Background

Q&A on Parliament's inquiry into mass surveillance of EU citizens

[10-03-2014 - 16:34]

The plenary vote on Parliament's inquiry into mass surveillance of EU citizens concludes a 6-month investigation by its Civil Liberties Committee. MEPs looked into alleged spying by the US and some EU member states, assessed its impact on EU citizens' rights (e.g. data protection, freedom of expression, presumption of innocence and effective remedy), recommended ways to prevent further breaches, explored redress mechanisms and suggested how to improve the IT security of EU institutions.

The committee started work in September 2013, on a mandate granted to it by Parliament as a whole on 4 July 2013, following the revelations by former US National Security.Agency contractor Edward Snowden.

Its conclusions were summed up in a report approved by the committee on 12 February and will be put to a vote by Parliament as a whole on 12 March.

The resolution was drafted by MEP Claude Moraes (S&D, UK).

Contact

Natalia DASILVA
BXL: (+32) 2 28 44301
STR: (+33) 3 881 73661
PORT: (+32) 498 98 39 85
EMAIL: libe-press@europarl.europa.eu
TWITTER: EP_Justice

Isabel Teixeira NADKARNI
BXL: (+32) 2 28 32198
STR: (+33) 3 881 76758
PORT: (+32) 498 98 33 36
EMAIL: libe-press@europarl.europa.eu
TWITTER: EP_Justice

How could mass surveillance affect EU-US deals?

Parliament's consent to the final Transatlantic Trade and Investment Partnership (TTIP) deal with the US “could be endangered as long as blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not fully stopped”, MEPs say. It should therefore withhold its consent to the TTIP agreement unless it fully respects EU fundamental rights, the resolution stresses, adding that data protection should be ruled out of the trade talks.

MEPs also call for the "immediate suspension" of the Safe Harbour privacy principles (voluntary data protection standards for non-EU companies transferring EU citizens’ personal data to the US). These principles “do not provide adequate protection for EU citizens” say MEPs, urging the US to propose new personal data transfer rules that meet EU data protection requirements.

The Terrorist Finance Tracking Programme (TFTP) deal should also be suspended until allegations that US authorities have access to EU citizens’ bank data outside the agreement are clarified, MEPs insist.

What do MEPs say about mass surveillance allegations in EU countries?

The resolution to be voted by the full House on 12 March also looks at the surveillance activities within the EU, pointing out the "lack of control and effective oversight" by certain EU member states over their intelligence communities and their cooperation and involvement with US surveillance programmes.

The **UK, France, Germany, Sweden, the Netherlands and Poland** should clarify the allegations of mass surveillance activities and their compatibility with EU laws, including:

- mass surveillance of cross border telecommunications,
- untargeted surveillance on cable-bound communications,
- potential agreements between intelligence services and telecom companies as regards access and exchange of personal data and access to transatlantic cables, and
- US intelligence personnel and equipment on EU territory without oversight on surveillance operations.

Other EU countries, in particular those participating in the "9-eyes" (UK, **Denmark,** France and the Netherlands) and "14-eyes" arrangements (those countries plus Germany, **Belgium, Italy, Spain** and Sweden) are also urged to review their national laws and practices governing the activities of intelligence services, so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny and that they comply with fundamental rights obligations.

MEPs also question the compatibility of some member states' "massive economic espionage activities" with the EU internal market and competition law.

UK GCHQ intelligence agency

The resolution mentions the systems of the UK intelligence agency Government Communications Headquarters (GCHQ), such as the "Tempora" programme. It refers to the allegations of 'hacking' or tapping into the Belgian telecom firm Belgacom systems by GCHQ and also recalls that former columnist from the Guardian, Glenn Greenwald, told the inquiry that the NSA and GCHQ had targeted SWIFT networks.

MEPs call on the UK to revise its current legal framework, which is made up of a "complex interaction" between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000.

MEPs also take note of the detention of Greenwald's partner David Miranda and the seizure of the material in his possession by the UK authorities under the UK Terrorism Act (and also the request made to the Guardian newspaper to destroy or hand over the material). "This constitutes a possible serious interference with the right of freedom of expression and media freedom", they say, adding that "legislation intended to fight terrorism could be misused in such instances".

Call on the Netherlands to be cautious

One of the world's biggest Internet Exchange Points is located in Amsterdam (AMS-IX). MEPs calls on the Netherlands to refrain from extending the powers of its intelligence services in such a way as to enable untargeted and large-scale surveillance also to be performed on cable-bound communications of innocent citizens. They also ask for caution regarding the presence and operation of US intelligence personnel on Dutch territory.

Refrain from bilateral "anti-spying" deals with the US

The resolution deems bilateral "anti-spying" arrangements concluded or under negotiation between some EU countries (the UK, France and Germany) and the US as "counterproductive and irrelevant, due to the need for a European approach to this problem". MEPs ask member states for more information on developments on an "EU-wide mutual no-spy arrangement".

Does the resolution suggest any measures to protect whistle blowers?

Yes. MEPs call on the EU to establish an "effective and comprehensive European whistle blower protection programme", paying particular attention to the complexity of whistle blowing in the field of intelligence. They also call on EU countries to "thoroughly examine the possibility of granting whistle blowers international protection from prosecution".

MEPs also propose a "European Digital Habeas Corpus", which includes action to ensure enhanced protection for whistle blowers.

Is Edward Snowden mentioned in the resolution?

