European Parliament
2014-2019

TEXTS ADOPTED
Provisional edition

P8_TA-PROV(2015)0388

Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens

European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP))

The European Parliament,

– having regard to the legal framework set by the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10 and 21 thereof, the Charter of Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof, the European Convention on Human Rights, in particular Articles 6, 8, 9, 10 and 13 thereof, and the case law of the European courts concerning security, privacy and freedom of speech,

– having regard to 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[1] (hereinafter 'the resolution'),

– having regard to the working document of 19 January 2015 entitled 'On the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU citizens'[2],

– having regard to the resolution of the Parliamentary Assembly of the Council of Europe of 21 April 2015 on mass surveillance,

– having regard to the questions to the Council and to the Commission on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (O-000114/2015 – B8-0769/2015 and O-000115/2015 – B8-0770/2015),

– having regard to the motion for a resolution of the Committee on Civil Liberties, Justice and Home Affairs,

– having regard to Rules 128(5) and 123(2) of its Rules of Procedure,

---

1 Texts adopted, P7_TA(2014)0230.
2 PE546.737v01-00.

A. whereas in the resolution Parliament called on the US authorities and the Member States to prohibit blanket mass surveillance activities and bulk processing of personal data of citizens, and denounced the reported actions by intelligence services that have severely affected EU citizens' trust and their fundamental rights; whereas the resolution pointed towards the possible existence of other motives such as political and economic espionage, given the capacity of the reported mass surveillance programmes;

B. whereas the resolution launched 'A European Digital Habeas Corpus – protecting fundamental rights in a digital age', with eight specific actions, and instructed the Committee on Civil Liberties, Justice and Home Affairs to address Parliament within one year with a view to assessing the extent to which the recommendations have been followed;

C. whereas the working document of 19 January 2015 reported on developments since the adoption of the resolution, with the stream of revelations of alleged electronic mass surveillance activities continuing, and on the state of implementation of the proposed 'European Digital Habeas Corpus', indicating the limited response of the institutions, Member States and stakeholders called upon to act;

D. whereas in the resolution Parliament called on the Commission and other EU institutions, bodies, offices and agencies to act on the recommendations, in accordance with Article 265 TFEU ('failure to act');

E. whereas Wikileaks recently revealed the targeted surveillance of the communications of the last three French Presidents as well as of French cabinet ministers and the French Ambassador to the US; whereas this strategic and economic espionage has been carried out on a large scale over the last ten years by the NSA, targeted on all the French state structures as well as the biggest French companies;

F. whereas the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression states that encryption and anonymity provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age; whereas that report also states that any restrictions on encryption and anonymity must be strictly limited in accordance with the principles of legality, necessity, proportionality and legitimacy of objective;

1. Welcomes the inquiries by the German Bundestag, the Council of Europe, the UN and the Brazilian Senate, the debates in several other national parliaments and the work of numerous civil society actors that have contributed to the raising of general awareness regarding electronic mass surveillance;

2. Calls on the EU Member States to drop any criminal charges against Edward Snowden, grant him protection and consequently prevent extradition or rendition by third parties, in recognition of his status as whistleblower and international human rights defender;

3. Is, however, highly disappointed by the overall lack of sense of urgency and willingness shown by most Member States and the EU institutions in terms of seriously addressing the issues raised in the resolution and implementing the concrete recommendations contained therein, as well as by the lack of transparency towards or dialogue with Parliament;

4. Is concerned at some of the recent laws in some Member States that extend surveillance capabilities of intelligence bodies, including, in France, the new intelligence law adopted

by the National Assembly on 24 June 2015, several provisions of which, according to the Commission, raise important legal questions, in the UK, the adoption of the Data Retention and Investigatory Powers Act 2014 and the subsequent court decision that certain articles were unlawful and to be disapplied, and, in the Netherlands, the proposals for new legislation to update the Intelligence and Security Act of 2002; reiterates its call on all Member States to ensure that their current and future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies are in line with the standards of the European Convention on Human Rights and all relevant Union legislation; ;

