EUROPEAN PARLIAMENT 2014 - 2019

Committee on Civil Liberties, Justice and Home Affairs

19.1.2015

WORKING DOCUMENT

on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens

Committee on Civil Liberties, Justice and Home Affairs

Claude Moraes

I. Introduction

During the previous legislative term the LIBE Committee was instructed by the Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)) to conduct an in-depth inquiry. During the inquiry between September 2013 and January 2014 a total of 16 hearings were held[1]. The work of the inquiry led to the adoption of the European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs[2]. Paragraph 135 of this resolution instructs the LIBE Committee to address the plenary again one year after the adoption of the resolution.

The LIBE Committee of Inquiry was responsible for the challenging task of conducting an investigation into the electronic mass surveillance of EU citizens and drafting a resolution detailing specific findings and recommendations within a short period of time. As a result of this demanding timeframe, the nature of the adopted resolution was forward planning ensuring that the specific proposals made could be followed up in this new mandate and would remain high on the EU political agenda.

The purpose of this document is to update the Committee Members of the factual developments since the adoption of the resolution (part II) and the state of the implementation of the proposed 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' (part III). As such, it could act as a basis for deciding on the next steps to be taken by the European Parliament to follow up the European Parliament Resolution.

II. Developments since the vote of the resolution in plenary

New revelations and other relevant press reports

In accordance with Paragraph 133 of the resolution, the LIBE inquiry team is competent for monitoring any new revelations concerning the inquiry's mandate. Since the adoption of the resolution in Plenary there have been several new allegations reported in the media which include the following:

- March 18th 2014 – Reports that the NSA is intercepting and **recording the whole content of all phone calls of at least one country for 30 days**. The programme called **"Mystic"** reportedly began in 2009[3]. Later reports revealed that countries under such mass surveillance include Austria and the Bahamas.
- March 29th 2014 - Reports that the NSA and the GCHQ are engaged in the joint surveillance of **three German satellite and telecom companies** - Stellar, Cetel and

[1] The full list of hearings and links to all documents is available in a special publication which is available here: http://www.europarl.europa.eu/document/activities/cont/201410/20141016ATT91322/20141016ATT91322EN.pdf

[2] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))

[3] http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html

IABG[1]. There are further details reported of NSA surveillance of **German chancellor Angela Merkel and other world leaders.**

- May 31st 2014 - Reports that the NSA is collecting huge numbers of images of people from communications that it intercepts through its global surveillance operations for use in sophisticated **facial recognition programs**[2].
- June 18th 2014 - Reports of the **NSA's operations in Germany** stating that NSA has key facilities and surveillance architecture in Germany[3].
- July 3rd 2014 - Reports that the **NSA targeted privacy software users** worldwide including the TOR network and other privacy software users[4].
- August 25th 2014 - Reports of the **ICREACH search engine** that allows a wide range of U.S. government agencies to search the NSA's stores of phone and internet metadata which could access many millions of minimized records of American citizens[5].
- September 14th 2014 - Reports that the NSA and GCHQ infiltrated several global telecom companies including several German telecom providers in order to gain access to the data flowing over their networks. Reports state that the aim of this **Treasure Map programme** is to "map the entire Internet - any device, anywhere, all the time"[6].
- October 4th 2014 – Reports that the German foreign intelligence service BND handed over bulk data to the NSA that stemmed from mass telecommunications interception at the main European internet switch DECIX in Frankfurt between 2004 and 2008. Reports state that this **operation "Eikonal"** was hidden from the parliamentary oversight commission.
- October 10th 2014 - Reports that three of the major phone networks in the UK including EE, Vodafone and Three, give police **mobile call records without requiring staff to initiate a review of all police information requests**[7].
- November 7th 2014 – Reports that the UK intelligence services have routinely **intercepted privileged confidential communication of lawyers**[8].
- November 9th 2014 – Reports that the German BND is planning to follow the example of the NSA to buy previously unreleased software exploits (so-called **"zero-days"**) on the black market[9].
- November 21th 2014 -Reports that UK telecommunications company Cable and Wireless (bought by Vodafone in July 2012) provided UK GCHQ with access to internet traffic. The company which was part of a programme called "Mastering the Internet", operated under the pseudonym of "Gerontic" [10].

