte, at NSA og GCHQ havde haft SWIFT-netværk som mål;

AN. der henviser til, at de belgiske og hollandske databeskyttelsesmyndigheder den 13. november 2013 besluttede at foretage en fælles undersøgelse af SWIFT's betalingsnetværk for at fastslå, om tredjepart kunne opnå ubeføjet eller ulovlig adgang til europæiske borgeres bankdata[1];

AO. der henviser til, at USA's Department of Homeland Security (DHS) ifølge den fælles gennemgang af den europæisk-amerikanske PNR-aftale havde foretaget 23 indberetninger af PNR-data til NSA fra sag til sag til støtte for antiterrorsager på en måde, der var i overensstemmelse med aftalens betingelser;

AP. der henviser til, at det i den fælles gennemgang ikke bliver nævnt, at ikkeamerikanske statsborgere i henhold til amerikansk lov ved behandling af persondata til efterretningsformål ikke har nogen retlige eller administrative muligheder for at

[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.

beskytte deres rettigheder, samt at forfatningsmæssig beskyttelse kun ydes til amerikanske personer; der endvidere henviser til, at denne mangel på retlige eller administrative rettigheder annullerer den beskyttelse for EU-borgere, som er fastlagt i den eksisterende PNR-aftale;

*Overførsler baseret på EU's og USA's aftale om gensidig retshjælp i straffesager*

AQ. der henviser til, at *EU's og USA's* aftale om gensidig retshjælp i straffesager af 6. juni 2003[1] trådte i kraft 1. februar 2010 og er beregnet til at lette samarbejdet mellem EU og US for at bekæmpe kriminalitet på en mere effektiv måde under behørig hensyntagen til fysiske personers rettigheder og retsstatsprincippet;

*Rammeaftale om databeskyttelse inden for politisamarbejde og retligt samarbejde ("paraplyaftale")*

AR. der henviser til, at formålet med denne overordnede aftale er at fastlægge de retlige rammer for alle overførsler af persondata mellem EU og USA udelukkende med det formål at forebygge, efterforske, afsløre eller retsforfølge strafferetlige overtrædelser, herunder terrorisme, inden for rammerne af politisamarbejdet og det retlige samarbejde i straffesager; der endvidere henviser til, at forhandlingerne blev godkendt af Rådet den 2. december 2010;

AS. der henviser til, at denne aftale skulle sikre klare og præcise juridisk bindende principper for databehandling og navnlig skulle anerkende EU-borgeres ret til at få adgang til, korrigere og slette deres persondata i USA samt retten til en effektiv administrativ og retlig klageordning for EU-borgere og et uafhængigt tilsyn med databehandlingsaktiviteterne;

AT. der henviser til, at Kommissionen i sin meddelelse af 27. november 2013 påpegede, at "paraplyaftalen" skulle resultere i et højt beskyttelsesniveau for borgere på begge sider af Atlanten, samt at den skulle styrke europæernes tillid til dataudvekslinger mellem EU og USA og derved skabe grundlag for en videreudvikling af det sikkerhedsmæssige samarbejde og partnerskab mellem EU og USA;

AU. der henviser til, at forhandlingerne om aftalen ikke har gjort fremskridt som følge af USA's regerings vedvarende afvisning af at anerkende EU-borgeres ret til effektive administrative og retlige klagemuligheder og på grund af intentionen om at indføre omfattende undtagelser fra de principper om databeskyttelse, der er indeholdt i aftalen, såsom formålsbegrænsning, dataopbevaring eller videreoverførsler enten i hjemlandet eller i udlandet;

***Databeskyttelsesreform***

AV. der henviser til, at EU's rammelovgivning for databeskyttelse er ved at blive revideret med det formål at oprette et omfattende, konsistent, moderne og robust system til alle databehandlingsaktiviteter i EU; der endvidere henviser til, at Kommissionen i januar

[1] EUT L 181 af 19.7.2003, s. 25.

2012 fremsatte en række lovforslag: en generel forordning om databeskyttelse[1], som skal erstatte direktiv 95/46/EF og indføre en ensartet lovgivning i hele EU, samt et direktiv,[2] der skal opstille en harmoniseret ramme for alle retshåndhævende myndigheders databehandlingsaktiviteter med henblik på retshåndhævelse og skal begrænse de nuværende divergenser mellem de nationale love;

AW. der henviser til, at LIBE-udvalget den 21. oktober 2013 vedtog sine lovgivningsmæssige betænkninger om de to forslag og en afgørelse om at påbegynde forhandlinger med Rådet med henblik på at få de retlige instrumenter vedtaget i løbet af indeværende valgperiode;

AX. der henviser til, at Det Europæiske Råd på trods af, at det på mødet den 24. og 25. oktober 2013 opfordrede til en rettidig vedtagelse af et stærkt generelt EU-regelsæt for databeskyttelse for at fremme borgernes og virksomhedernes tillid til den digitale økonomi, alligevel ikke har været i stand til at nå frem til en fælles holdning til en generel forordning om databeskyttelse og til direktivet[3];

***It-sikkerhed og cloud computing***

AY. der henviser til, at beslutningen af 10. december[4] understreger det økonomiske potentiale for vækst og udvikling, der ligger i "cloud computing"-forretninger;

AZ. der henviser til, at niveauet for databeskyttelse i et cloud computing-miljø ikke må være lavere end det, der kræves i enhver anden databehandlingssammenhæng; der endvidere henviser til, at EU's databeskyttelseslovgivning, eftersom den er teknologisk neutral, allerede har fuld gyldighed for cloud computing-tjenester, der opererer i EU;

BA. der henviser til, at masseovervågningsaktiviteter giver efterretningsorganer adgang til personlige data, som er gemt af enkeltpersoner i EU-lande ifølge cloud-aftaler med store cloud-udbydere i USA; der endvidere henviser til, at USA's efterretningsmyndigheder har haft adgang til persondata, der var gemt på servere placeret på EU's territorium, ved at gå ind i de interne netværk tilhørende Yahoo og Google[5]; der henviser til, at sådanne aktiviteter udgør en krænkelse af internationale forpligtelser; der endvidere henviser til, at det ikke kan udelukkes, at efterretningsmyndigheder også har haft adgang til oplysninger, som er gemt på cloud-tjenester af medlemsstaters offentlige myndigheder eller virksomheder og institutioner;

***Demokratisk tilsyn med efterretningstjenester***

BB. der henviser til, at efterretningstjenesterne udfylder en vigtig funktion, idet de beskytter det demokratiske samfund mod indre og ydre trusler; der endvidere henviser til, at de har fået tildelt særlige beføjelser og værktøjer til dette formål; der henviser til, at disse beføjelser skal bruges efter retsstatsprincipper, da de ellers risikerer at miste

[1] COM(2012)0011 af 25.1.2012.
[2] COM(2012)0010 af 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] Washington Post, 31. oktober 2013.

legitimitet og undergrave samfundets demokratiske natur;

BC. der henviser til, at det høje hemmeligholdelsesniveau, der er uløseligt forbundet med efterretningstjenesterne – for at undgå at bringe igangværende operationer i fare, afsløre arbejdsmetoder eller sætte agenters liv på spil – forhindrer fuld gennemsigtighed, offentlig kontrol og almindelige demokratiske eller retlige undersøgelser;

BD. der henviser til, at den teknologiske udvikling har ført til et forøget internationalt samarbejde inden for efterretningstjenesterne, som også indebærer udveksling af personoplysninger og ofte tilslører grænsen mellem efterretnings- og retshåndhævelsessamarbejde;

BE. der henviser til, at de fleste af de eksisterende nationale tilsynsmekanismer og -organer blev oprettet eller moderniseret i 1990'erne og ikke er blevet tilstrækkeligt tilpasset til den hurtige teknologiske udvikling inden for det sidste årti;

BF. der henviser til, at det demokratiske tilsyn med efterretningsaktiviteter stadig foregår på nationalt plan på trods af den stigende udveksling af oplysninger mellem EU-medlemsstaterne og mellem medlemsstater og tredjelande; der henviser til, at der er en voksende kløft mellem niveauet for det internationale samarbejde på den ene side og den tilsynskapacitet, som er begrænset til det nationale niveau, på den anden, hvilket resulterer i utilstrækkelig og ineffektiv demokratisk kontrol;

***Hovedkonklusioner***

1. mener, at whistleblowers og journalisters afsløringer i pressen for nylig samt de vidneudsagn, der er blevet givet af eksperter i løbet af denne undersøgelse, har resulteret i afgørende beviser for eksistensen af vidtrækkende, komplekse og teknologisk yderst avancerede systemer, designet af USA's og nogle medlemsstaters efterretningstjenester for at indsamle, opbevare og analysere kommunikations- og lokaliseringsdata og -metadata vedrørende alle borgere rundt om i verden i en hidtil uset skala og på en måde, der er vilkårlig og ikke bygger på mistanke;

2. peger specifikt på de amerikanske NSA-efterretningsprogrammer, der muliggør en masseovervågning af EU-borgere gennem direkte adgang til de centrale servere hos førende amerikanske internetselskaber (programmet PRISM), analyse af indhold og metadata (programmet Xkeyscore), omgåelse af onlinekryptering (BULLRUN), adgang til computer- og telefonnetværk og adgang til lokaliseringsdata samt til den britiske efterretningstjeneste GCHQ's systemer, såsom dennes overvågningsaktivitet i kommunikationens tidlige fase (Tempora-programmet) og dekrypteringsprogram (Edgehill); mener, at det er sandsynligt, at der eksisterer programmer af lignende art, omend i en mere begrænset skala, i andre EU-lande, såsom Frankrig (DGSE), Tyskland (BND) og Sverige (FRA);

3. noterer sig beskyldningerne mod den britiske efterretningstjeneste GCHQ om "hacking" eller udnyttelse af Belgacom-systemerne; refererer endnu en gang oplysningerne fra Belgacom om, at man her ikke kunne bekræfte, at EU-institutioner var mål herfor eller berørt heraf, og at den anvendte malware var yderst kompliceret

og havde krævet så omfattende økonomiske og personalemæssige ressourcer at udvikle og anvende, at disse ikke kunne være tilgængelige for private enheder eller hackere;

4. fastslår, at der har været tilfælde af alvorlige brud på tillid: tillid mellem de to transatlantiske partnere, tillid mellem EU-medlemsstater, tillid mellem borgerne og deres regeringer, tillid til respekten for retsstatsprincipperne og tillid til sikkerheden i it-tjenesterne; mener, at der er et påtrængende behov for en omfattende plan, hvis man skal genopbygge tilliden inden for alle disse dimensioner;

5. bemærker, at flere regeringer hævder, at disse masseovervågningsprogrammer er nødvendige for at bekæmpe terrorisme; støtter helhjertet kampen mod terrorisme, men er af den faste overbevisning, at den aldrig i sig selv kan retfærdiggøre vilkårlige, hemmelige og sommetider endog ulovlige masseovervågningsprogrammer; udtrykker derfor bekymring angående lovligheden, nødvendigheden og proportionaliteten af disse programmer;

6. anser det for meget tvivlsomt, om dataindsamling af et sådant omfang kun styres af kampen mod terrorisme, eftersom den involverer indsamling af alle mulige data vedrørende alle borgere; påpeger derfor den mulige eksistens af andre magtrelaterede motiver, såsom politisk og økonomisk spionage;

7. sætter spørgsmålstegn ved foreneligheden mellem visse medlemsstaters massive økonomiske spionageaktiviteter inden for EU's indre marked og de konkurrenceregler, der er nedfældet i afsnit I og afsnit VII i traktaten om Den Europæiske Unions funktionsmåde; bekræfter igen princippet om loyalt samarbejde, som det er nedfældet i artikel 4, stk. 3, i traktaten om Den Europæiske Union, og princippet om, at medlemsstaterne skal afholde sig fra at træffe foranstaltninger, der kan bringe virkeliggørelsen af Unionens mål i fare;

8. konstaterer, at internationale traktater samt EU's og USA's lovgivning såvel som nationale tilsynsmekanismer ikke har kunnet levere de nødvendige kontrolforanstaltninger og den nødvendige demokratiske ansvarlighed;

9. fordømmer på det skarpeste den kolossale, systematiske og altomfattende indsamling af uskyldige menneskers personlige data, som ofte omfatter intime personoplysninger; understreger, at efterretningstjenesternes massive, vilkårlige overvågningssystemer udgør et alvorligt indgreb i borgernes grundlæggende rettigheder; understreger endvidere, at privatlivets fred ikke er en luksusrettighed, men at den er grundstenen i et frit og demokratisk samfund; fremhæver desuden, at masseovervågning har potentielt alvorlige konsekvenser for pressefrihed, menings- og ytringsfrihed og er et væsentligt potentiale for misbrug af de indsamlede oplysninger mod politiske modstandere; understreger, at disse masseovervågningsaktiviteter også ser ud til at medføre ulovlige handlinger fra efterretningstjenesternes side og rejse spørgsmål om de nationale loves ekstraterritorialitet;