The resolution mentions Edward Snowden's name once."The revelations based on documents leaked by the former NSA contractor Edward Snowden put political leaders under the obligation to address the challenges of overseeing and controlling intelligence agencies in surveillance activities and assessing the impact of their activities on fundamental rights and the rule of law in a democratic society", it says.

On 7 March 2014, Mr Snowden gave written replies to a set of questions sent by MEPs to his lawyers. The content of his replies was debated by Civil Liberties MEPs on 10 March 2014, as part of the inquiry activities.

What is the "digital new deal" that MEPs propose?

The resolution calls for a “digital new deal” in Europe to boost its IT independence. This strategy should foresee the allocation of adequate resources at national and EU level. The ultimate goal is to boost the IT industry and to allow European companies to exploit the EU's privacy competitive advantage.

Trust in US cloud computing and cloud data storage providers has been damaged by surveillance practices, MEPs note. They suggest that Europe develops its own clouds and IT solutions to ensure a high standard of personal data protection. They also note that by 2016, the cloud market is likely to be worth $207 billion a year, double its 2012 value.

The resolution recognises that there is an acute vulnerability in the IT security of EU institutions. It therefore asks for a review and assessment of technical capabilities, including possible open source software, the use of cloud storage by the EP, impact of increased use of mobile tools and a plan for more use of encryption technologies.

How has the Civil Liberties Committee organised its work?

The Civil Liberties Committee inquiry began in September 2013. A total of 16 hearings have been held since then. MEPs heard journalists unveiling the case and discussed with several other actors the allegations of NSA tapping into the SWIFT data used in the TFTP programme, the allegations of “hacking” / tapping into the Belgacom systems by GCHQ and the role of parliamentary oversight of intelligence services at national level, among other issues. They also heard US civil society, US congressman, former whistle blowers, intelligence officers and representatives from companies such as Microsoft, Google and Facebook.

A Civil Liberties Committee delegation also went to Washington DC on 28-30 October 2013 to gather further insights into the allegations of mass surveillance of EU citizens by the NSA and its impact on EU-US cooperation. Members of the delegation met representatives of main federal departments involved in the NSA’s mass surveillance activities, Chairman of the House Select Committee on Intelligence Mike Rogers, and National Security Council Senior Director for European Affairs, Dr Karen Donfried, as well as private stakeholders and legal experts and academics.

They also met Congressman Jim Sensenbrenner, author of the Patriot Act 2001, before he spoke before the Committee inquiry on 11 November 2013, in Brussels.

Did anyone refuse to appear before the inquiry?

In the course of the Civil Liberties Committee hearings, MEPs heard privacy and IT security experts, whistle blowers, representatives of Google, Facebook and Microsoft, journalists, lawyers and members of national committees conducting oversight of intelligence services (the full list is available on pages 54-60 of the draft resolution).

However, a number of experts declined to take part in the committee's public hearings, such as US National Security Agency Director Keith Alexander (although he met Mr Moraes and Elmar Brok (EPP, DE) on 29 October 2013 in Washington DC), US Representative to the EU Robert A. Wood, GCHQ Director Sir Ian Lobban, representatives of French, German and Polish intelligence services and representatives of Yahoo, Amazon, Orange, British Telecom and Vodafone. The Dutch Ministers of the Interior and Justice also declined to participate in the hearings (for further details, see pages 61 and 62 of the draft resolution).

What happens next?

MEPs propose a "priority plan" to be implemented in the months and years to come among EU institutions, member states, EU citizens, national parliaments and the IT industry.

The so-called "European Digital Habeas Corpus - protecting fundamental rights in a digital age" includes the following 8 recommendations / actions for the next Parliament (2014-2019):

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens, including in the event of data transfers from the EU to the US for law enforcement purposes;

Action 3: Suspend Safe Harbour until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with the highest EU standards;

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

Action 5: Evaluate any agreement, mechanism or exchange with third countries involving personal data in order to ensure that the right to privacy and to the protection of personal data is not violated due to surveillance activities, and take necessary follow-up actions;

Action 6: Protect the rule of law and the fundamental rights of EU citizens, (including from threats to the freedom of the press), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations), as well as ensuring enhanced protection for whistleblowers;

Action 7: Develop a European strategy for greater IT independence (a ‘digital new deal’ including the allocation of adequate resources at national and EU level) in order to boost IT industry and allow European companies to exploit the EU privacy competitive advantage;

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

Parliament undertakes to act as the "EU citizens’ rights advocate", with the following timetable to monitor implementation:

• Spring 2014: a formal call on the European Council to include the ‘European Digital Habeas Corpus - protecting fundamental rights in a digital age’- in the guidelines to be adopted under Article 68 TFEU;

• April 2014-March 2015: a monitoring group based on the Civil Liberties inquiry team responsible for monitoring any new revelations concerning the inquiry's mandate and scrutinising the implementation of this resolution;

• July 2014 onwards: a standing oversight mechanism for data transfers and judicial remedies within the competent committee;

• Autumn 2014: a commitment that the ‘European Digital Habeas Corpus - protecting fundamental rights in a digital age’ and related recommendations will serve as key criteria for the approval of the next Commission;

• 2014: a conference bringing together high-level European experts in the various fields conducive to IT security (including mathematics, cryptography and privacy-enhancing technologies) to help foster an EU IT strategy for the next legislative term;

• 2014-2015: a Trust/Data/Citizens’ Rights group to be convened on a regular basis between the European Parliament and the US Congress, as well as with other committed

third-country parliaments, including that of Brazil;

• 2014-2015: a conference with the intelligence oversight bodies of European national parliaments.