[1] http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html
[2] http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=0
[3] https://firstlook.org/theintercept/2014/06/17/germany-nsas-largest-listening-post-europe/
[4] http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html
[5] https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton
[6] http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html
[7] http://www.theguardian.com/world/2014/oct/10/automatic-police-access-customers-mobile-phone-records-like-cash-machine-ripa-three-ee-vodafone
[8] http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client-abdel-hakim-belhaj-mi5-mi6-gchq
[9] http://www.spiegel.de/politik/deutschland/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001844.html
[10] http://www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq
http://uk.reuters.com/article/2014/11/20/uk-britain-security-telecomunications-idUKKCN0J42HQ20141120?feedType=RSS&feedName=internetNews

- November 24th 2014 **- Reports that a** highly sophisticated **and complex spyware known as "Regin"** was found on infected internal computer systems and email servers at Belgacom and has also been identified on the same European Union computer systems[1].
- December 4th 2014: Reports that the NSA - under the operation codenamed AURORAGOLD - has spied on hundreds of companies and organizations internationally, including the UK based trade group GSM Association, in an effort to find security weaknesses in cell phone technology that it can exploit for surveillance[2].

A. International developments

United Nations

- The Right to Privacy in the Digital Age, **25/11/2014**
The Third Committee of the United Nations General Assembly adopted this resolution based on initiatives tabled by Brazil and Germany. The resolution will be submitted to the General Assembly Plenary for adoption in mid-December[3].

The resolution emphasises the importance of the right to privacy in the digital age. It affirms that the same rights people have offline must also be protected on line, including the right to privacy and notes that the rapid pace of technological developments enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy.
Unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, and can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale. It emphasises that while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights, in particular as regards the right to privacy. This also applies when they intercept digital communications of individuals and/or collect personal data and when they require disclosure of personal data from third parties, including private companies.

Business enterprises have a responsibility to respect human rights as set out in UN documents[4]. It expresses its concern on the negative impact of surveillance and/or interception of communications, including extraterritorial surveillance, in particular when carried out on a mass scale. The operative part of the resolution calls on all States to respect the right to privacy, including in the context of digital communication; to take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; to review their procedures, practices and legislation regarding the

[1] https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/
[2] https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones
[3] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1
[4] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. A/HRC/17/31, annex
http://www.new-york-un.diplo.de/Vertretung/newyorkvn/en/__pr/speeches-statements/2014/20141125-braun-on-privacy.html?archive=3759636

surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy; to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data; and to provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.

- The Right to Privacy in the Digital Age, 30/06/2014

The United Nations High Commissioner for Human Rights presented a report based on the protection and promotion of privacy in the context of surveillance and/or the interception of digital communications and the collection of personal data[1]. The report states that "mass surveillance emerging as a dangerous habit rather than an exceptional measure" and affirmed "that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication". While the report focuses on privacy, it also states that mass surveillance also impacts on "the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life".

In addition, the report calls for States to immediately review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings States should take steps to address them and to ensure that effective and independent oversight regimes and practices are in place.

- Promotion and protection of human rights and fundamental freedoms while countering terrorism, 23/10/2014

In December 2013, the United Nations special rapporteur on counter-terrorism, Ben Emmerson, reported that the UN would conduct an investigation into the surveillance powers of American and British intelligence agencies following Edward Snowden's revelations. The subsequent report was presented to the General Assembly in October 2014. The main conclusions and recommendations of the report, include:

- The technical reach of the surveillance programmes currently in operation are so wide that they could be compatible with article 17 of the International Covenant on Civil and Political Rights (ICCPR) only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world.
- Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17.
- In line with article 17 of ICCPR there is an urgent need for States using this technology to revise and update national legislation to ensure consistency with international human rights law.
- States should establish strong and independent oversight bodies that are adequately resourced and mandated to conduct ex ante review.

[1] http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf

·States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant.

US

- **Focus on US citizens**

- More transparency in US intelligence operations (e.g. Statistical transparency report regarding the use of National Securities Authorities (June 2014))

Since the adoption of the European Parliament Resolution, the Privacy Civil Liberties Oversight Board (PCLOB) issued on July 2014 its report on the Surveillance Program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act[1]. The report focuses on the impact of Section 702 FISA on US persons. The report states that "*the treatment of non-US persons in US surveillance programs raises important but difficult legal and policy questions. ... The President's recent initiative under Presidential Policy Directive 28 on Signals Intelligence ("PPD-28") will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws".* The PCLOB has considered it most productive to assess these issues in the context of review process of the PPD-28[2].