10. ser overvågningsprogrammerne som endnu et skridt mod etableringen af en fuldt udbygget forebyggelsesstat, hvor man har ændret det etablerede paradigme for strafferetten i demokratiske samfund og i stedet indført en blanding af

retshåndhævelse og efterretningsaktiviteter med udflydende retsgarantier, som ofte ikke er på linje med de demokratiske kontrolforanstaltninger og grundlæggende rettigheder, især forhåndsformodningen om manglende skyld; erindrer i denne forbindelse om den tyske forbundsforfatningsdomstols afgørelse[1] om at forbyde brugen af præventive slæbegarn ("präventive Rasterfahndung"), så længe der ikke er bevis for en konkret fare for andre højtrangerende juridisk beskyttede rettigheder, således at en generel trusselsituation eller internationale spændinger ikke er tilstrækkelige til at retfærdiggøre sådanne skridt;

11. insisterer på, at hemmelige love, traktater og domstole er en krænkelse af retsstatsprincipperne; fremhæver, at enhver kendelse afsagt af en domstol eller et tribunal og enhver beslutning af en administrativ myndighed, som er truffet i en ikke-EU-stat, og som direkte eller indirekte godkender overvågningsaktiviteter som dem, der har været genstand for nærværende undersøgelse, ikke automatisk må blive godkendt eller træde i kraft, men skal enkeltvis underkastes de relevante nationale behandlinger vedrørende gensidig anerkendelse og juridisk bistand, herunder regler, der har gyldighed i kraft af bilaterale aftaler;

12. gør opmærksom på, at ovennævnte bekymringer forværres af den hurtige teknologiske udvikling og de samfundsmæssige forandringer; finder, at eftersom internettet og de mobile anordninger findes overalt i det moderne dagligliv (den allestedsnærværende computerisering), og de fleste internetfirmaers forretningsmodel bygger på behandling af persondata af alle slags, som truer personens integritet, er dette et problem af en hidtil uset størrelse;

13. anser det for en klar konklusion, som det blev understreget af de teknologiske eksperter, der afgav vidneforklaring for undersøgelsen, at der på det nuværende trin af den teknologiske udvikling ikke er nogen garanti for, hverken for de offentlige EU-institutioner eller for borgerne, at deres it-sikkerhed eller deres privatliv kan sikres mod indbrud fra veludstyrede tredjelandes eller EU-efterretningstjenesters side (100 % it-sikkerhed findes ikke); bemærker, at denne alarmerende situation kun kan udbedres, hvis europæerne er villige til at ofre tilstrækkelige ressourcer, både menneskelige og økonomiske, på bevarelsen af Europas uafhængighed og selvstændighed;

14. afviser på det kraftigste den ide, at disse emner kun handler om national sikkerhed og derfor kun falder ind under medlemsstaternes kompetence; erindrer om følgende afgørelse i Domstolen for kort tid siden: "selv om det tilkommer medlemsstaterne at træffe de nødvendige foranstaltninger til at opretholde deres indre og ydre sikkerhed, medfører alene den omstændighed, at en afgørelse vedrører statens sikkerhed, ikke, at EU-retten ikke finder anvendelse"[2]; erindrer endvidere om, at det er beskyttelsen af alle EU-borgeres privatsfære, der er på spil, ligesom alle EU's kommunikationsnetværks sikkerhed og pålidelighed er det; mener derfor, at diskussioner og aktioner på EU-niveau ikke blot er legitime, men også er et emne, der handler om EU's autonomi og suverænitet;

15. påskønner de aktuelle diskussioner, undersøgelser og revisioner vedrørende emnet for

[1] Nr. 1 BvR 518/02 af 4. april 2006.
[2] Nr. 1 BvR 518/02 af 4. april 2006.

denne undersøgelse mange steder i verden; henviser til den globale regeringsovervågningsreform (Global Government Surveillance Reform), som verdens førende teknologivirksomheder støtter op om, og som opfordrer til radikale forandringer i de nationale overvågningslove, herunder et internationalt forbud mod masseindsamling af data, for at hjælpe med at bevare offentlighedens tillid til internettet; noterer med stor interesse de anbefalinger, der for nylig blev udsendt af den amerikanske præsidents undersøgelsesudvalg om efterretnings- og kommunikationsteknologi; opfordrer på det kraftigste regeringerne til at tage fuldt hensyn til disse opfordringer og anbefalinger og foretage en grundig gennemgang af deres nationale rammer for efterretningstjenester med henblik på at indføre passende garantier og tilsyn;

16. påskønner de institutioner og eksperter, som har bidraget til denne undersøgelse; finder det beklageligt, at flere medlemsstaters myndigheder har afslået at samarbejde med den undersøgelse, som Europa-Parlamentet har gennemført på borgernes vegne; glæder sig over åbenheden hos adskillige kongresmedlemmer og medlemmer af nationale parlamenter;

17. er klar over, at det inden for en begrænset tidsramme kun har været muligt at gennemføre en foreløbig undersøgelse af alle de centrale spørgsmål siden juli 2013; erkender både omfanget af de berørte afsløringer samt det forhold, at de er fortløbende af natur; vælger derfor en fremadrettet procedure bestående af en række specifikke forslag og en mekanisme med henblik på opfølgende aktioner i den næste valgperiode, så det sikres, at resultaterne stadig ligger højt oppe på EU's politiske dagsorden;

18. agter at kræve, at der fra Kommissionens side planlægges stærke politiske tiltag efter valgene i maj 2014, så forslagene og anbefalingerne fra denne undersøgelse kan blive gennemført; forventer et fuldt engagement heri fra kandidaterne under de kommende parlamentshøringer af de nye kommissærer;

***Henstillinger***

19. opfordrer de amerikanske myndigheder og EU's medlemsstater til at forbyde generelle masseovervågningsaktiviteter og massebehandling af personoplysninger;

20. opfordrer visse EU-medlemsstater, herunder Det Forenede Kongerige, Tyskland, Frankrig, Sverige og Nederlandene, til om nødvendigt at gennemgå deres nationale lovgivning og praksis vedrørende efterretningsaktiviteter for at sikre, at de stemmer overens med den europæiske menneskerettighedskonventions standarder og opfylder forpligtelserne i de grundlæggende rettigheder vedrørende databeskyttelse, privatlivets fred og uskyldsformodningen; fremhæver navnlig i lyset af de omfattende medierapporter, der omhandler masseovervågning i Det Forenede Kongerige, at den nuværende rammelovgivning, som består af et "komplekst samspil" mellem tre forskellige retsakter – menneskerettighedsloven af 1998 (Human Rights Act 1998), loven om efterretningstjenester af 1994 (Intelligence Services Act 1994) og loven om undersøgelsesbeføjelser af 2000 (Regulation of Investigatory Powers Act 2000) – bør revideres;

21. opfordrer medlemsstaterne til ikke at acceptere data fra tredjelande, som er indsamlet

ulovligt, eller tillade tredjelandes regeringer eller agenturer at foretage overvågningsaktiviteter på deres område, som er ulovlige i henhold til den nationale lovgivning, eller ikke opfylder retsgarantierne i internationale eller europæiske instrumenter, herunder beskyttelse af menneskerettighederne i henhold til traktaten om Den Europæiske Union (TEU), den europæiske menneskerettighedskonvention og EU's charter om grundlæggende rettigheder;

22. opfordrer medlemsstaterne til straks at opfylde deres positive forpligtelse i henhold til den europæiske menneskerettighedskonvention til at beskytte deres borgere mod overvågning, som strider mod kravene deri, herunder når målet dermed er at sikre den nationale sikkerhed, fra tredjelande og sikre, at retsstatsprincippet ikke svækkes som følge af ekstraterritorial anvendelse af et tredjelands lovgivning;

23. opfordrer Rådets generalsekretær til at indlede en artikel 52-procedure ifølge hvilken de høje kontraherende parter på anmodning fra Europarådets generalsekretær skal forklare, hvordan deres interne lovgivning sikrer en effektiv gennemførelse af konventionens bestemmelser;

24. opfordrer medlemsstaterne til straks at træffe passende foranstaltninger, herunder retslige foranstaltninger, over for brud på deres suverænitet og dermed overtrædelse af folkeretten generelt, som overtrædes via masseovervågningsprogrammer; opfordrer endvidere EU's medlemsstater til at bruge alle tilgængelige internationale foranstaltninger til at forsvare EU-borgeres grundlæggende rettigheder, navnlig ved at udløse den mellemstatslige klageprocedure i henhold til artikel 41 i den internationale konvention om borgerlige og politiske rettigheder;

25. opfordrer USA til straks at tage sin lovgivning op til revision for at bringe den i overensstemmelse med folkeretten, at anerkende EU-borgeres ret til privatlivets fred og andre rettigheder, at sikre EU-borgeres ret til domstolsprøvelse og undertegne tillægsprotokollen om borgernes klageret i henhold til den internationale konvention om borgerlige og politiske rettigheder;

26. er absolut modstander af indgåelsen af en tillægsprotokol eller retningslinjer til Europarådets konvention om it-kriminalitet (Budapestkonventionen) om grænseoverskridende adgang til opbevarede computerdata, som kan medføre legitimering af efterretningstjenesternes adgang til data, som opbevares i en anden jurisdiktion, uden dennes tilladelse og uden brug af eksisterende instrumenter til gensidig retshjælp, eftersom dette kan resultere i, at retshåndhævende myndigheder får uhindret fjernadgang til servere og computere i andre jurisdiktioner, og desuden ville være i strid med Europarådets konvention 108;

27. opfordrer Kommissionen til inden juli 2014 at gennemføre en vurdering af, hvorvidt forordning (EF) nr. 2271/96 finder anvendelse i lovvalgssager vedrørende overførsel af personoplysninger;

***International dataoverførsel***

*Amerikansk rammelovgivning om databeskyttelse og Safe Harbour*

28. bemærker, at virksomheder, som medierne har afsløret som deltagere i det amerikanske NSA's storstilede masseovervågning af registrerede i EU, er virksomheder, som på grundlag af selvcertificering har tilsluttet sig Safe Harbour, og at Safe Harbour er det retsinstrument, som anvendes ved overførsel af personoplysninger i EU til USA (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); udtrykker bekymring over, at disse organisationer har indrømmet, at de ikke krypterer oplysninger og kommunikation mellem deres datacentre og dermed gør det muligt for efterretningstjenester at indsamle oplysninger[1];

29. mener, at amerikanske efterretningstjenesters adgang til personoplysninger i EU, som behandles af Safe Harbour, ikke i sig selv opfylder kriteriet om undtagelse i henhold til "national sikkerhed";

30. mener, at Safe Harbour-principperne under de aktuelle omstændigheder ikke giver EU-borgere tilstrækkelig beskyttelse, og at disse overførsler derfor bør gennemføres i henhold til andre instrumenter som f.eks. kontraktbestemmelser eller bindende virksomhedsregler med specifikke beskyttelsesforanstaltninger;

31. opfordrer Kommissionen til at træffe foranstaltninger, der straks suspenderer Kommissionens beslutning 520/2000, som erklærede tilstrækkeligheden af Safe Harbour-principperne om privatlivets fred, og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium;

32. opfordrer medlemsstaternes kompetente myndigheder, det vil sige databeskyttelsesmyndighederne, til at gøre brug af deres eksisterende beføjelser og straks suspendere datastrømmene til alle organisationer, som på grundlag af selvcertificering har tilsluttet sig de amerikanske Safe Harbour-principper, og kræve, at sådanne datastrømme udelukkende gennemføres i henhold til andre instrumenter, forudsat at de indeholder de nødvendige beskyttelsesforanstaltninger med hensyn til beskyttelse af privatlivets fred og borgernes grundlæggende rettigheder og frihedsrettigheder;

33. opfordrer Kommissionen til senest i juni 2014 at fremlægge en fyldestgørende vurdering af den amerikanske rammelovgivning om privatlivets fred, der omfatter kommercielle aktiviteter samt retshåndhævelses- og efterretningsaktiviteter som svar på, at EU's og USA's retssystemer vedrørende beskyttelse af personoplysninger bevæger sig i hver sin retning;

*Overførsel til tredjelande med afgørelse om tilstrækkelighed*

34. minder om, at det i direktiv 95/46/EF fastlægges, at videregivelse af personoplysninger til tredjelande kun må finde sted, hvis det pågældende tredjeland, uden at dette berører overholdelsen af de nationale bestemmelser, som er vedtaget i