5. Welcomes the inquiry by the German Bundestag into mass surveillance; is strongly concerned about the revelations of mass surveillance of telecommunications and internet traffic inside the Union by the German foreign intelligence agency BND in cooperation with the NSA; considers this a breach of the principle of sincere cooperation under Article 4(3) TEU;

6. Asks its President to call on the Secretary-General of the Council of Europe to launch the Article 52 procedure, according to which 'on receipt of a request from the Secretary-General of the Council of Europe any High Contracting Party shall furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention';

7. Considers the Commission's reaction so far to the resolution to be highly inadequate given the extent of the revelations; calls on the Commission to act on the calls made in the resolution by December 2015 at the latest; reserves the right to bring an action for failure to act or to place certain budgetary resources for the Commission in a reserve until all the recommendations have been properly addressed;

8. Stresses the significance of the ruling of the Court of Justice of the European Union (CJEU) of 8 April 2014 declaring invalid Directive 2006/24/EC on Data Retention; recalls that the Court stipulated that the interference of this instrument with the fundamental right to privacy has to be limited to what is strictly necessary; highlights the fact that this ruling presents a novel aspect insofar as the Court of Justice refers specifically to a particular body of case law of the European Court of Human Rights concerning the issue of 'general programmes of surveillance' and has now effectively incorporated the same principles, stemming from that particular case law of the European Court of Human Rights, into EU law in this same field; stresses that it is therefore to be expected that the Court of Justice will, in future, also apply the same reasoning when assessing the validity, under the Charter, of other EU and Member State legislative acts in this same field of 'general programmes of surveillance';

Data Protection Package

9. Welcomes the opening of informal interinstitutional negotiations on the draft General Data Protection Regulation and the Council's adoption of a general approach on the draft Data Protection Directive; reiterates its intention to conclude negotiations on the Data Protection Package in 2015;

10. Reminds the Council of its commitment to respect the Charter of Fundamental Rights of the European Union in its amendments to the Commission proposals; reiterates in particular that the level of protection offered should not be lower than that already established by Directive 95/46/EC;

11. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals, and that the two must therefore be treated as a package to be adopted simultaneously, in order to ensure that all data processing activities in the EU provide a high level of protection in all circumstances; underlines that the objective of strengthening the rights and protections of individuals with regard to the processing of their personal data must be met when adopting the package;

EU-US umbrella agreement

12. Notes that since the adoption of the resolution the negotiations with the US on the EU-US framework agreement on the protection of personal data when transferred and processed for law enforcement purposes (hereinafter the 'umbrella agreement') have been completed and the draft agreement has been initialled;

13. Welcomes the efforts by the US administration to rebuild trust through the umbrella agreement, and particularly welcomes the fact that the Judicial Redress Act of 2015 was successfully passed by the House of Representatives on 20 October 2015, underlining the substantial and positive steps taken by the US to meet EU concerns; considers it of paramount importance to ensure the same rights in all the same circumstances of effective judicial redress for EU citizens/individuals whose personal data are processed in the EU and transferred to the US, without any discrimination between EU and US citizens; calls on the US Senate to pass legislation guaranteeing this; underlines that one prerequisite for signature and conclusion of the umbrella agreement is the adoption of the Judicial Redress Act in the US Congress;

Safe Harbour

14. Recalls that the resolution calls for the immediate suspension of the Safe Harbour Decision as it does not provide adequate protection of personal data for EU citizens;

15. Recalls that any international agreement concluded by the EU takes precedence over EU secondary law, and therefore stresses the need to ensure that the umbrella agreement does not restrict the data subject rights and safeguards applying to data transfer in accordance with EU law; urges the Commission, therefore, to assess in detail precisely how the umbrella agreement would interact with, and have an effect on, the EU legal framework for data protection, including, respectively, the current Council framework decision, the Data Protection Directive (95/46/EC) and the future data protection directive and regulation; calls on the Commission to present a legal assessment report on this matter to Parliament before initiating the ratification procedure;

16. Recalls that the Commission addressed 13 recommendations to the US in its communications of 27 November 2013 on the functioning of the Safe Harbour, in order to ensure an adequate level of protection;