The newly created NSA's Civil Liberties and Privacy Office released its first report on 7 October 2014[3]. It focuses on US persons protections. It states that it is in the process of developing implementation instructions of PPD-28 to apply equal protections to non-US persons to the maximum extent feasible consistent with national security.

- **US intelligence reform**

In July 2014 a bipartisan group of 19 senators submitted a new draft of the USA Freedom Act, namely a bill aimed at controlling NSA activities[4]. The bill focused only on safeguarding the rights of Americans citizens, and initially gathered the support of many privacy groups, technology companies, and the intelligence community. However, following an amendment adopted by the House Rules Committee of Congress many privacy groups publicly withdrew their support for the Bill on the basis that key safeguards were no longer in the text[5].On 19th November 2014, the US Senate rejected the bill. The White House have subsequently signalled its "strong support" for the bill and have publicly stated that they will work with Congress to "pass legislation that strikes a similar balance" in 2015[6].

- **Promise to give EU citizens some data protection/privacy/judicial redress**

In the framework of the negotiations for the "umbrella agreement" at the EU-US Ministerial

[1] http://www.pclob.gov/Library/702-Report.pdf
This report complements the first PCLOB report of 23 January 2014 devoted to Section 215 of Patriot Act.
[2] PCLOB report on Section 702 FISA (pages 98-102). See also
http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/
[3] https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf
[4] https://www.aclu.org/blog/national-security/senate-jumps-race-rein-nsa-surveillance
[5] https://cdt.org/blog/why-we-cant-support-the-new-usa-freedom-act/
https://www.eff.org/deeplinks/2014/05/eff-dismayed-houses-gutted-usa-freedom-act
[6] http://www.theguardian.com/us-news/2014/nov/19/white-house-revive-mass-surveillance-legislation-next-congress

of 24/25 June, US Attorney General Holder[1] announced that he would "*seek to work with Congress to enact legislation that would provide EU citizens with the right to seek redress in US courts if personal data is shared with US authorities by their home countries for law enforcement purposes under the proposed agreement is subsequently intentionally or willfully disclosed, to the same extent that US citizens could seek judicial redress in US courts for such disclosures of their own law enforcement information under the Privacy Act*"[2]. However, this would not change the discrimination of non-US persons under the Foreign Intelligence Surveillance Act due to scope of the "umbrella" agreement.

Brazil

Within the context of the inquiry conducted by Brazilian authorities, a Law on the Civil Framework for the internet called "Marco Civil da Internet" was adopted on 23 April 2014[3]. The law establishes the principles, guarantees, rights and obligations for the use of Internet in Brazil.
The Inquiry Committee presented its final report 17 April 2014[4].

The international "NETmundial" conference, hosted by the Brazilian government in April 2014, adopted a multi-stakeholder declaration of principles for internet governance, which includes a call for review of the surveillance programmes and the respect for the right to privacy[5].

B. Developments in Member States

Germany

In April 2014 a Committee of Inquiry on the mass surveillance revelations of the German Bundestag started its work[6]. The Committee on "Digitale Agenda" also discusses the issues[7].

France

The digital agenda is also high in the French government's agenda, with a draft law on the digital society being expected to be tabled before the French Parliament at the beginning of 2015[8]. In an extensive report the French Senate has discussed a new strategy for the European Union in the world governance of Internet[9]. Furthermore, the French Council of State has included in its Annual report 2014, entitled "Le numérique et les droits fondamentaux", fifty recommendations linked with "rethinking the protection of fundamental rights" in the context

[1] On 25th September 2014, the Justice Department announced US Attorney General Holder would resign when his successor was confirmed.
[2] http://europa.eu/rapid/press-release_STATEMENT-14-208_en.htm
http://www.justice.gov/opa/pr/attorney-general-holder-pledges-support-legislation-provide-eu-citizens-judicial-redress
[3] http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm
[4] http://www.senado.leg.br/atividade/materia/getPDF.asp?t=149208&tp=1
[5] http://netmundial.br/wp-content/uploads/2014/04/NETmundialPublicConsultation-FinalReport20140421.pdf
http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
[6] See the following website for information: http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss
[7] http://www.bundestag.de/bundestag/ausschuesse18/a23
[8] http://www.lemonde.fr/pixels/article/2014/09/09/le-conseil-d-etat-veut-un-encadrement-des-activites-des-espions-sur-internet_4484206_4408996.html
[9] Rapport d'information "L'Europe au secours de l'Internet: démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne", G. Gorce, C. Morin-Desailly, http://www.senat.fr/notice-rapport/2013/r13-696-2-notice.html

of digital society[1]. Among others, the report contains recommendations on the oversight of intelligence services, net neutrality, the right to be forgotten, cooperation at EU and international level in order to effectively respect fundamental rights and set basic principles of internet governance.