[1] Washington Post, 31. oktober 2013.

henhold til direktivets andre bestemmelser, sikrer et tilstrækkeligt beskyttelsesniveau, idet formålet med denne bestemmelse er at sikre, at EU's databeskyttelseslovgivning fortsat yder beskyttelse i forbindelse med personoplysninger, der videregives uden for EU;

35. minder om, at det i direktiv 95/46/EF fastlægges, at et tredjelands beskyttelsesniveau skal vurderes på grundlag af samtlige de forhold, der har indflydelse på en videregivelse eller en type videregivelse af oplysninger; minder ligeledes om, at samme direktiv giver Kommissionen gennemførelsesbeføjelser til at erklære, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau på grundlag af kriterierne i direktiv 95/46/EF; der henviser til, at direktiv 95/46/EF ligeledes giver Kommissionen beføjelser til at erklære, at et tredjeland ikke sikrer et tilstrækkeligt beskyttelsesniveau;

36. minder om, at medlemsstaterne i sidstnævnte tilfælde skal træffe de nødvendige foranstaltninger for at forebygge overførsel af data af samme type til det pågældende tredjeland, og at Kommissionen bør indlede forhandlinger med henblik på at afhjælpe situationen;

37. opfordrer Kommissionen og medlemsstaterne til straks at foretage en vurdering af, hvorvidt den tilstrækkelige beskyttelse i New Zealands og Canadas lovgivning om beskyttelse af personoplysninger og elektroniske dokumenter som erklæret i Kommissionens afgørelse 2013/651 og Kommissionens beslutning 2002/2 af 20. december 2001 er påvirket af, at landenes nationale efterretningstjenester har deltaget i masseovervågning af EU-borgere, og om nødvendigt træffe tilstrækkelige foranstaltninger til at suspendere eller omgøre beslutningerne om tilstrækkelighed; forventer, at Kommissionen senest i december 2014 aflægger rapport til Europa-Parlamentet om sine resultater om ovennævnte lande;

*Overførsel baseret på kontraktbestemmelser og andre instrumenter*

38. minder om, at nationale databeskyttelsesmyndigheder har angivet, at hverken standardkontraktbestemmelser eller bindende virksomhedsregler er udarbejdet med tanke på adgang til personoplysninger til masseovervågningsformål, og at en sådan adgang ikke ville stemme overens med undtagelsesklausulerne i kontraktbestemmelserne eller de bindende virksomhedsregler, som henviser til ekstraordinære undtagelser for en legitim interesse i et demokratisk samfund, samt hvor det er nødvendigt og forholdsmæssigt;

39. opfordrer medlemsstaterne til at forbyde eller suspendere datastrømme til tredjelande baseret på standardkontraktbestemmelser, kontraktbestemmelser eller bindende virksomhedsregler, som er godkendt af de nationale kompetente myndigheder, hvor det fastslås, at den lovgivning, som dataimportøren er underlagt, pålægger denne krav, som rækker videre end de restriktioner, som er nødvendige i et demokratisk samfund, og som sandsynligvis kan have en betydelig negativ indvirkning på garantierne i henhold til den gældende databeskyttelseslovgivning og standardkontraktbestemmelserne, eller fordi der ved fortsat overførsel er en overhængende risiko for på betydelig vis at skade de registrerede;

[1] EUT L 28 af 30.1.2013, s. 12.

40. opfordrer Artikel 29-Gruppen til at udstede retningslinjer og henstillinger om de beskyttelsesforanstaltninger, som kontraktinstrumenter vedrørende internationale overførsler af EU-personoplysninger bør indeholde for at sikre beskyttelse af privatlivets fred og borgernes grundlæggende rettigheder og frihedsrettigheder, navnlig under hensyntagen til tredjelandes lovgivning om efterretning og national sikkerhed, og om de virksomheder, som modtager dataene i et tredjeland, deltager i et tredjelands efterretningstjenesters masseovervågningsaktiviteter;

41. opfordrer Kommissionen til at undersøge de standardkontraktbestemmelser, den har fastsat, med henblik på at vurdere, om de yder den nødvendige beskyttelse med hensyn til adgang til personoplysninger, som overføres i henhold til efterretningsbestemmelserne og, hvor det er relevant, gennemgå disse;

*Overførsler på grundlag af aftalen om gensidig retshjælp*

42. opfordrer Kommissionen til inden udgangen af 2014 at foretage en dybdegående vurdering af den eksisterende aftale om gensidig retshjælp i henhold til artikel 17 deri for at kontrollere, om den er gennemført i praksis, og navnlig om USA har anvendt den effektivt til at tilegne sig oplysninger eller dokumentation i EU, og om aftalen er omgået med henblik på at fremskaffe oplysningerne direkte i EU og vurdere indvirkningen på borgernes grundlæggende rettigheder; en sådan vurdering bør ikke kun vedrøre officielle amerikanske udtalelser som et tilstrækkeligt grundlag for analysen, men bør baseres på specifikke EU-evalueringer; denne dybdegående vurdering bør også omhandle konsekvenserne af at anvende Unionens forfatningsarkitektur på dette instrument for at bringe det i overensstemmelse med EU-retten under hensyntagen til navnlig protokol nr. 36 og artikel 10 deri samt erklæring nr. 50 om denne protokol;

*Gensidig retshjælp i EU i straffesager*

43. anmoder Kommissionen om at underrette Parlamentet om medlemsstaternes faktiske brug af konventionen om gensidig retshjælp i straffesager mellem medlemsstaterne, navnlig afsnit III om aflytning af telekommunikation; opfordrer Kommissionen til som ønsket at fremsætte et forslag i overensstemmelse med erklæring nr. 50 om protokol nr. 36 inden udgangen af 2014 med henblik på at tilpasse den til rammerne i Lissabontraktaten;

*Overførsler baseret på TFTP- og PNR-aftaler*

44. mener, at oplysningerne fra Kommissionen og det amerikanske finansministerium ikke præciserer, om amerikanske efterretningstjenester har adgang til finansielle SWIFT-meddelelser i EU ved at aflytte SWIFT-net eller bankers driftssystemer eller kommunikationsnet, alene eller i samarbejde med EU's nationale efterretningstjenester og uden at anvende eksisterende bilaterale kanaler til gensidig retshjælp og retligt samarbejde;

45. gentager sin beslutning af 23. oktober 2013 og anmoder Kommissionen om at suspendere TFTP-aftalen;

46. opfordrer Kommissionen til at reagere på bekymringerne om, at tre af de store computerreservationssystemer, som anvendes af luftfartsselskaber i hele verden, er placeret i USA, og at PNR-data gemmes i cloud-systemer, der befinder sig på amerikansk jord i henhold til amerikansk lovgivning, som ikke giver tilstrækkelig databeskyttelse;

*Rammeaftale om databeskyttelse inden for politisamarbejde og retligt samarbejde ("paraplyaftale")*

47. mener, at en tilfredsstillende løsning i henhold til "paraplyaftalen" er en forudsætning for at genoprette tilliden mellem de transatlantiske partnere fuldt ud;

48. anmoder om, at forhandlingerne med USA om "paraplyaftalen" straks genoptages, idet den bør indeholde klare rettigheder for EU-borgere og effektive administrative og retlige klagemuligheder, som kan håndhæves i USA uden forskelsbehandling;

49. anmoder Kommissionen og Rådet om ikke at indlede nogen nye sektoraftaler eller -ordninger om overførsel af personoplysninger til retshåndhævelsesformål, før "paraplyaftalen" er trådt i kraft;

50. opfordrer indtrængende Kommissionen til at give detaljerede oplysninger om de forskellige punkter i forhandlingsmandatet og den seneste status inden april 2014;

*Databeskyttelsesreform*

51. opfordrer Rådets formandskab og flertallet af medlemsstaterne, som støtter et højt niveau af databeskyttelse, til at udvise lederskab og ansvar og fremskynde deres arbejde med hele databeskyttelsespakken, så den kan vedtages i 2014, og så EU's borgere inden for den nærmeste fremtid er bedre beskyttet;

52. understreger, at både databeskyttelsesforordningen og databeskyttelsesdirektivet er nødvendige for at beskytte borgernes grundlæggende rettigheder, og at de derfor skal behandles som en pakke, som skal vedtages samtidig, for at sikre, at der for alle databehandlingsaktiviteter i EU under alle omstændigheder sikres et højt beskyttelsesniveau;

*Cloud computing*

53. bemærker, at tilliden til amerikansk cloud computing og udbydere af cloud-tjenester er påvirket negativt af ovennævnte praksis; understreger derfor, at udviklingen af europæiske cloud-tjenester er et vigtigt led i væksten og beskæftigelsen og tilliden til cloud computing-tjenester og -udbydere og med hensyn til at sikre et højt niveau af beskyttelse af personoplysninger;

54. gentager sin alvorlige bekymring over den obligatoriske direkte videregivelse til tredjelandsmyndigheder af EU-personoplysninger og oplysninger, der behandles som en del af cloud-aftaler, som er pålagt cloud-udbydere, der er underlagt lovgivning i tredjelande eller anvender servere, der er placeret i tredjelande, til opbevaring, og om direkte fjernadgang til personoplysninger og oplysninger, der behandles af

tredjelandes retshåndhævende myndigheder og efterretningstjenester;

55. beklager, at denne adgang sædvanligvis opnås ved tredjelandsmyndighedernes direkte håndhævelse af deres egen lovgivning uden at gøre brug af de internationale instrumenter, der er blevet oprettet vedrørende retligt samarbejde, såsom aftaler om gensidig retshjælp eller andre former for retligt samarbejde;

56. opfordrer Kommissionen og medlemsstaterne til at fremskynde arbejdet med at oprette et europæisk cloud-partnerskab;

57. minder om, at alle virksomheder, der leverer tjenesteydelser i EU, skal overholde EU-retten uden undtagelser og er ansvarlige for eventuelle overtrædelser;

*Den transatlantiske handels- og investeringspartnerskabsaftale*

58. anerkender, at EU og USA forhandler om et transatlantisk handels- og investeringspartnerskab, som er af stor strategisk betydning i forhold til at skabe yderligere økonomisk vækst, og for at både EU og USA kan sætte en fremtidig global lovgivningsstandard;

59. understreger på det kraftigste i lyset af den digitale økonomis betydning for forholdet og årsagen til at genopbygge tilliden mellem EU og USA, at Europa-Parlamentet kun vil godkende den endelige aftale om et transatlantisk handels- og investeringspartnerskab, hvis aftalen fuldt ud overholder de grundlæggende rettigheder i EU's charter, og at beskyttelse af borgernes privatliv i forbindelse med behandling og formidling af personoplysninger fortsat skal være underlagt artikel XIV i GATS;

***Demokratisk tilsyn med efterretningstjenester***

60. understreger, at flertallet af de nuværende tilsynsorganer i EU og USA, til trods for, at tilsynet med efterretningstjenesternes aktiviteter bør baseres på såvel demokratisk legitimitet (stærk rammelovgivning, forudgående tilladelse og efterfølgende kontrol) og tilstrækkelige teknisk evner og ekspertise, i dramatisk grad mangler begge dele, navnlig tekniske evner;

61. opfordrer som i Echelons tilfælde alle nationale parlamenter, som endnu ikke har gjort dette, til at indføre meningsfuldt tilsyn med efterretningsaktiviteter fra parlamentarikere eller ekspertorganer med retlige undersøgelsesbeføjelser; opfordrer de nationale parlamenter til at sikre, at sådanne tilsynsudvalg/-organer har tilstrækkelige ressourcer, teknisk ekspertise og retlige midler til at kunne kontrollere efterretningstjenesterne;

62. opfordrer til, at der oprettes en gruppe på højt plan til at styrke efterretningssamarbejdet på EU-plan kombineret med en reel tilsynsmekanisme, der sikrer både demokratisk legitimitet og tilstrækkelig teknisk kapacitet; understreger, at gruppen på højt plan bør samarbejde tæt med de nationale parlamenter om at foreslå yderligere skridt i retning af øget tilsynssamarbejde i EU;

63. opfordrer denne gruppe på højt plan til at definere bindende minimumsstandarder på

europæisk plan eller retningslinjer for (forudgående og efterfølgende) tilsyn med efterretningstjenester på grundlag af eksisterende bedste praksis og henstillinger fra internationale organer (FN, Europarådet osv.);

64. opfordrer gruppen på højt plan til at fastsætte strenge grænser for varigheden af enhver pålagt overvågning, medmindre en fortsættelse deraf begrundes behørigt af godkendelses-/tilsynsmyndigheden;

65. opfordrer gruppen på højt plan til at udarbejde kriterier for øget gennemsigtighed, som bygger på det generelle princip om adgang til information og de såkaldte "Tshwane-principper".[1];