17. Welcomes that in its ruling of 6 October 2015 the CJEU declared invalid the Commission Adequacy Decision 2000/520/EC on the US Safe Harbour; stresses that this ruling has confirmed the long-standing position of Parliament regarding the lack of an adequate level of protection under this instrument; calls on the Commission to immediately take the necessary measures to ensure that all personal data transferred to the US are subject to an effective level of protection that is essentially equivalent to that guaranteed in the EU;

18. Objects to the fact that Parliament has not received any formal communication from the Commission regarding the state of implementation of the 13 recommendations, despite the Commission's announcement that it would do so by summer 2014; underlines that, following the CJEU's decision to invalidate Decision 2000/520/EC, it is now urgent that the Commission provide a thorough update on the negotiations thus far and the impact of the judgment on the further negotiations that were announced; invites the Commission to reflect immediately on alternatives to Safe Harbour and on the impact of the judgment on any other instruments for the transfer of personal data to the US, and to report on the matter by the end of 2015;

19. Urges the Commission to assess the legal impact and implications of the Court of Justice ruling of 6 October 2015 in the Schrems case (C-362/14) vis-à-vis any agreements with third countries allowing for the transfer of personal data, such as the EU-US Terrorist Finance Tracking Programme (TFTP) Agreement, passenger name record (PNR) agreements, the EU-US umbrella agreement and other instruments under EU law which involve the collection and processing of personal data;

Democratic oversight

20. While fully respecting that national parliaments have full competence in the oversight of national intelligence services, calls on all those national parliaments which have not yet done so to thoroughly evaluate and install meaningful oversight of intelligence activities and to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means and access to all relevant documents in order to be able to effectively and independently oversee intelligence services and information exchanges with other foreign intelligence services; re-expresses its commitment to cooperate closely with national parliaments to ensure that effective oversight mechanisms are in place including by sharing best practices and common standards;

21. Intends to follow up the Conference on the Democratic oversight of Intelligence Services in the European Union, held on 28 and 29 May 2015, and to continue its efforts aimed at ensuring the sharing of best practices on intelligence oversight, in close coordination with national parliaments; welcomes the joint concluding remarks of the co-chairs of this conference declaring their intention to convene a follow-up conference in two years' time;

22. Considers that the existing tools for cooperation among oversight bodies, for instance the European Network of National Intelligence Reviewers (ENNIR), should be supported and their use should be increased, possibly by making use of the potential of IPEX for the exchange of information between national parliaments, in compliance with its scope and technical capacity;

23. Reiterates its call for the suspension of the Terrorist Finance Tracking Programme (TFTP) agreement;

24. Stresses that a common definition of 'national security' is needed for the EU and its Member States to ensure legal certainty; notes that the lack of a clear definition allows for arbitrariness and abuses of fundamental rights and the rule of law by executives and intelligence communities in the EU;

25. Encourages the Commission and the Member States to introduce sunset and extension provisions in legislation that allows the collection of personal data or the surveillance of European citizens; stresses that such provisions are essential safeguards for ensuring that

an instrument which is invasive for privacy is regularly scrutinised as regards its necessity and proportionality in a democratic society;

Rebuilding trust

26. Stresses that a healthy EU-US relationship remains absolutely vital for both partners; notes that revelations about surveillance have undermined public support for the relationship, and stresses that measures need to be taken to ensure that trust is rebuilt, in particular in the light of the current urgent need for cooperation on a large number of geopolitical issues of common concern; emphasises in this context that a negotiated solution between the US and the EU as a whole, respecting fundamental rights, needs to be found;

27. Welcomes the recent legislative and judicial decisions taken in the US to limit mass surveillance by the NSA, including the adoption of the USA Freedom Act in Congress without any amendments as the result of bicameral and bipartisan compromise, and the ruling of the Second Circuit Court of Appeals on the NSA's telephone record collection programme; regrets, however, the fact that these decisions focus mainly on US persons while the situation of EU citizens remains the same;

28. Considers that any decision to use surveillance technology should be based on a thorough assessment of necessity and proportionality; welcomes the results of the SURVEILLE research project, which offers a methodology for assessing surveillance technologies taking legal, ethical and technological considerations into account;

29. Emphasises that the EU should contribute to the development of international standards/principles at UN level, in line with the UN International Covenant on Civil and Political Rights, in order to create a global framework for data protection, including specific limitations with regard to collection for national security purposes;