UK

On 17 October 2013, the Intelligence and Security Committee (ISC) of UK Parliament announced that it would be broadening its initial inquiry into the laws which govern the intelligence agencies' ability to intercept private communications. In addition to considering whether the current statutory framework governing access to private communications remains adequate, the Committee is also considering the appropriate balance between the individual right to privacy and our collective right to security. Since then, the Privacy and Security Inquiry have held a number of public hearings including with the Director of GCHQ, the Director General of MI5, the Chief of MI6, MPs, academics and civil society members.

On 18 July 2014, the UK Parliament adopted the Data Retention and Investigatory Powers Act, expanding the surveillance powers established in an earlier set of laws known as the Regulation of Investigatory Powers Act ("RIPA"). The new act empowers the UK Secretary of State for the Home Department to issue interception warrants for communications content that is stored outside of the UK's territorial jurisdiction, and gives the UK authorities extremely broad powers to obtain, access, and store communications metadata (such as the date, time, sender, recipient, and subject line of an e-mail).

Belgium

In September 2013 Belgacom denounced to the criminal judicial authorities a hacking incident affecting the company. The case is currently under investigation by the prosecutor's office. The Belgian data protection authority decided not to proceed to a parallel investigation. Press coverage and IT security company Symantec reported recently that Belgacom had been the victim of a complex malware, called REGIN, which originated allegedly from US or UK intelligence agencies.

Netherlands

In a letter to the Dutch parliament of 21 November 2014, the Dutch government announced its plans to propose new legislation making interception possibilities of communications "technologically neutral", where it currently allows for the interception of satellite communications. The Dutch government will introduce an amendment to the Dutch Intelligence and Security Act 2002 (Wet op de Inlichten- en Veiligheidsdiensten 2002) which in practice will allow for intelligence services to also intercept cable-bound communications.

C. Data protection developments and Court cases

EU Article 29 Working Party

In April 2014 the EU Article 29 Working Party adopted its opinion on surveillance of electronic communications[2] which concludes that secret, mass and indiscriminate surveillance

[1] http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2014-Le-numerique-et-les-droits-fondamentaux

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security.

In February 2014, the EU Article 29 Working Party issued its opinion on the necessity and proportionality principle, setting out a toolbox of steps in order to ensure AFSJ measures touching personal data rights are fully compliant with the legal requirement of proportionality and necessity[1].

On 26 November 2014, the EU Data Protection Authorities assembled in the Article 29 Working Party issued a joint statement. They reaffirmed that secret, massive and indiscriminate surveillance is neither legal with regard to EU Treaties and legislation nor ethically acceptable. Unrestricted bulk retention of personal data for security purposes is not acceptable in a democratic society; processing of personal data for surveillance purposes must be take place under adequate safeguards in accordance with Article 8 ECHR, including independent and effective supervision, current EU instruments framed for data transfers between private parties provide a legal basis for transfer of data to a third country for the purpose of massive and indiscriminate surveillance Finally they also stated that where public or private parties collect massive amounts of data providing very precise information on private lives, the storage should be organised in a manner enabling an independent authority to effectively control compliance with data protection rules, storage in the EU is an effective manner to facilitate it.

Schrems vs Facebook

The Irish High Court has made a request to the Court of Justice of the European Union for a preliminary ruling relating to the interpretation of the Commission adequacy decision on the US Safe Harbour. The purpose of this question is to know if a Commission adequacy decision must be interpreted in accordance with the Charter, namely articles 7 and 8 thereof and if in the context of on-going mass surveillance, the Safe Harbor decision is still applicable[2].

CJEU Digital Rights Ireland judgement

On 8 April 2014, the Court of Justice of the European Union repealed the Directive 2006/24/EC on the retention of telecommunications data because of its disproportionate intrusion into the fundamental right to data protection[3].

Other court cases

- UK based NGO Privacy International has taken 3 separate challenges to the Investigatory Powers Tribunal (IPT) in the UK referring to the Prism and Tempora surveillance programme and over blanket FOIA denials from GCHQ over requests for Five Eyes agreements.