66. har til hensigt at arrangere en konference med nationale tilsynsorganer, både parlamentariske og uafhængige, inden udgangen af 2014;

67. opfordrer medlemsstaterne til at udnytte bedste praksis til at give deres tilsynsorganer bedre adgang til oplysninger om efterretningsaktiviteter (herunder fortrolige oplysninger og oplysninger fra andre tjenester) og fastsætte beføjelserne til at gennemføre besøg på stedet, en række solide forhørsbeføjelser, passende ressourcer og tilstrækkelig teknisk ekspertise, streng uafhængighed af deres respektive regeringer og en rapporteringspligt til deres respektive parlamenter;

68. opfordrer medlemsstaterne til at udvikle samarbejdet mellem tilsynsorganerne, navnlig inden for European Network of National Intelligence Reviewers (ENNIR);

69. opfordrer indtrængende Kommissionen til inden september 2014 at fremsætte et forslag til et retsgrundlag for aktiviteterne i EU's efterretningsanalysecenter (IntCen) samt en reel tilsynsmekanisme, som er tilpasset dets aktiviteter, herunder regelmæssig rapportering til Europa-Parlamentet;

70. opfordrer Kommissionen til inden september 2014 at fremsætte et forslag til en sikkerhedsundersøgelsesprocedure i EU for alle, der beklæder offentlige hverv i EU, eftersom det nuværende system, som anvender de sikkerhedsundersøgelser, der benyttes i statsborgernes medlemsstater, indeholder forskellige krav og procedurer af forskellig længde i de nationale systemer, og parlamentsmedlemmerne og deres personale behandles således forskelligt, afhængig af deres nationalitet;

71. minder om bestemmelserne i den interinstitutionelle aftale mellem Europa-Parlamentet og Rådet om fremsendelse til Europa-Parlamentet og dettes behandling af Rådets klassificerede informationer på andre områder end dem, der er omfattet af den fælles udenrigs- og sikkerhedspolitik, som har til formål at forbedre tilsynet på EU-plan;

***EU-agenturer***

72. opfordrer Europols fælles kontrolinstans til sammen med de nationale databeskyttelsesmyndigheder at foretage en fælles kontrol inden udgangen af 2014 for

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

at finde ud af, om data og personoplysninger, der deles med Europol, er indhentet på lovlig vis af de nationale myndigheder, navnlig hvis oplysningerne eller dataene indledningsvist blev indhentet af efterretningstjenester i EU eller et tredjeland, og om der er indført tilstrækkelige foranstaltninger til at forebygge anvendelse og videreformidling af sådanne oplysninger eller data;

73. opfordrer Europol til at anmode medlemsstaternes kompetente myndigheder om i overensstemmelse med deres kompetencer at indlede en efterforskning med hensyn til eventuel cyberkriminalitet og cyberangreb begået af regeringer eller private aktører i forbindelse med de undersøgte aktiviteter;

***Ytringsfrihed***

74. udtrykker dyb bekymring om udviklingen af trusler mod pressefriheden og den afdæmpende virkning, som statslige myndigheders intimidering har på journalister, navnlig med hensyn til beskyttelse af fortrolige journalistiske kilder; gentager sine opfordringer i sin beslutning af 21. maj 2013 om "EU-chartret: Standarder for mediefrihed i EU";

75. mener, at tilbageholdelsen af Miranda og beslaglæggelsen af hans materiale i henhold til bilag 7 i terrorloven af 2000 (Terrorism Act 2000) (og anmodningen til *The Guardian* om at ødelægge eller aflevere materialet) udgør en overtrædelse af ytringsfriheden i henhold til artikel 10 i den europæiske menneskerettighedskonvention og artikel 11 i EU's charter;

76. opfordrer Kommissionen til at fremsætte et forslag til en omfattende ramme for beskyttelse af whistleblowere i EU, hvori der navnlig tages hensyn til de særlige forhold i forbindelse med whistleblowing inden for efterretning, hvor bestemmelserne om whistleblowing i finansverdenen kan være utilstrækkelige, og hvori der gives en stærk garanti for immunitet;

***EU's it-sikkerhed***

77. påpeger, at nylige hændelser med al tydelighed viser den akutte sårbarhed i EU og navnlig i EU's institutioner, nationale regeringer og parlamenter, store europæiske virksomheder, europæisk it-infrastruktur og -net over for sofistikerede angreb med avanceret software; bemærker, at disse angreb kræver finansielle og menneskelige ressourcer, som sandsynligvis stammer fra statslige virksomheder, der handler på vegne af udenlandske regeringer eller endda fra visse nationale EU-regeringer, der støtter dem; ser i denne forbindelse hackingen eller aflytningen af telekommunikationsselskabet Belgacom som et bekymrende eksempel på et angreb mod EU's it-kapacitet;

78. mener, at EU kan benytte de afsløringer af masseovervågning, som har indledt denne krise, som en mulighed for at tage initiativ til og opbygge en selvstændig og vigtig it-ressourcekapacitet på mellemlangt sigt; opfordrer Kommissionen og medlemsstaterne til at anvende offentlige indkøb som løftestang i forhold til at støtte denne ressourcekapacitet i EU ved at gøre EU's standarder for sikkerhed og privatlivets fred til et vigtigt krav i forbindelse med offentlige indkøb af it-varer og -tjenester;

79. er dybt bekymret over indikationerne på, at udenlandske efterretningstjenester har forsøgt at sænke it-sikkerhedsstandarder og installere bagdøre i en lang række it-systemer;

80. opfordrer medlemsstaterne, Kommissionen, Rådet og Det Europæiske Råd til at se på EU's farlige mangel på selvstændighed med hensyn til it-værktøjer, -virksomheder og -udbydere (hardware, software, tjenester og net) samt kryptering og kryptografisk kapacitet;

81. opfordrer Kommissionen, standardiseringsorganer og ENISA til senest i september 2014 at udvikle minimumsstandarder og -retningslinjer for sikkerhed og privatlivets fred til it-systemer, -net og -tjenester, herunder cloud computing-tjenester, for bedre at beskytte EU-borgernes personoplysninger; mener, at sådanne standarder bør fastlægges i en åben og demokratisk proces og ikke drives af et enkelt land, en enkelt enhed eller et enkelt multinationalt selskab; mener, at selv om der i forbindelse med bekæmpelse af terrorisme skal tages højde for reelle retshåndhævelses- og efterretningsbekymringer, bør de ikke medføre en generel undergravning af afhængigheden af alle it-systemer;

82. påpeger, at såvel telekommunikationsvirksomheder og EU og nationale tilsynsmyndigheder på telekommunikationsområdet tydeligvis har forsømt deres brugeres og kunders it-sikkerhed; opfordrer Kommissionen til at bruge sine eksisterende beføjelser i henhold til rammedirektivet om e-databeskyttelse og telekommunikation til at øge beskyttelsen af fortrolig kommunikation ved at vedtage foranstaltninger, der sikrer, at terminaludstyr er foreneligt med brugernes ret til at kontrollere og beskytte deres personoplysninger, og sikre et højt sikkerhedsniveau i telekommunikationsnet og -tjenester, herunder ved at kræve den mest avancerede kryptering af kommunikation;

83. støtter EU's cyberstrategi, men mener, at den ikke omfatter alle mulige trusler og bør udvides til at omfatte ondsindet statslig adfærd;

84. opfordrer Kommissionen til senest i januar 2015 at fremlægge en handlingsplan for udvikling af mere EU-uafhængighed i it-sektoren, herunder en mere sammenhængende tilgang til at fremme europæisk it-teknologisk kapacitet (herunder it-systemer, udstyr, tjenester, cloud computing, kryptering og anonymisering) og til at beskytte vigtig it-infrastruktur (også med hensyn til ejerskab og sårbarhed);

85. opfordrer Kommissionen til inden for rammerne af det næste arbejdsprogram i Horisont 2020-programmet at vurdere, om der bør afsættes flere ressourcer til at fremme europæisk forskning, udvikling, innovation og uddannelse inden for it-teknologi, navnlig teknologier og infrastrukturer, der fremmer privatlivets fred, kryptering, sikre computerløsninger, open source-sikkerhedsløsninger og informationssamfundet;

86. anmoder Kommissionen om at kortlægge eksisterende ansvarsområder og senest i juni 2014 at gennemgå behovet for et bredere mandat, bedre koordinering og/eller yderligere ressourcer og teknisk kapacitet til Europols center for bekæmpelse af cyberkriminalitet, ENISA, CERT-EU og EDPS for at gøre dem mere effektive i

forhold til at undersøge store brud på it-sikkerheden i EU og gennemføre (eller hjælpe medlemsstaterne og EU's organer med at gennemføre) tekniske undersøgelser på stedet i forbindelse med store brud på it-sikkerheden;

87. mener, at det er nødvendigt, at EU støttes af et it-akademi, der samler de bedste europæiske eksperter på alle relevante områder, og som har til opgave at yde videnskabelig rådgivning til alle relevante EU-institutioner og -organer om it-teknologi, herunder sikkerhedsrelaterede strategier; anmoder indledningsvist Kommissionen om at nedsætte et uafhængigt videnskabeligt ekspertpanel;

88. opfordrer Europa-Parlamentets sekretariat til senest i september 2014 at gennemføre en grundig gennemgang og vurdering af Europa-Parlamentets it-sikkerheds afhængighed med fokus på: budgetmidler, personaleressourcer, teknisk kapacitet, intern organisation og alle relevante elementer for at kunne opnå et højt sikkerhedsniveau for Europa-Parlamentets it-systemer; mener, at en sådan vurdering som minimum bør kunne omfatte en analyse af oplysninger og henstillinger vedrørende:

- behovet for regelmæssige, strenge og uafhængige sikkerhedsaudit og udbredelsestest med en udvælgelse af udefrakommende sikkerhedseksperter, der sikrer gennemsigtighed og garanterer deres referencer i forhold til tredjelande og enhver form for særlige interesser;

- inddragelse i udbudsprocedurer for nye it-systemer af specifikke krav vedrørende it-sikkerhed/privatlivets fred, herunder eventuelt et krav om open source-software som betingelse for et køb;

- listen over amerikanske virksomheder, som har indgået en aftale med Europa-Parlamentet inden for it og telekommunikation, under hensyntagen til afsløringerne om NSA's aftaler med en virksomhed som RSA, hvis produkter Europa-Parlamentet angiveligt anvender til at beskytte medlemmernes og personalets fjernadgang til data;

- pålidelighed og resiliens af kommerciel tredjepartssoftware, som EU's institutioner anvender i deres it-systemer med hensyn til EU's eller tredjelandes retshåndhævelses- og efterretningsmyndigheders udbredelse og indtrængen;

- anvendelse af flere open source-systemer og færre kommercielle standardsystemer;

- virkningen af den øgede brug af mobile værktøjer (smartphones og tablets, både professionelle og personlige) og indvirkningen på systemets it-sikkerhed;

- sikkerheden i kommunikationen mellem forskellige arbejdspladser i Europa-Parlamentet og de it-systemer, som anvendes i Europa-Parlamentet;

- brug og placering af servere og it-centre til Europa-Parlamentets it-systemer og betydningen for systemernes sikkerhed og integritet;

- den reelle gennemførelse af de eksisterende regler om sikkerhedsbrud og omgående underretning af de kompetente myndigheder fra udbyderne af offentligt tilgængelige telekommunikationsnet;

- Europa-Parlamentets brug af cloud-opbevaring, herunder hvilken type data der opbevares, hvordan indholdet og adgangen beskyttes, og hvor cloud-ordningen er placeret for at præcisere de gældende juridiske databeskyttelsesregler;

- en plan, der giver mulighed for at anvende mere kryptografiske teknologier, navnlig autentificeret kryptering fra endepunkt til endepunkt for alle it- og kommunikationstjenester som cloud computing, e-mail, instant messaging og telefoni;

- brug af elektroniske signaturer i e-mail;

- en analyse af fordelene ved at anvende den såkaldte GNU Privacy Guard som standardkrypteringsstandard for e-mail, som samtidig vil muliggøre brug af digitale signaturer;

- muligheden for at oprette en sikker instant messaging-tjeneste i Europa-Parlamentet, der tillader sikker kommunikation, hvor servere kun ser krypteret indhold;

89. opfordrer EU's institutioner og agenturer, navnlig Det Europæiske Råd, Rådet, EU-Udenrigstjenesten (herunder EU's delegationer), Kommissionen, Domstolen og Den Europæiske Centralbank, til senest i december 2014 at foretage en lignende øvelse; opfordrer medlemsstaterne til at foretage tilsvarende vurderinger;