30. Is convinced that only if credible norms are established at the global level can a 'surveillance arms race' be avoided;

Private companies

31. Welcomes the initiatives of the private ICT sector in terms of developing cryptographic security solutions and internet services that improve privacy; encourages the continued development of user-friendly application settings helping customers manage what information they share with whom and how; notes that various companies have also announced plans to enable end-to-end encryption in response to mass surveillance revelations;

32. Reiterates that under Article 15(1) of Directive 2000/31/EC Member States shall not impose a general obligation on providers of transmission, storage and hosting services to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity; recalls in particular that the CJEU, in its Judgments C-360/10 and C-70/10, rejected measures for the 'active monitoring' of almost all users of the services concerned (internet access providers in one case, a social network in the other) and specified that any injunction requiring a hosting services provider to undertake general monitoring shall be precluded;

33. Welcomes the publication of transparency reports by IT and telecommunications companies about government demands for user data; calls on the Member States to publish statistics on their requests to private companies for private user information;

The TFTP agreement

34. Is disappointed that the Commission disregarded Parliament's clear call for the suspension of the TFTP agreement, given that no clear information was given to clarify whether SWIFT data would have been accessed outside TFTP by any other US government body; intends to take this into account when considering giving consent to future international agreements;

Other personal data exchange with third countries

35. Stresses its position that all agreements, mechanisms and adequacy decisions for exchanges with third countries involving personal data require rigorous monitoring and immediate follow-up action by the Commission as the guardian of the Treaties;

36. Welcomes the EU-US Riga statement of 3 June 2015 on enhancing transatlantic cooperation in the area of freedom, security and justice, in which the signatories committed to enhancing the implementation of the US-EU Mutual Legal Assistance Agreement (MLAT), to concluding its review as foreseen by the Agreement, and to conducting workshops to discuss the issues concerned with the competent national authorities; underlines that MLATs are the instrument on the basis of which law enforcement authorities of Member States should cooperate with authorities of third countries; calls, in this regard, on the Member States and the US government to adhere to the above-mentioned commitments with a view to a swift conclusion of the US-EU MLAT review;

37. Calls on the Commission to report to Parliament by the end of 2015 on the gaps identified in different instruments used for international data transfers as regards access by law enforcement and intelligence services of third countries, and on the means to address those gaps so as to ensure the continuity of the required adequate protection of EU personal data transferred to third countries;

Protection of the rule of law and the fundamental rights of EU citizens/enhanced protection for whistleblowers and journalists

38. Considers that EU citizens' fundamental rights remain in danger and that too little has been done to ensure their full protection in case of electronic mass surveillance; regrets the limited progress in ensuring the protection of whistleblowers and journalists;

39. Deplores the fact that many mass and large-scale intelligence programmes seem to be also driven by the economic interests of the companies that develop and run those programmes, as was the case with the ending of the NSA's targeted 'Thinthread' programme and its replacement by the large-scale surveillance programme 'Trailblazer', which was outsourced to SAIC in 2001;

40. Reiterates its serious concern regarding the work within the Council of Europe's Cybercrime Convention Committee on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 (Budapest Convention) with regard to transborder access to stored computer data with consent or where publicly available, and opposes any conclusion of an additional protocol or guidance intended to broaden the scope of this

provision beyond the current regime established by this Convention, which is already a major exception to the principle of territoriality as it could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLA agreements or other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process; underlines that the EU has exercised its competence in the area of cybercrime and that the prerogatives of both the Commission and Parliament should therefore be respected;

41. Regrets that the Commission has not responded to Parliament's request to conduct an examination as to a comprehensive European whistleblower protection programme, and calls on the Commission to present a communication on this subject, by the end of 2016 at the latest;

42. Welcomes the resolution adopted on 23 June 2015 by the Parliamentary Assembly of the Council of Europe on 'Improving the protection of whistleblowers', and in particular its point 9 on the importance of whistleblowing to ensure that legal limits placed on surveillance are respected, and its point 10 calling on the EU to enact whistle blower protection laws, also covering employees of national security or intelligence services and of private firms working in this field, and to grant asylum, as far as possible under national law, to whistleblowers threatened by retaliation in their home countries, provided their disclosures qualify for protection under the principles advocated by the Assembly;