- 7 internet service and communication providers from the UK, Germany, US, Netherlands, Korea, Zimbabwe, along with Privacy International took a collective action against GCHQ targeting, attacking and exploitation of networks maintaining communications infrastructure. There is no hearing date scheduled at the Investigatory Powers Tribunal (IPT) in the UK.

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf
[2] [2014] IEHC 310, http://www.bailii.org/ie/cases/IEHC/2014/H310.html
[3] CJEU: Judgment of the Court (Grand Chamber) of 8 April 2014 in Joined Cases C-293/12 and C-594/12, OJ C 175, 10.6.2014, p. 6–7

- Twitter, Yahoo and others took the US Government to court in order to be more transparent about access requests by intelligence services.

- Microsoft challenged a decision of US law enforcement authorities to comply with a sealed search warrant for a consumer email account it stores in Dublin, Ireland. The US judge ruled in July that since Microsoft is a US company, it should comply with US laws. Microsoft has agreed to be held in contempt of court in order to appeal the ruling that said it must hand over user data stored outside US[1]. Several US IT companies have supported Microsoft in its legal claim. The Irish government has called on the Commission to intervene in the case[2].

- Twitter recently sued the FBI and the Department of Justice in order to be able to release more information about government surveillance of its own users[3]. The case is relevant because Twitter asserts the right to be able to say that it is not under surveillance[4].

- Several court cases have also been filed across the US in order to challenge the NSA's bulk phone records programme[5].

D. Technical Developments

IT companies

- Google and Apple have recently announced that their operating systems for mobile devices (smartphones, tablets) will enable customers' encryption of their devices preventing these companies gaining access to data stored therein. A number of actors have publicly expressed their concerns on these initiatives including the Director of the FBI, the Director of Europol and the Chief of the UK Intelligence agency GCHQ. US Attorney General Eric Holder has expressed similar concerns[6]. Many company officials and independent security experts said that increasingly widespread use of encryption technology makes mass surveillance more difficult .

- Yahoo, Google Whatsapp and others announced plans to introduce end-to-end encryption. Law enforcement authorities have raised concerns about this practice which they claim would hinder criminal investigations.

IETF

The Internet Engineering Task Force's Internet Architecture Board has called on protocol designers, developers & operators to encrypt internet traffic by default[7].

[1] https://vpncreative.net/2014/09/01/microsoft-refuses-relinquish-overseas-data/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+vpncreative+%28VPN+Creative%29?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+vpncreative+%28VPN+Creative%29
[2] http://www.rte.ie/news/2014/1118/660564-tech-data-commission/
[3] http://abcnews.go.com/Technology/wireStory/twitter-sues-fbi-doj-release-nsa-request-info-26022908
[4] http://justsecurity.org/16221/twitters-amendment-suit-warrant-canary-question/
[5] https://www.aclu.org/blog/national-security/challenge-nsas-mass-surveillance-inches-way-court-system
[6] http://www.theguardian.com/society/2014/oct/01/eric-holder-raises-concerns-over-privacy-advances-by-technology-companies
[7] https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

E. Policy Developments at EU Institutions

Position of the Commission on the European Parliament resolution

On 25 June the Commission adopted its position on the resolution[1].

On 18 July, Vice President Neelie Kroes responded to the issues related to her area of competence on the EU Digital Agenda, underlining that the LIBE Inquiry resolution would provide guidance for the Commission in the next legislative mandate.

The European Commission has also made attempts to contribute to a solution to the surveillance problem, in particular through the EU-US ad-hoc working group on data protection. However, since the adoption of their report[2] no further developments have been reported through this channel.

European Council

In its resolution of 2 April 2014 on the mid-term review of the Stockholm Programme the Parliament explicitly called on the European Council "to address the recommendations and calls made in its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens´ fundamental rights and on transatlantic cooperation in Justice and Home Affairs;" (see paragraph 24 of the resolution). Despite this explicit call, the European Council's strategic guidelines of 26/27 June 2014 for legislative and operational planning within the area of freedom, security and justice do not mention at all the topic of electronic mass surveillance.

IT Security in EU Institutions

Paragraph 101 of the Resolution refers to IT security within the European Parliament and devising recommendations to strengthen IT security in the EU's institutions and conduct a thorough review and assessment of Parliament's IT security dependability.

In line with this, the Monitoring Group have received an intermediate report by DGITEC in outlined a Roadmap and Action Plan on EU ICT Security.