90. understreger, at der med hensyn til EU's optræden udadtil straks bør foretages vurderinger af relevante budgetbehov, og at der straks bør træffes de første foranstaltninger vedrørende EU-Udenrigstjenesten, og at der skal tildeles tilstrækkelige midler i forslaget til budget for 2015;

91. mener, at de store it-systemer, som anvendes inden for frihed, sikkerhed og retfærdighed, som f.eks. Schengeninformationssystem II, Visainformationssystemet, Eurodac og eventuelle kommende systemer, bør udvikles og styres på en måde, der sikrer, at dataene ikke misbruges som følge af en amerikansk forespørgsel i henhold til Patriot Act; anmoder eu-LISA om inden udgangen af 2014 at underrette Europa-Parlamentet om pålideligheden af de indførte systemer;

92. opfordrer Kommissionen og EEAS til at træffe foranstaltninger på internationalt plan, navnlig sammen med FN, og i samarbejde med interesserede parter (som f.eks. Brasilien) og gennemføre en EU-strategi for demokratisk forvaltning af internettet for at forhindre ubehørig påvirkning af ICANN's og IANA's aktiviteter fra en enkelt enhed, en enkelt virksomhed eller et enkelt land ved at sikre, at alle interesserede parter er passende repræsenteret i disse organer;

93. opfordrer til at tage internettets overordnede arkitektur med hensyn til datastrømme og -opbevaring op til fornyet overvejelse og tilstræbe mere dataminimering og

gennemsigtighed og mindre central masseopbevaring af rådata samt undgå unødvendig dirigering af trafik gennem lande, som ikke opfylder de grundlæggende standarder for grundlæggende rettigheder, databeskyttelse og privatlivets fred;

94. opfordrer medlemsstaterne til i samarbejde med ENISA, Europols center for bekæmpelse af cyberkriminalitet, it-beredskabsenheder og nationale databeskyttelsesmyndigheder og enheder for cyberkriminalitet til at indlede en uddannelses- og oplysningskampagne for at give borgerne mulighed for at foretage et mere oplyst valg om, hvilke personoplysninger, der skal gives online, og hvordan de bedst beskyttes, herunder gennem "digital hygiejne", kryptering og sikker cloud computing, med fuld udnyttelse af platformen for almennyttige oplysninger som omhandlet i forsyningspligtdirektivet;

95. opfordrer Kommissionen til senest i september 2014 at vurdere mulighederne for at opfordre software- og hardwareproducenter til at indføre mere sikkerhed og privatliv ved hjælp af standardfunktioner i deres produkter, herunder muligheden for at indføre retligt ansvar for producenter for ikkereparerede kendte sårbarheder eller installation af hemmelige bagdøre, og hindringer for ubehørig og uforholdsmæssig indsamling af personlige masseoplysninger og om nødvendigt fremsætte lovforslag;

***Genopbygning af tillid***

96. mener, at undersøgelsen har vist, at USA skal genoprette tilliden hos sine partnere, eftersom det primært er amerikanske efterretningstjenesters aktiviteter, som er på spil;

97. påpeger, at tillidskrisen omfatter:

- samarbejdsånden inden for EU, eftersom nogle nationale efterretningsaktiviteter kan hæmme opnåelsen af Unionens mål;

- borgere, som erkender, at det ikke kun er tredjelande eller multinationale selskaber, men også deres egen regering, som kan udspionere dem;

- overholdelse af retsstatsprincippet og troværdigheden af demokratiske beskyttelsesforanstaltninger i et digitalt samfund;

*Mellem EU og USA*

98. minder om det vigtige historiske og strategiske partnerskab mellem EU's medlemsstater og USA baseret på en fælles tro på demokratiet, retsstatsprincippet og grundlæggende rettigheder;

99. mener, at USA's masseovervågning af borgere og udspionering af politiske ledere i høj grad har været til skade for forholdet mellem EU og USA og haft en negativ indvirkning på tilliden til amerikanske organisationer med aktiviteter i EU; dette forværres ydermere af manglen på retlige og administrative klagemidler i den amerikanske lovgivning for EU's borgere, navnlig i forbindelse med overvågningsaktiviteter til efterforskningsformål;

100. anerkender i lyset af de globale udfordringer, som EU og USA står over for, at det transatlantiske partnerskab skal styrkes yderligere, og at det er vigtigt, at det transatlantiske samarbejde om at bekæmpe terrorisme fortsætter; fastholder imidlertid, at USA skal træffe klare foranstaltninger for at genoprette tilliden, og understreger de fælles grundlæggende værdier, der ligger til grund for partnerskabet;

101. er klar til at indlede en aktiv dialog med amerikanske modparter, så EU-borgeres rettigheder vedrørende privatlivets fred inddrages i den løbende amerikanske offentlige debat og drøftelserne i Kongressen om en reform af overvågningen og en gennemgang af tilsynet med efterretningstjenesterne, og at retten til lige information og beskyttelse af privatlivets fred garanteres i de amerikanske domstole, og den nuværende forskelsbehandling ikke fastholdes;

102. fastholder, at der skal gennemføres de nødvendige reformer, og at EU-borgere skal gives reelle garantier for at sikre, at brug af overvågning og databehandling til udenlandske efterretningsformål begrænses af tydeligt fastlagte betingelser og knyttes til en rimelig mistanke om eller en sandsynlig årsag til terrorisme eller kriminelle handlinger; understreger, at dette formål skal være underlagt et gennemsigtigt retligt tilsyn;

103. mener, at der er behov for tydelige politiske signaler fra vores amerikanske partnere for at vise, at USA skelner mellem venner og fjender;

104. opfordrer Kommissionen og den amerikanske regering til i forbindelse med de løbende forhandlinger om en paraplyaftale mellem EU og USA om dataoverførsel til retshåndhævelsesformål at inddrage EU-borgeres ret til oplysninger og domstolsprøvelse og afslutte disse forhandlinger inden sommeren 2014 i overensstemmelse med løftet på mødet mellem EU og USA om retlige og indre anliggender den 18. november 2013;

105. opfordrer USA til at tiltræde Europarådets konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (konvention 108), ligesom det tiltrådte konventionen fra 2001 om it-kriminalitet, og dermed styrke det fælles retsgrundlag blandt transatlantiske allierede;

106. opfordrer EU's institutioner til at undersøge mulighederne for at fastlægge en adfærdskodeks sammen med USA, som kan garantere, at USA ikke udøver spionage mod EU's institutioner og faciliteter;

*I Den Europæiske Union*

107. mener endvidere, at EU's medlemsstaters deltagelse og aktiviteter har medført tab af tillid; mener, at kun fuld klarhed over formålet med og midlerne til overvågning, offentlig debat og endelig en revision af lovgivningen, herunder en styrkelse af det retlige og parlamentariske tilsynssystem kan genoprette den mistede tillid;

108. er klar over, at visse EU-medlemsstater kommunikerer bilateralt med de amerikanske myndigheder om beskyldninger om spionage, og at nogle af disse har indgået (Det Forenede Kongerige) eller regner med at indgå (Tyskland, Frankrig) såkaldte

antispionageaftaler; understreger, at disse medlemsstater skal tage fuld højde for EU's interesser som helhed;

109. mener, at sådanne aftaler ikke må være i strid med EU-traktaterne, navnlig princippet om loyalt samarbejde (i henhold til artikel 4, stk. 3, i TEU), eller undergrave EU's politikker generelt og mere specifikt det indre marked, loyal konkurrence og økonomisk, industriel og social udvikling; forbeholder sig ret til at indlede traktatprocedurer, såfremt sådanne aftaler viser sig at være i strid med Unionens samhørighed eller de grundlæggende principper, den er baseret på;

*På internationalt plan*

110. opfordrer Kommissionen til senest i januar 2015 at fremlægge en EU-strategi for demokratisk forvaltning af internettet;

111. opfordrer medlemsstaterne til at følge opfordringen fra den 35. internationale konference for kommissærer for databeskyttelse og privatlivets fred til at fremme vedtagelsen af en tillægsprotokol til artikel 17 i den internationale konvention om borgerlige og politiske rettigheder, som bør baseres på de standarder, som den internationale konference har udarbejdet og godkendt, og bestemmelserne i den generelle bemærkning nr. 16 til konventionen for at skabe globalt gældende standarder for databeskyttelse og beskyttelse af privatlivets fred i overensstemmelse med retsstatsprincippet; anmoder den højtstående repræsentant/Kommissionens næstformand og EU-Udenrigstjenesten om at være proaktive i deres tilgang;

112. opfordrer medlemsstaterne til at udarbejde en sammenhængende og stærk strategi i FN og navnlig støtte beslutningen om retten til privatlivets fred i en digital tidsalder, som blev indledt af Brasilien og Tyskland og vedtaget af det tredje udvalg i FN's Generalforsamling (menneskerettighedsudvalget) den 27. november 2013;

***Prioritetsplan: Et europæisk digitalt habeas corpus***

113. beslutter at sende ovennævnte henstillinger til EU-borgere, institutioner og medlemsstater som en prioritetsplan for næste valgperiode;

114. beslutter at lancere et europæisk digitalt habeas corpus til beskyttelse af privatlivets fred baseret på følgende syv foranstaltninger med et kontrolorgan i Europa-Parlamentet:

Foranstaltning 1: vedtage databeskyttelsesreformpakken i 2014;

Foranstaltning 2: indgå paraplyaftalen mellem EU og USA, som skal sikre reelle mekanismer for domstolsprøvelse for EU-borgere i forbindelse med dataoverførsler fra EU til USA til retshåndhævelsesformål;

Foranstaltning 3: suspendere Safe Harbour-ordningen, indtil der er foretaget en fuldstændig gennemgang, og de nuværende smuthuller er lukket, så det sikres, at overførsel af personoplysninger til kommercielle formål fra Unionen til USA kun kan finde sted i overensstemmelse med de højeste EU-standarder;

Foranstaltning 4: suspendere TFTP-aftalen, indtil i) forhandlingerne om paraplyaftalen er afsluttet; ii) der er foretaget en grundig undersøgelse på grundlag af en EU-analyse, og der reelt er taget hånd om alle Parlamentets bekymringer i beslutningen af 23. oktober;

Foranstaltning 5: beskytte retsstatsprincippet og EU-borgeres grundlæggende rettigheder, navnlig med fokus på truslen mod pressefrihed og tavshedspligt (herunder i advokat-klient-forhold) samt bedre beskyttelse af whistleblowere;

Foranstaltning 6: udarbejde en europæisk strategi for it-uafhængighed (på nationalt plan og EU-plan);

Foranstaltning 7: udvikle EU som reference for demokratisk og neutral forvaltning af internettet;

115. opfordrer EU-institutionerne og medlemsstaterne til at støtte og fremme det europæiske digitale habeas corpus; påtager sig at fungere som kontrolorgan for EU-borgernes rettigheder med følgende tidsplan for overvågning af gennemførelsen;

- April til juli 2014: en overvågningsgruppe baseret på LIBE-undersøgelsesgruppen med ansvar for at overvåge nye afsløringer i medierne om undersøgelsens mandat og undersøgelse af gennemførelsen af denne beslutning;

- Fra juli 2014: en stående tilsynsmekanisme for dataoverførsel og domstolsprøvelse i det kompetente udvalg;

- Foråret 2014: en formel opfordring til Det Europæiske Råd om at indarbejde det europæiske digitale habeas corpus i de retningslinjer, som skal vedtages i henhold til artikel 68 i TEUF;

- Efteråret 2014: et løfte om, at det europæiske digitale habeas corpus og dermed forbundne henstillinger skal tjene som de vigtigste kriterier for godkendelsen af den næste Kommission;

- 2014-2015: en tillids-/data-/borgerrettighedsgruppe, som skal mødes løbende, mellem Europa-Parlamentet og den amerikanske Kongres samt med andre engagerede tredjelandsparlamenter, herunder Brasilien;

- 2014-2015: en konference med de europæiske nationale parlamenters efterretningstilsynsorganer;

- 2015: en konference, der samler europæiske eksperter på højt plan inden for de forskellige områder vedrørende it-sikkerhed (herunder matematik, kryptografi og teknologier til forbedring af privatlivets fred) for at hjælpe med at fremme en it-strategi i EU for næste valgperiode;

116. pålægger sin formand at sende denne beslutning til Det Europæiske Råd, Rådet, Kommissionen, medlemsstaternes parlamenter og regeringer, nationale databeskyttelsesmyndigheder, EDPS, eu-LISA, ENISA, Agenturet for Grundlæggende

Rettigheder, Artikel 29-Gruppen, Europarådet, USA's Kongres, USA's regering, præsidenten, regeringen og parlamentet i Den Føderative Republik Brasilien og De Forenede Nationers generalsekretær.

