US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

2013/2188(INI) - 21/02/2014 - Committee report tabled for plenary, single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the own-initiative report by Claude MORAES (S&D, UK) 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.

The report noted that in comparison to actions taken both by EU institutions and by certain EU Member States, the European Parliament has taken very seriously its obligation to shed light on the revelations on the indiscriminate practices of mass surveillance of EU citizens and instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter.

Main findings of the report:

Members considered that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, admissions by authorities, and the insufficient response to these allegations, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner.

They pointed specifically to:

- US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN);
- systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), etc.

They emphasised that trust has been profoundly shaken between the two transatlantic partners. In order to rebuild trust in all these dimensions, an immediate and comprehensive response plan comprising a series of actions which are subject to public scrutiny is needed.

Noting that several governments claim that these mass surveillance programmes are necessary to combat terrorism, Members stated that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes. The report strongly rejected the notion that all issues related to mass surveillance programmes are purely a matter of national security and therefore the sole competence of Member States. Discussion and action at EU level are not only legitimate, but also a matter of EU autonomy.

The US authorities and the EU Member States are called upon to prohibit blanket mass surveillance activities.

Members States are called upon to:

- comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny;
- immediately fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law.

The Commission is called upon to:

- carry out, before July 2014, an assessment of the applicability of Regulation (EC) No 2271/96 to cases of conflict of laws on transfers of personal data;
- present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles. In this respect, the US authorities are urged to put forward a proposal for a new framework for transfers of personal data from the EU to the US which meets Union law data protection requirements and provides for the required adequate level of protection;
- present, by December 2014, a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities, and concrete recommendations based on the absence of a general data protection law in the US;
- engage with the US administration in order to establish a legal framework providing for a high level of protection of individuals with regard to the protection of their personal data when transferred to the US and ensure the equivalence of EU and US privacy frameworks;
- conduct, before the end of 2014, an in-depth assessment of the existing Mutual Legal Assistance Agreement;
- react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy;
- present, by December 2014, a proposal for an EU security clearance procedure for all EU office holders;
- present draft legislation to ban the use of backdoors by law enforcement agencies;
- present, by January 2015 at the latest, an Action Plan to develop greater EU independence in the IT sector, including a more coherent approach to boosting European IT technological capabilities (including IT systems, equipment, services, cloud computing, etc);
- put forward by December 2014, legislative proposals to encourage software and hardware manufacturers to introduce more security and privacy by design and by default features in their products, including by introducing disincentives for the undue and disproportionate collection of mass personal data and legal liability on the part of manufacturers for unpatched known vulnerabilities, faulty or insecure products or the installation of secret backdoors enabling unauthorised access to and processing of data;

Members called for the setting up of a High-Level Group to propose, in a transparent manner and in collaboration with parliaments, recommendations and further steps to be taken for enhanced democratic oversight, including parliamentary oversight, of intelligence services and increased oversight collaboration in the EU, in particular as regards its cross-border dimension.

Lastly, the report stressed the decision to launch A European Digital Habeas Corpus - protecting fundamental rights in a digital age with the following 8 actions as well as a timetable to be respected. The implementation of which it will oversee, inter alia:

- the adoption of the Data Protection Package in 2014;
- the conclusion of the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens;
- the suspension of Safe Harbour until a full review has been conducted and current loopholes are remedied;
- the suspension of 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;
- the enhanced protection for whistleblowers;
- the development of a European strategy for greater IT independence.