The External Action Service has taken steps to enhance its secure communication facilities but more work remains to be done and it should also be noted that parts of the EU institutions dealing with internal policies, which can also have a bearing on external actors, may be subject to espionage attempts.

European Central Bank contract with Verizon

Concern has been raised as the ECB's continual online service contract with Verizon despite allegations that the company was involved in spying activities of the NSA. In Berlin, the Government has indicated that they will not renew their contract with the American telecom operator as a result of these allegations[3].

III. State of play of the implementation of the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age'

With the resolution of 12 March the Parliament decided to launch a 'European Digital Habeas

[1] Available at http://www.oeil.ep.parl.union.eu/oeil/spdoc.do?i=24263&j=0&l=en
[2] Council document 16987/13, 27 November 2013,
[3] http://www.lemonde.fr/pixels/article/2014/11/10/espionnage-les-entreprises-americaines-face-a-une-suspicion-grandissante-en-allemagne_4521458_4408996.html

Corpus - protecting fundamental rights in a digital age' with 8 actions. These are listed below and the developments towards their implementation since the adoption of the resolution are indicated briefly.

Action 1: Adopting the Data Protection Package in 2014
Parliament adopted the first reading positions on the Data Protection Regulation and Directive on 12 March 2014. The Council has not yet been able to agree on a position which could allow for the start of Interinstitutional negotiations.
Partial agreements have been reached in the JHA Council of July, October and December 2014 in respect of chapters relating to international data flows and obligations of controllers and processors and public sector. Further partial agreements are expected under Latvian presidency with a view to starting inter-institutional negotiations.

Action 2: Concluding the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens, including in the event of data transfers from the EU to the US for law enforcement purposes
The US administration has announced its intention to present in Congress legal initiatives to grant EU citizens with the right to seek redress in U.S. courts if personal data shared with US authorities by their home countries for law enforcement purposes under the proposed agreement is subsequently intentionally or willfully disclosed, to the same extent that US citizens could seek judicial redress in US courts for such disclosures of their own law enforcement information under the Privacy Act. The Commission has informed on 3 December 2014 about the state of play of the negotiations. It is not clear whether US legal initiatives will provide EU individuals with judicial redress for all the cases in which EU law does.

Action 3: Suspending Safe Harbour until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with the highest EU standards
In its position of 25th June on the resolution, the Commission stated that it "is engaging with the US on implementing the 13 Safe Harbour recommendations. Remedies should be identified by summer 2014 and implemented as soon as possible. On that basis, the Commission will undertake a complete stock-taking of the functioning of Safe Harbour." Also in its Communication on the functioning of the Safe Harbour (COM(2013)0847) and rebuilding trust in EU-US data flows (COM(2013)0846) the Commission announced that remedies to shortcomings of the decision would be identified by summer 2014 and implemented as soon as possible.
The European Parliament has not received a detailed analysis or update on the developments with discussions on Safe Harbour despite the transmitted deadline of summer 2014 from the Commission.
During his Parliamentary Hearing, Vice-President designate Ansip informed Members of the European Parliament that suspension of the Safe Harbour is an option considered by the Commission if there is no satisfactory solution to problems identified by the Commission.

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

properly addressed
In its position of 25th June on the resolution, the Commission recalled its steps already undertaken (formal consultations under Article 19 of the Agreement with the US, the dialogue with SWIFT, reporting of the results to the Parliament on 27 November 2013). It also stated that the investigation by the Dutch and the Belgian data protection authorities into the security of financial messaging data at the Designated Provider "did not find any violations of legal security requirements or any indications that third parties have had or could have had unlawful access to financial messaging data related to European citizens". Furthermore "the recently conducted third joint review provided further assurances that the Agreement has been properly implemented by the US side." The Commission concluded that it "does not have, at this stage, the intention to propose suspending the Agreement".
The Commission has not indicated if the ruling of the ECJ of 8/4/2014 on the data retention directive will impact on this instrument which provides for bulk processing retention and transfer of personal data.

Action 5: Evaluating any agreement, mechanism or exchange with third countries involving personal data in order to ensure that the right to privacy and to the protection of personal data is not violated due to surveillance activities, and take necessary follow-up actions
The Commission in its position indicated that both Commission adequacy decisions and standard contractual clauses for international transfers enable the Commission to monitor and assess their implementation and report on any finding affecting the proper functioning. The Commission in its reply has not given an explanation as to why it does not intend to monitor and assess the adequacy decisions of Canada and New Zealand despite information published about the involvement of these countries in electronic mass surveillance activities.