## BEGRUNDELSE

*"Herskerens opgave består, uanset om det er en monark eller en forsamling, i at opfylde det formål til hvilket denne fik tildelt sine beføjelser, nemlig at sørge for folkets sikkerhed"*
*Hobbes, Leviathan (kapital XXX)*

*"Vi kan ikke rose vort samfund over for andre ved at afvige fra de grundlæggende standarder, som gør det værd at rose"*
*Lord Bingham of Cornhill,*
*Tidligere retspræsident (Lord Chief Justice) i England og Wales*

### Metode

I juli 2013 fik LIBE-udvalget ansvaret for den ekstremt ufordrende opgave med at udfylde plenarforsamlingens mandat[1] til at undersøge elektronisk masseovervågning af EU-borgere inden for en meget kort tidshorisont på mindre end seks måneder.

I denne periode holdt udvalget over 15 høringer om hver af de specifikke grupper af spørgsmål, som er omhandlet i beslutningen af 4. juli, godt hjulpet af indlæg fra både europæiske og amerikanske eksperter med vidt forskellig viden og baggrund: EU-institutioner, nationale parlamenter, Kongressen, akademikere, journalister, civilsamfundet, sikkerheds- og teknologieksperter og det private erhvervsliv. Derudover besøgte en delegation fra LIBE-udvalget Washington den 28.-30. oktober 2013 for at mødes med repræsentanter fra såvel den udøvende som den lovgivende magt (akademikere, sikkerhedseksperter, repræsentanter fra erhvervslivet)[2]. En delegation fra Udenrigsudvalget (AFET) var ligeledes i byen på samme tidspunkt. Et par møder blev holdt samlet.

Ordføreren, skyggeordførerne[3] fra de forskellige politiske grupper og tre medlemmer fra AFET-udvalget[4] har været medforfattere på en række arbejdsdokumenter[5], så det har været muligt at fremlægge undersøgelsens vigtigste resultater. Ordføreren vil gerne takke alle skyggeordførerne og AFET-medlemmerne for deres tætte samarbejde og deres store engagement i hele denne krævende proces.

### Problemets omfang

**Øget fokus på sikkerhed kombineret med teknologisk udvikling har gjort staterne i stand til at vide mere om borgerne end nogensinde før.** Når efterretningstjenesterne er i

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_da.pdf.
[2] Se rapport fra delegationen til Washington.
[3] Liste over skyggeordførere: Axel Voss (PPE), Sophia in't Veld (ALDE), Jan Philipp Albrecht (Verts/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).
[4] Liste over AFET-medlemmer: José Ignacio Salafranca Sánchez-Neyra (PPE), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).
[5] Jf. bilag I.

stand til at indsamle data med indholdet af kommunikation såvel som metadata, og når de kan følge borgernes elektroniske aktiviteter, navnlig disses brug af smartphones og tabletcomputere, så er tjenesterne faktisk i stand til at vide næsten alt om en person. Dette har medvirket til en fundamental omlægning af efterretningstjenesternes arbejde og fremgangsmåder, som bevæger sig væk fra den traditionelle model med målrettet overvågning som en nødvendig og rimelig terrorbekæmpelsesforanstaltning og over mod masseovervågningssystemer.

**Processen med den forøgede masseovervågning har ikke tidligere været genstand for nogen offentlig debat eller demokratisk beslutningsproces. Der er behov for at diskutere overvågningens formål og omfang og dens plads i et demokratisk samfund. Er situationen som følge af Edward Snowdens afsløringer et tegn på en generel drejning i samfundet mod at acceptere privatlivets freds endeligt til gengæld for sikkerhed?** Står vi over for et brud på privatlivets fred og intimitet, som er så stort, at det er muligt, ikke blot for kriminelle, men også for it-virksomheder og efterretningstjenester, at kende alle detaljer om en borgers liv? Skal vi blot acceptere dette uden yderligere diskussion? Eller er det lovgiverens ansvar at tilpasse de politiske og retlige værktøjer, så de begrænser risikoen og forhindrer, at der sker yderligere skade, hvis mindre demokratiske kræfter kommer til magten?

**Reaktioner på masseovervågning og en offentlig debat**

Debatten om masseovervågning er ikke ligeligt fordelt i EU. Faktisk er der i mange medlemsstater slet ikke nogen offentlig debat, og mediernes opmærksomhed varierer. Tyskland synes at være det land, hvor reaktionerne på afsløringerne har været kraftigst, og der har været omfattende offentlige diskussioner om konsekvenserne af dem. I Det Forenede Kongerige og Frankrig synes reaktionerne trods undersøgelser i The Guardian og Le Monde at være mere begrænsede, hvilket kan hænge sammen med påstandene om landenes nationale efterretningstjenesters aktiviteter med NSA. LIBE-undersøgelsesudvalget har hørt værdifulde indlæg fra parlamentariske tilsynsorganer i Belgien, Nederlandene, Danmark og endda Norge. Men det britiske og franske parlament har afvist at deltage. Disse forskelle viser endnu en gang den ulige fordeling af kontrol og tilsyn i EU vedrørende disse spørgsmål, og at der er behov for et endnu tættere samarbejde mellem de parlamentariske organer, som er ansvarlige for tilsyn.

Efter Edward Snowdens afsløringer i massemedierne har den offentlige debat været delt mellem primært to typer reaktioner. På den ene side står de, der afviser legitimiteten af de offentliggjorde oplysninger med den begrundelse, at de fleste rapporter i medierne er baseret på fejlfortolkninger. Derudover argumenterer mange, uden dog at tilbagevise afsløringerne, mod gyldigheden af afsløringerne på grund af de påståede sikkerhedsrisici i forhold til den nationale sikkerhed og bekæmpelse af terrorisme.

På den anden side står de, der mener, at oplysningerne kræver en oplyst offentlig debat på grund af de store problemer, de medfører for vigtige demokratiske spørgsmål som f.eks. retsstatsprincippet, grundlæggende rettigheder, borgernes privatliv, offentligt ansvar for retshåndhævelse og efterretningstjenester mv. Dette gælder navnlig journalister og redaktører på verdens største mediehuse, som er interesserede i afsløringerne, herunder The Guardian, Le Monde, Der Spiegel, The Washington Post og Glenn Greenwald.

Reaktionerne ovenfor er baseret på en række begrundelser, der, hvis de følges, kan føre til helt modsatte beslutninger om, hvordan EU bør eller ikke bør reagere.

**Fem argumenter for ikke at reagere**

– *Efterretning/national sikkerhed: EU har ingen kompetence*

Edward Snowdens afsløringer vedrører efterretningsaktiviteter i USA og visse medlemsstater, men national sikkerhed er en national kompetence, og EU har ikke kompetence på dette område (med undtagelse af EU's interne sikkerhed), og der kan derfor ikke træffes foranstaltninger på EU-plan.

– *Terrorisme: fare for whistlebloweren*

Enhver opfølgning på disse afsløringer eller blot overvejelser om dette svækker yderligere både USA's og EU's sikkerhed, eftersom den ikke fordømmer offentliggørelsen af dokumenter, hvis indhold, selv om det redigeres i henhold til de involverede medieaktørers forklaringer, kan give terrorgrupper værdifulde oplysninger.

– *Forræderi: ingen legitimitet for whistlebloweren*

Som primært amerikanere og briter har fremført, er alle debatter, som indledes, eller alle foranstaltninger, som planlægges i kølvandet på Edward Snowdens afsløringer reelt partisk og irrelevant, eftersom de tager udgangspunkt i landsforræderi.

– *Realisme: almene strategiske interesser*

Selv om visse fejltagelser og ulovlige aktiviteter skulle blive bekræftet, ville de skulle holdes op mod behovet for at bevare det særlige forhold mellem USA og Europa for at bevare fælles økonomiske, erhvervsmæssige og udenrigspolitiske interesser.

– *God regeringsførelse: Stol på din regering*

Den amerikanske regering og europæiske regeringer vælges demokratisk. Inden for sikkerhed og endda når der gennemføres efterretningsaktiviteter for at bekæmpe terrorisme, overholder de som princip demokratiske standarder. Denne formodning om god og lovlig regeringsførelse påhviler ikke kun indehaverne af den udøvende magt i disse stater, men også mekanismen med kontrol og tilsyn, som ligger i deres forfatningssystemer.

Som det kan ses, er argumenterne for ikke at reagere mange og stærke. Dette kan forklare, hvorfor de fleste EU-regeringer efter nogle indledende stærke reaktioner har foretrukket ikke at reagere. Ministerrådets vigtigste foranstaltning har været at nedsætte en transatlantisk gruppe af eksperter om databeskyttelse, som har holdt tre møder og udarbejdet en endelig rapport. En anden gruppe siges at have holdt møde om efterretningsspørgsmål mellem de amerikanske og medlemsstaternes myndigheder, men der er ingen tilgængelige oplysninger om dette. Det Europæiske Råd omtalte overvågningsproblemet i en enkel udtalelse fra stats-

og regeringscheferne[1]. Indtil videre har kun få nationale parlamenter indledt undersøgelser.

**Fem grunde til at reagere**

– *Masseovervågning: Hvilket samfund ønsker vi at bo i?*

Siden den første afsløring i juni 2013 er der gentagne gange henvist til Georges Orwells roman "1984". Siden angrebet den 11. september har fokus på sikkerhed og mere målrettet og specifik overvågning alvorligt skadet og undergravet begrebet privatlivets fred. Såvel Europas som USA's historie viser os faren ved masseovervågning og hældningen mod samfund uden privatliv.

– *De grundlæggende rettigheder*

Masseovervågning og vilkårlig overvågning er en trussel mod borgernes grundlæggende rettigheder, herunder retten til privatlivets fred, databeskyttelse, pressefrihed, retfærdig rettergang, som alle er knæsat i EU's traktater, chartret om grundlæggende rettigheder og den europæiske menneskerettighedskonvention. Disse rettigheder kan ikke omgås eller forhandles til gengæld for nogen fordele, medmindre dette er behørigt fastlagt i retsinstrumenter og er i fuld overensstemmelse med traktaterne.

– *EU's interne sikkerhed*

Nationale kompetencer inden for efterretning og national sikkerhed udelukker ikke parallelle EU-kompetencer. EU har udøvet sine kompetencer fra EU-traktaterne i forbindelse med national sikkerhed ved at fastlægge en række lovgivningsinstrumenter og internationale aftaler, som har til formål at bekæmpe alvorlig kriminalitet og terrorisme, fastlægge en intern sikkerhedsstrategi og agenturer, der arbejder på dette område. Derudover er der udviklet andre tjenester, som afspejler behovet for et øget samarbejde på EU-plan om efterretningsrelaterede spørgsmål: INTCEN (i EU-Udenrigstjenesten) og koordinatoren for antiterrorisme (i Rådets generalsekretariat), idet ingen af disse har et retsgrundlag.

– *Mangelfuldt tilsyn*

*Samtidig med at efterretningstjenesterne udfylder en uundværlig funktion, idet de beskytter mod indre og ydre trusler, skal de operere efter retsstatsprincippet, og for at gøre dette skal de være underlagt en streng og grundig tilsynsmekanisme. Det demokratiske tilsyn med efterretningsaktiviteter føres på nationalt plan, men som følge af sikkerhedstruslernes internationale karakter foregår der nu en enorm udveksling af oplysninger mellem medlemsstaterne og med tredjelande som USA. Der er behov for bedre tilsynsmekanismer på nationalt plan såvel som på EU-plan, hvis de traditionelle tilsynsmekanismer ikke skal blive ineffektive og forældede.*

[1] Det Europæiske Råds konklusioner af 24.-25. oktober 2013, navnlig: "Stats- og regeringscheferne noterede sig, at Frankrig og Tyskland agter at søge bilaterale samtaler med USA med henblik på inden årets udgang at nå frem til en forståelse om de gensidige forbindelser på området. De noterede sig, at andre EU-lande er velkomne til at tilslutte sig dette initiativ. De gjorde endvidere opmærksom på den eksisterende arbejdsgruppe mellem EU og USA om det beslægtede spørgsmål om databeskyttelse og opfordrede til hurtige og konstruktive fremskridt på dette område."

– *Afkølingseffekten på medierne og beskyttelse af whistleblowere*

Edward Snowdens afsløringer og de efterfølgende rapporter i medierne har fremhævet mediernes centrale rolle i et demokrati i forhold til at sikre regeringernes ansvarlighed. Hvis tilsynsmekanismerne viser sig ude af stand til at forhindre eller kontrollere masseovervågningen, er mediernes og whistleblowernes rolle af den allerstørste betydning for afsløringen af eventuelle ulovligheder eller tilfælde af magtmisbrug. Reaktioner fra de amerikanske og britiske myndigheder over for medierne har vist både pressens og whistleblowernes sårbarhed og det tvingende behov for at beskytte dem yderligere.