43. Stresses that mass surveillance severely undermines the professional confidentiality privilege of regulated professions including doctors, journalists and lawyers; underlines in particular the rights of EU citizens to be protected against any surveillance of confidential communications with their lawyers which would violate the Charter of Fundamental Rights of the European Union, notably Articles 6, 47 and 48 thereof, and Directive 2013/48/EU on the right of access to a lawyer; calls on the Commission to present a communication on the protection of confidential communications in professions with legal professional privilege, by the end of 2016 at the latest;

44. Calls on the Commission to prepare guidelines for Member States on how to bring any instruments of personal data collection for the purpose of the prevention, detection, investigation and prosecution of criminal offences, including terrorism, in line with the judgments of the CJEU of 8 April 2014 on data retention (Cases C-293/12 and C-594/12) and of 6 October 2015 on Safe Harbour (Case C-362/14); points in particular to paragraphs 58 and 59 of the data retention judgment and to paragraphs 93 and 94 of the Safe Harbour judgment, which clearly demand a targeted approach for data collection rather than a 'full take';

45. Highlights the fact that the most recent case law, and in particular the judgment of the CJEU of 8 April 2014 on data retention, clearly sets out as a legal requirement the demonstration of necessity and proportionality for any measures involving the collection and use of personal data potentially interfering with the right of respect for private and family life and the right to data protection; finds it regrettable that political considerations often undermine compliance with these legal principles in the decision-making process; calls on the Commission to ensure, as part of its Better Regulation agenda, that all EU legislation is of high quality, complies with all the legal standards and case law, and is in line with the EU Charter of Fundamental Rights; recommends that the impact assessment of all law-enforcement and security measures involving the use and collection of personal data always includes a necessity and proportionality test;

European strategy for greater IT independence

46. Is disappointed by the lack of action by the Commission to follow up the detailed recommendations made in the resolution for increasing IT security and online privacy in the EU;

47. Welcomes the steps taken so far to strengthen Parliament's IT security, as outlined in the action plan on EP ICT Security prepared by DG ITEC; asks for these efforts to be continued and the recommendations made in the resolution fully and swiftly carried out; calls for fresh thinking and, if necessary, legislative change in the field of procurement to enhance the IT security of the EU institutions; calls for the systematic replacement of proprietary software by auditable and verifiable open-source software in all the EU institutions, for the introduction of a mandatory 'open-source' selection criterion in all future ICT procurement procedures, and for efficient availability of encryption tools;

48. Strongly reiterates its call for the development, within the framework of new initiatives such as the Digital Single Market, of a European strategy for greater IT independence and online privacy that will boost the IT industry in the EU;

49. Intends to submit further recommendations in this field following its conference on 'Protecting on-line privacy by enhancing IT security and EU IT autonomy', scheduled for the end of 2015, which will build on the findings of the recent STOA study on the mass surveillance of IT users;

Democratic and neutral internet governance

50. Welcomes the Commission's aim to make the EU a reference player for internet governance, as well as its vision of a multi-stakeholder model for internet governance as reiterated at the Global Multistakeholder Meeting on the Future of Internet Governance (NETMundial) held in Brazil in April 2014; looks forward to the outcome of the ongoing international work in this field, including in the framework of the Internet Governance Forum;

51. Warns against the obvious downward spiral for the fundamental right to privacy and personal data protection occurring when every bit of information on human behaviour is considered to be potentially useful in combating future criminal acts, necessarily resulting in a mass surveillance culture where every citizen is treated as a potential suspect and leading to the corrosion of societal coherence and trust;

52. Intends to take account of the findings of the in-depth research by the Fundamental Rights Agency concerning the protection of fundamental rights in the context of surveillance, and in particular regarding the current legal situation of individuals with respect to the remedies available to them in relation to the practices concerned;

Follow-up

53. Instructs its Committee on Civil Liberties, Justice and Home Affairs to continue to monitor developments in this field and the follow-up to the recommendations made in the resolution;

o

o o

54. Instructs its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States, and the Council of Europe.