Action 6: Protecting the rule of law and the fundamental rights of EU citizens, (including from threats to the freedom of the press), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations), as well as ensuring enhanced protection for whistleblowers
In its position of 25th June on the resolution, the Commission noted that it has no overall competence in the area of media freedom and pluralism and instead invites the Member States to take appropriate measures to safeguard the right of journalists to protect their sources and to protect journalists from undue influence.

Concerning the call for enhanced protection for whistleblowers including in the field of intelligence, the Commission has responded by saying there is no EU competence in this area. It has not responded to Parliament's request to conduct an examination as to a possible European whistleblower protection programme including in the field of intelligence or the possibility of international protection to whistleblowers from protection.

The Commission has not responded to the issue of mass surveillance and its impact on professional confidentiality including for journalists, lawyers, doctors and other regulated professions.

Action 7: Developing a European strategy for greater IT independence (a 'digital new deal' including the allocation of adequate resources at national and EU level) in order to boost IT industry and allow European companies to exploit the EU privacy competitive advantage
In its position of 25th June on the resolution, the Commission welcomed the different

recommendations and ideas listed in the resolution in this field. The Commission indicated that it is developing a European strategy for IT independence and is working toward a European strategy to boost European IT industry. The Commission also reiterated that it has made three concrete proposals linked to these issues: the proposed Data Protection Regulation, the proposed Network and Information Security Directive, and the proposed Telecoms Single Market Regulation.

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

On 14 March 2014 the United States Government announced plans for the "transition out of the IANA function", which will allow a more global multi-stakeholder basis for this important element of governance of the Internet.

In April 2014 the Global Multistakeholder Meeting on the Future of Internet Governance (NETMundial) took place in Brazil. In this conference, the Commission reiterated its aim to make the EU a reference player for Internet governance and its vision of a multi-stakeholder model for internet governance, based on transparent and democratic involvement of all relevant actors and groups.

IV. Preparations for next steps

Given the nature of the resolution of 12 March as a forward-looking document it contains a series of recommendations, requests and calls for a follow-up. They are addressed not only to the US but also to Member States, EU institutions and agencies, Parliament's administration, international organisations, national Parliaments and businesses. By way of example the following can be mentioned:

- Key requests are those addressed to US and Member States' authorities with the aim of ending the practices of mass-surveillance identified and putting in place clear legal frameworks to prohibit such activities.
- Further requests are addressed to the European institutions and especially the Commission. They deal, in particular, with international transfers of data and the various international agreements. They also include calls on the Commission to initiate a number of proposals, for example in the field of cloud computing, the use of back-doors, security of IT systems, EU independence in the IT sector, EU routing, as well as certification and validation for IT hardware.
- Further requests are made to a number of EU agencies such as ENISA (on security and privacy standards), FRA (research on the protection of fundamental rights in the context of surveillance), eu-LISA (reliability of SIS II, VIS, Eurodac), Europol (request Member States to initiate criminal investigations) and international organisations including the Council of Europe (launch of the Article 52 procedure) and the United Nations (additional protocol to Article 17 of the ICCPR).
- The Parliament's administration was tasked to provide information, analysis and recommendations on a wide range of issues aimed at enhancing Parliament's IT security.
- Finally, the resolution also contains a series of activities to be undertaken by Parliament itself such as in general terms on following-up the work of the inquiry but also on concrete measures such as a conference on protecting on-line privacy by enhancing IT security and EU IT autonomy and a conference with intelligence oversight bodies of European national parliaments.

Paragraph 133 first indent of the resolution tasked a monitoring group based on the LIBE inquiry team with the responsibility of monitoring any new revelations concerning the inquiry's mandate and scrutinising the implementation of the resolution. Paragraph 135 of the resolution instructed the LIBE Committee to address Parliament in Plenary on this matter a year after the adoption of the resolution in order to assess the extent to which the recommendations adopted by Parliament have been followed.

Based on the above, a monitoring group has been established by the LIBE Coordinators with the aim to closely scrutinise the implementation of the resolution - including through regular slots in the agenda of the LIBE Committee - and to draw up a report to assess the extent to which the recommendations adopted by Parliament have been followed, to analyse any instances where they have not been followed and to come up with further details and proposals for the implementation of the European Digital Habeas Corpus.