EU opfordres til at vælge mellem en "business as usual"-politik (tilstrækkelige argumenter for ikke at reagere, vent og se) og en "reality check"-politik (overvågning er ikke noget nyt, men der er tilstrækkelige beviser på et hidtil uset omfang af efterretningstjenesterne og deres kapacitet til, at EU bør reagere).

**Habeas corpus i et overvågningssamfund**

I 1679 vedtog det britiske parlament habeas corpus-loven som et stor skridt i retning af at sikre retten til en dommer i en tid med rivaliserende jurisdiktioner og lovkonflikter. I dag sikrer vores demokratier reelle rettigheder for en person, som er dømt eller tilbageholdt og rent fysisk er genstand for en straffesag eller indbringes for en domstol. Men dennes personoplysninger, som lægges, behandles, opbevares eller spores på digitale net, udgør en "samling personoplysninger", en slags digital samling, som er specifik for hver enkelt person og kan afsløre meget af dennes identitet og alle former for vaner og præferencer.

Habeas corpus anerkendes som et grundlæggende retsinstrument til at sikre den enkeltes frihed mod vilkårlige statslige foranstaltninger. Det, der er behov for i dag, er en udvidelse af habeas corpus til det digitale område. Retten til privatlivets fred og respekten for den enkeltes integritet og værdighed er på spil. Massesamlinger af data, der ikke overholder EU's databeskyttelsesregler, og specifikke overtrædelser af proportionalitetsprincippet inden for dataforvaltning er i strid med medlemsstaternes forfatningsmæssige traditioner og fundamentet for den europæiske forfatningsmæssige orden.

Det nye og vigtige i dag er, at disse risici ikke kun stammer fra kriminelle handlinger (som EU's lovgiver har vedtaget en række instrumenter imod) eller fra mulige cyberangreb fra regeringer i lande med en mindre demokratisk historik. Der er en erkendelse af, at sådanne risici også kan stamme fra retshåndhævelses- og efterretningstjenester i demokratiske lande, som placerer EU-borgere eller -virksomheder i lovkonflikter, hvilket medfører mindre retssikkerhed og eventuelle overtrædelser af rettigheder uden reelle klagemekanismer.

Der er behov for forvaltning af nettet for at sikre beskyttelsen af personoplysninger. Inden udviklingen af de moderne stater var der ingen garantier for sikkerheden på veje og stræder, og der var en risiko for den fysiske integritet. I dag er informationsvejene ikke sikre, selv om de dominerer vores hverdag. Integriteten af digitale data skal sikres, naturligvis mod kriminelle, men også mod statslige myndigheders eller kontrahenters eventuelle magtmisbrug eller misbrug fra private virksomheder i hemmelige retlige tiltag.

**LIBE-undersøgelsesudvalgets henstillinger**

Mange af problemerne i dag ligner i høj grad de problemer, som blev afsløret af Europa-Parlamentets undersøgelse om Echelon-programmet i 2001. Den tidligere lovgiver kunne ikke følge op på resultaterne og henstillingerne fra Echelon-undersøgelsen, og dette bør være en vigtig lære for denne undersøgelse. Det er derfor, der i denne beslutning i erkendelse af både omfanget af afsløringerne, og at disse fortsætter, planlægges fremad, så det sikres, at der fremsættes specifikke forslag til opfølgende foranstaltninger i Parlamentets næste mandatperiode, og at resultaterne fortsat står højt på EU's politiske dagsorden.

På grundlag af denne vurdering ønsker ordføreren at fremlægge følgende foranstaltninger til afstemning i Parlamentet:

**Et europæisk digitalt habeas corpus til beskyttelse af privatlivets fred på grundlag af syv foranstaltninger:**

Foranstaltning 1: vedtage databeskyttelsesreformpakken i 2014;

Foranstaltning 2: indgå paraplyaftalen mellem EU og USA, som skal sikre reelle mekanismer for domstolsprøvelse for EU-borgere i forbindelse med dataoverførsler fra EU til USA til retshåndhævelsesformål;

Foranstaltning 3: suspendere Safe Harbour-ordningen, indtil der er foretaget en fuldstændig gennemgang, og de nuværende smuthuller er lukket, så det sikres, at overførsel af personoplysninger til kommercielle formål fra Unionen til USA kun kan finde sted i overensstemmelse med de højeste EU-standarder;

Foranstaltning 4: suspendere TFTP-aftalen, indtil i) forhandlingerne om paraplyaftalen er afsluttet; ii) der er foretaget en grundig undersøgelse på grundlag af en EU-analyse, og der reelt er taget hånd om alle Parlamentets bekymringer i beslutningen af 23. oktober;

Foranstaltning 5: beskytte retsstatsprincippet og EU-borgeres grundlæggende rettigheder, navnlig med fokus på truslen mod pressefrihed og tavshedspligt (herunder i advokat-klient-forhold) samt bedre beskyttelse af whistleblowere;

Foranstaltning 6: udarbejde en europæisk strategi for it-uafhængighed (på nationalt plan og EU-plan);

Foranstaltning 7: udvikle EU som reference for demokratisk og neutral forvaltning af internettet.

Efter undersøgelsens afslutning bør Europa-Parlamentet fortsat fungere som kontrolorgan for EU-borgernes rettigheder med følgende tidsplan for overvågning af gennemførelsen:

- April til juli 2014: en overvågningsgruppe baseret på LIBE-undersøgelsesgruppen med ansvar for at overvåge nye afsløringer i medierne om undersøgelsens mandat og undersøgelse af gennemførelsen af denne beslutning;

- Fra juli 2014: en stående tilsynsmekanisme for dataoverførsel og domstolsprøvelse i

det kompetente udvalg;

- Foråret 2014: en formel opfordring til Det Europæiske Råd om at indarbejde det europæiske digitale habeas corpus i de retningslinjer, som skal vedtages i henhold til artikel 68 i TEUF;

- Efteråret 2014: et løfte om, at det europæiske digitale habeas corpus og dermed forbundne henstillinger skal tjene som de vigtigste kriterier for godkendelsen af den næste Kommission;

- 2014-2015: en tillids-/data-/borgerrettighedsgruppe, som skal mødes løbende, mellem Europa-Parlamentet og den amerikanske Kongres samt med andre engagerede tredjelandsparlamenter, herunder Brasilien;

- 2014-2015: en konference med de europæiske nationale parlamenters efterretningstilsynsorganer;

- 2015: en konference, der samler europæiske eksperter på højt plan inden for de forskellige områder vedrørende it-sikkerhed (herunder matematik, kryptografi, teknologier til forbedring af privatlivets fred …) for at hjælpe med at fremme en it-strategi i EU for næste valgperiode.

## BILAG I: LISTE OVER ARBEJDSDOKUMENTER

**LIBE-udvalgets undersøgelse**

| Ordfører og skyggeordførere som medforfattere | Emner | Europa-Parlamentets beslutning af 4. juli 2013 (se punkt 15-16) |
|---|---|---|
| Moraes (S&D) | USA's og EU's medlemsovervågningsprogrammer og deres konsekvenser for EU-borgernes grundlæggende rettigheder | 16, litra a), b), c), d) |
| Voss (PPE) | USA's overvågningsaktiviteter med hensyn til EU-data og mulige retlige konsekvenser for transatlantiske aftaler og det transatlantiske samarbejde | 16, litra a), b), c) |
| In't Veld (ALDE) og Ernst (GUE/NGL) | Demokratisk tilsyn med medlemsstaternes efterretningstjenester og EU's efterretningsorganer | 15, 16, litra a), c), e) |
| Albrecht (Verts/EFA) | Forholdet mellem overvågningspraksis i EU og USA og EU's bestemmelser om databeskyttelse | 16, litra c), e), f) |
| Kirkhope (ECR) | Omfanget af international, europæisk og national sikkerhed i et EU-perspektiv | 16, litra a), b) |
| AFET 3-medlemmer | Udenrigspolitiske aspekter af undersøgelsen om elektronisk masseovervågning af EU-borgere | 16, litra a), b), f) |

## BILAG II: LISTE OVER HØRINGER OG EKSPERTER:

LIBE-UDVAGETS UNDERSØGELSE
VEDRØRENDE NSA'S OVERVÅGNINGSPROGRAM,
OVERVÅGNINGSORGANER I FORSKELLIGE MEDLEMSSTATER
OG KONSEKVENSERNE HERAF FOR EU-BORGERNES GRUNDLÆGGENDE RETTIGHEDER OG FOR DET TRANSATLANTISKE SAMARBEJDE INDEN FOR RETLIGE OG INDRE ANLIGGENDER

I forlængelse af Europa-Parlamentets beslutning af 4. juli 2013 (stk. 16), har LIBE-udvalget afholdt en række høringer for at indsamle oplysninger om de forskellige aspekter, vurdere konsekvenserne af de behandlede overvågningsaktiviteter, navnlig i forbindelse med de grundlæggende rettigheder og databeskyttelsesreglerne, udforske klagemekanismerne og fremsætte anbefalinger for at beskytte EU-borgernes rettigheder samt for at styrke it-sikkerheden i EU-institutionerne.

| Dato | Emne | Eksperter |
|---|---|---|
| 5. september 2013, 15.00-18.30 (BXL) | - Udveksling af synspunkter med journalister, der har præsenteret sagen og offentliggjort oplysninger<br><br>- Opfølgning på Det Midlertidige Udvalg om Echelon-aflytningssystemet | • Jacques FOLLOROU, Le Monde<br>• Jacob APPELBAUM, undersøgende journalist, softwareudvikler og forsker i computersikkerhed forbundet med Torprojektet<br>• Alan RUSBRIDGER, ansvarshavende redaktør for nyheder og medier på The Guardian (via videokonference)<br>• Carlos COELHO (MEP), tidligere formand for Det Midlertidige Udvalg om Echelon-aflytningssystemet<br>• Gerhard SCHMID (tidligere MEP og ordfører for Echelon-betænkningen 2001)<br>Duncan CAMPBELL, undersøgende journalist og forfatter af STOA-rapporten "Interception Capabilities 2000" |
| 12. september 2013, | - Feedback på mødet i den transatlantiske EU-USA- | • Darius ŽILYS, formandskabet for Rådet, direktør for afdelingen |

| | | |
|---|---|---|
| 10.00-12.00 (STR) | ekspertgruppe om databeskyttelse af 19/20. september 2013 - arbejdsmetode og samarbejde med LIBE-udvalgets undersøgelse (for lukkede døre)<br><br>- Udveksling af synspunkter med artikel 29-arbejdsgruppen om databeskyttelse | for international lovgivning, det litauiske justitsministerium, (medformand for EU-USA-ad hoc-arbejdsgruppen om databeskyttelse)<br>• Paul NEMITZ, direktør for GD JUST, Kommissionen (medformand for EU-USA-ad hoc-arbejdsgruppen om databeskyttelse)<br>• Reinhard PRIEBE, direktør for GD JUST, Kommissionen (medformand for EU-USA-ad hoc-arbejdsgruppen om databeskyttelse)<br><br>• Jacob KOHNSTAMM, formand |
| 24. september 2013, 9.00-11.30 og 15.00-18.30 (BXL)<br><br>**med AFET** | - Beskyldninger om, at NSA har udnyttet SWIFT-data, der anvendes i TFTP-programmet<br><br>- Feedback på mødet i den transatlantiske EU-USA-ekspertgruppe om databeskyttelse af 19./20. september 2013<br><br>- Udveksling af synspunkter med det amerikanske civilsamfund (del I) | • Cecilia MALMSTRÖM, medlem af Kommissionen<br>• Rob WAINWRIGHT, direktør for Europol<br>• Blanche PETRE, chefjurist i SWIFT<br><br>• Darius ŽILYS, formandskabet for Rådet, direktør for afdelingen for international lovgivning, det litauiske justitsministerium, (medformand for EU-USA-ad hoc-arbejdsgruppen om databeskyttelse)<br>• Paul NEMITZ, direktør for GD JUST, Kommissionen (medformand for EU-USA-ad hoc-arbejdsgruppen om databeskyttelse)<br>• Reinhard PRIEBE, direktør for GD JUST, Kommissionen (medformand for EU-USA-ad hoc-arbejdsgruppen om databeskyttelse)<br>• Jens-Henrik JEPPESEN, direktør, europæiske anliggender, Center for |

| | | |
|---|---|---|
| | | Democracy & Technology (CDT)<br>• Greg NOJEIM, ledende jurist og direktør for projektet om frihed, sikkerhed og teknologi, Center for Democracy & Technology (CDT), (via videokonference)<br><br>• Dr. Reinhard KREISSL, koordinator, Increasing Resilience in Surveillance Societies (IRISS), (via videokonference)<br><br>• Caspar BOWDEN, uafhængig forsker, tidligere chefrådgiver vedrørende privatlivets fred i Microsoft, forfatter af notat fra temaafdelingen bestilt af LIBE-udvalget vedrørende USA's overvågningsprogrammer og deres konsekvenser for EU-borgernes privatliv |
| | - Effektiviteten af overvågningen i forbindelse med bekæmpelse af kriminalitet og terrorisme i Europa<br><br>- Præsentation af studiet om USA's overvågningsprogrammer og deres konsekvenser for EU-borgernes privatliv | |
| 30. september 2013, 15.00-18.30 (BXL) **med AFET** | - Udveksling af synspunkter med det det amerikanske civilsamfund (del II)<br><br>- Whistlebloweres aktiviteter inden for overvågning og deres retsbeskyttelse | • Marc ROTENBERG, Electronic Privacy Information Center (EPIC)<br>• Catherine CRUMP, American Civil Liberties Union (ACLU)<br><br>Udtalelser fra whistleblowere:<br>• Thomas DRAKE, tidligere højtstående ansat i NSA<br>• J. Kirk WIEBE, tidligere senioranalytiker i NSA<br>• Annie MACHON, tidligere efterretningsofficer i MI5<br><br>Udtalelser fra ngo'er om retsbeskyttelse af whistleblowere:<br>• Jesselyn RADACK, advokat og repræsentant for seks whistleblowere, Government Accountability Project<br>• John DEVITT, Transparency International, Irland |
| 3. oktober | - Beskyldninger om | • Geert STANDAERT, |

| | | |
|---|---|---|
| 2013, 16.00-18.30 (BXL) | "hacking"/udnyttelse af Belgacom-systemerne af efterretningstjenesterne (UK GCHQ) | vicedirektør for levering af tjenesteydelser, BELGACOM S.A.<br>• Dirk LYBAERT, generalsekretær, BELGACOM S.A.<br>• Frank ROBBEN, Commission de la Protection de la Vie Privée Belgique, medordfører for "dossier Belgacom" |
| 7. oktober 2013, 19.00-21.30 (STR) | - Konsekvenserne af USA's overvågningsprogrammer for Safe Harbour<br><br>- Konsekvenserne af USA's overvågningsprogrammer for andre instrumenter til international transfer (kontraktbestemmelser, bindende virksomhedsregler) | • Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (TYSKLAND)<br>• Christopher CONNOLLY - Galexia<br>• Peter HUSTINX, Europæisk Tilsynsførende for Databeskyttelse<br><br>• Isabelle FALQUE-PIERROTIN, direktør for CNIL (FRANKRIG) |
| 14. oktober 2013, 15.00-18.30 (BXL) | - Elektronisk masseovervågning af EU-borgere og internationale borgere,<br><br>Europarådet og<br><br>EU-retten<br><br>- Retssager om overvågningsprogrammer | • Martin SCHEININ, FN's tidligere særlige rapportør om fremme og beskyttelse af menneskerettighederne i forbindelse med terrorbekæmpelse, professor ved det europæiske universitetsinstitut og leder af FP7-projekt "SURVEILLE"<br><br>• Judge Bostjan ZUPANÈIÈ, dommer ved Den Europæiske Menneskerettighedsdomstol (via videokonference)<br><br>• Douwe KORFF, juraprofessor, London Metropolitan University<br><br>• Dominique GUIBERT, |

| | | |
|---|---|---|
| | | viceformand for "Ligue des Droits de l'Homme" (LDH)<br>• Nick PICKLES, direktør for Big Brother Watch<br>• Constanze KURZ, computerforsker, projektleder ved Forschungszentrum für Kultur und Informatik |
| 7. november 2013, 9.00-11.30 og 15.00-18.30 (BXL) | - Betydningen af EU's IntCen i EU's efterretningsaktiviteter (for lukkede døre)<br><br>- Nationale programmer for masseovervågning af personoplysninger i EU-medlemsstaterne og deres forenelighed med EU-retten<br><br>- Betydningen af parlamentarisk kontrol med efterretningstjenesterne på nationalt plan i en tid med masseovervågning (del I)<br>(Venedigkommissionen)<br>(Det Forenede Kongerige)<br><br>- Den transatlantiske EU-USA-ekspertgruppe | • Ilkka SALMI, direktør for EU's efterretningsanalysecenter (IntCen)<br><br>• Sergio CARRERA, seniorforsker og leder af afdelingen for retlige og indre anliggender, Det Europæiske Center for Politiske Studier (CEPS), Bruxelles<br>• Francesco RAGAZZI, lektor i internationale forhold, Leiden University<br><br>• Iain CAMERON, medlem af Kommissionen for Demokrati gennem Ret "Venedigkommissionen"<br>• Ian LEIGH, juraprofessor, Durham University<br>• David BICKFORD, tidligere juridisk direktør for sikkerheds- og efterretningstjenesterne MI5 og MI6<br>• Gus HOSEIN, administrerende direktør, Privacy International<br><br>• Paul NEMITZ, direktør - grundlæggende rettigheder og medborgerskab, GD JUST, Kommissionen<br>• Reinhard PRIEBE, direktør - krisestyring og indre sikkerhed, Generaldirektoratet for Indre Anl iggender, Kommissionen |
| 11. november 2013, 15.00-18.30 (BXL) | - USA's overvågningsprogrammer og deres konsekvenser for EU-borgernes privatliv (udtalelse af Jim SENSENBRENNER, medlem af den amerikanske kongres) | • Jim SENSENBRENNER, Repræsentanternes Hus i USA, (medlem af retsudvalget og formand for underudvalget om kriminalitet, terrorisme, |

| | | |
|---|---|---|
| | | indenlandsk sikkerhed og undersøgelser) |
| | - Betydningen af parlamentarisk kontrol med efterretningstjenesterne på nationalt plan i en tid med masseovervågning (Nederlandene, Sverige (del II) | • Peter ERIKSSON, formand for det svenske parlaments forfatningsudvalg (Rigsdagen)<br>• A.H. VAN DELDEN, formand for det uafhængige hollandske bedømmelsesudvalg vedrørende efterretnings- og sikkerhedstjenester (CTIVD) |
| | - NSA's programmer til elektronisk masseovervågning og it-virksomhedernes rolle (Microsoft, Google, Facebook) | • Dorothee BELZ, vicedirektør, rets- og virksomhedsanliggender, Microsoft EMEA (Europa, Mellemøsten og Afrika)<br>• Nicklas LUNDBLAD, direktør, offentlige politikker og forbindelser til regeringerne, Google<br>• Richard ALLAN, direktør for offentlige politikker i EMEA, Facebook |
| 14. november 2013, 15.00-18.30 (BXL) **med AFET** | - It-sikkerhed i EU-institutionerne (del I) (EP, COM (CERT-EU), (eu-LISA) | • Giancarlo VILELLA, generaldirektør, GD ITEC, Europa-Parlamentet<br>• Ronald PRINS, direktør og medstifter af Fox-IT<br>• Freddy DEZEURE, leder af taskforcen CERT-EU, GD DIGIT, Kommissionen<br>• Luca ZAMPAGLIONE, sikkerhedsansvarlig, eu-LISA |
| | - Betydningen af parlamentarisk kontrol med efterretningstjenesterne på nationalt plan i en tid med masseovervågning (del III) (Belgien, Danmark) | • Armand DE DECKER, næstformand for det belgiske senat, medlem af overvågningsudvalget i udvalget for tilsyn med efterretningstjenesterne<br>• Guy RAPAILLE, formand for udvalget for tilsyn med efterretningstjenesterne (Comité R)<br>• Karsten LAURITZEN, medlem af retsudvalget, retsordfører i |

| | | |
|---|---|---|
| | | Folketinget |
| 18. november 2013, 19.00-21.30 (STR) | - Retssager og andre klager over nationale overvågningsprogrammer (del II) (polsk ngo) | • Adam BODNAR, næstformand for bestyrelsen, Helsingfors-menneskerettighedsinstituttet, (Polen) |
| 2. december 2013, 15.00-18.30 (BXL) | - Betydningen af parlamentarisk kontrol med efterretningstjenesterne på nationalt plan i en tid med masseovervågning (del IV) (Norge) | • Michael TETZSCHNER, medlem af det stående udvalg for kontrol og konstitutionelle anliggender, Norge (Stortinget) |
| 5. december 2013, 15.00-18.30 (BXL) | - It-sikkerhed i EU-institutionerne (del II)<br><br>- Konsekvenserne af masseovervågning for fortrolighedsforholdet mellem advokater og klienter | • Olivier BURGERSDIJK, strategileder, det europæiske center for bekæmpelse af cyberkriminalitet, EUROPOL<br>• Udo HELMBRECHT, administrerende direktør for ENISA<br>• Florian WALTHER, uafhængig it-sikkerhedskonsulent<br>• Jonathan GOLDSMITH, generalsekretær for Council of Bars and Law Societies of Europe (CCBE) |
| 9. december 2013, (STR) | - Genopretning af tilliden til datastrømmen mellem EU og USA<br><br>- Beslutning 1954 fra Europarådet (2013) om "national sikkerhed og adgang til oplysninger" | • Viviane REDING, næstformand for Kommissionen<br><br>• Arcadio DÍAZ TEJERA, medlem af det spanske senat, medlem af Europarådets Parlamentariske Forsamling og ordfører for dets beslutning 1954 (2013) om "national sikkerhed og adgang til oplysninger" |
| 17.-18. december (BXL) | Parlamentarisk undersøgelsesudvalg om spionage af det brasilianske senat<br><br>It-midler til beskyttelse af privatlivets fred | • Vanessa GRAZZIOTIN, formand for det parlamentariske undersøgelsesudvalg om spionage<br>• Ricardo DE REZENDE FERRAÇO, ordfører, formand for det parlamentariske undersøgelsesudvalg om spionage<br><br>• Bart PRENEEL, professor i computersikkerhed og industriel kryptering på University KU Leuven, Belgien |

| | | |
|---|---|---|
| | Udveksling af synspunkter med journalister, der har offentliggjort oplysningerne (del II) (videokonference) | • Stephan LECHNER, direktør, Institut for Beskyttelse af Borgerne og Borgernes Sikkerhed (IPSC), Det Fælles Forskningscenter (FFC), Kommissionen<br>• Christopher SOGHOIAN, Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union<br>• Christian HORCHERT, it-sikkerhedskonsulent, Tyskland<br>• Glenn GREENWALD, forfatter og klummeskribent med fokus på national sikkerhed og borgerlige frihedsrettigheder, tidligere for The Guardian |

## BILAG III: LISTE OVER EKSPERTER, DER AFVISTE AT DELTAGE I DEN OFFENTLIGE HØRING, DER INDGÅR LIBE-UNDERSØGELSEN

### 1. Eksperter, der afviste invitationen fra LIBE-formanden

**USA**

- Keith Alexander, general for den amerikanske hær, direktør for NSA[1]
- Robert S. Litt, chefjurist, kontoret for direktøren for den nationale efterretningstjeneste[2]
- Robert A. Wood, chargé d'affaires, USA's repræsentant i EU

**Det Forenede Kongerige**

- Iain Lobban, direktør for det britiske Government Communications Headquarters (GCHQ)

**Frankrig**

- Bajolet, Directeur général de la Sécurité Extérieure, Frankrig
- Calvar, Directeur Central de la Sécurité Intérieure, Frankrig

**Nederlandene**

- Ronald Plasterk, minister for indenlandske anliggender og anliggender i kongedømmet, Nederlandene
- Ivo Opstelten, sikkerheds- og justitsminister, Nederlandene

**Polen**

- Dariusz Łuczak, leder af indenrigsefterretningstjenesten i Polen
- Maciej Hunia, leder af den polske udenrigsefterretningstjeneste

**Private it-virksomheder**

- Tekedra N. Mawakana, global leder af offentlige politikker og stedfortrædende chefjurist, Yahoo
- Saskia Horsch, seniorleder af offentlige politikker, Amazon

[1] Ordføreren mødte Alexander sammen med formand Brok og senator Feinstein i Washington den 29. oktober 2013.
[2] LIBE-Delegatione mødtes med Litt i Washington den 29. oktober 2013.

**Telekommunikationsselskaber i EU**

- Doutriaux, Orange
- Larry Stone, direktør for offentlige anliggender og regeringsrelaterede anliggender, British Telecom, Det Forenede Kongerige
- Telekom, Tyskland
- Vodafone

**2. Eksperter, der ikke besvarede invitationen fra LIBE-formanden**

**Tyskland**

- Gerhard Schindler, Präsident des Bundesnachrichtendienstes

**Nederlandene**

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

**Sverige**

- Ingvar Åkesson,
  Försvarets Radioanstalt (FRA)