



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 12 September 2013

13547/13

**PE 395
JAI 762
JUR 462
PESC 1069
JAIEX 73
RELEX 801
DATAPROTECT 126**

NOTE

from: General Secretariat of the Council
to: Delegations

Subject: Summary of the hearing of the Civil Liberties, Justice and Home Affairs
Committee of the European Parliament, held in Brussels on 5 September 2013:
Inquiry on Electronic Mass Surveillance of EU Citizens

The meeting was chaired by Mr Aguilar (S&D, ES) and Ms in 't Veld (ALDE, NL).

Mr Aguilar explained that the report on the Inquiry on Electronic Mass Surveillance of EU Citizens had to be prepared in the next 4 months, voted on by LIBE in December and by the Plenary in January 2014. He regretted that a video conference with Mr Greenwald could not take place at this meeting but said that it could be arranged for a further meeting.

SESSION I

Exchange of views with the journalists unveiling the case and having made public the facts

The first invited speaker, Mr FOLLOROU of the French newspaper *Le Monde*, presented his inquiry into massive storage and interception of personal data in France, carried out by DGSE, the Directorate-General for External Security of the French state, which has a mandate to operate outside French territory.

The main issue at stake was who had access to the data stored. His investigation showed that various French law enforcement agencies were able to connect directly to this database (financial crime investigation services, anti-terrorism, customs) in order to access data on individuals as well as metadata. Metadata actually made it possible to reconstruct the life of an individual.

Unfortunately there was little interest in France in this question, as political stakeholders seem to believe it was normal for a state to carry out such activities. In his view there was a clear lack of scrutiny and many questions remained unanswered. He thanked the EP for taking this issue seriously, and stressed it was a basic question of democracy: technologies could always be misused and proper controls must be established. He emphasised that these activities had been to a large extent "outside the law but not illegal."

Jacob APPELBAUM, investigative journalist, software developer and computer security researcher with the Tor Project

The second invited speaker, Mr Appelbaum, stated that US technology companies had mechanisms in their systems which allowed intelligence services to intercept data, assisting the PRISM programme. He pointed out that the NSA was not bound by any European legislation and in any case cared little what these laws said. That being so, wiretapping could happen without any judicial oversight being required. He encouraged the EP to get all the relevant dossiers from the various intelligence services. On the question of the purpose of the surveillance systems, he asserted that having control was the main purpose for the existence of these systems. He confirmed that the surveillance systems were also used for economic espionage. Moreover, he argued that the systems were also used for military purposes and political prosecution, notably resulting in drone attacks on individuals in third countries.

On the issue of the right balance between security and respect for civil rights, he pointed out that communication networks were, by their nature, not secure; in fact various government agencies collaborated against their own citizens. In addition, he estimated that USD 52.6 billion were available annually for intelligence services to develop and maintain their surveillance systems. He also confirmed that intelligence services from the Five Eyes countries (United Kingdom, United States of America, Canada, Australia and New Zealand) collaborated to circumvent national legislation. Furthermore, he affirmed that the NSA also intercepted European control systems, such as hospitals and energy plants.

He disagreed with the claim that this was a post- 9/11 issue, because the NSA had already been collecting data from US citizens for a long time, most of the time legally, due to the existence of the Patriot Act. He confirmed that surveillance equipment was being exported to repressive regimes in order to locate political and human rights activists.

Alan RUSBRIDGER, Editor-in-Chief of Guardian News and Media (via videoconference)

Mr Rusbridger said that it was important to understand that entire populations were put under unprecedented electronic surveillance, which required a proper public debate. However the facts on which debate could be based were still missing, and states were clearly reluctant to reveal such information.

He explained the circumstances surrounding Snowden's revelations to Mr Greenwald, a journalist and lawyer linked to the Guardian. Various legal issues quickly arose across different jurisdictions worldwide (UK, USA, Hong Kong), the material obtained carried extensive security risks and required extensive editing. He stressed that the Guardian had acted responsibly. He spoke about the detention of David Miranda, who was part of the Guardian team, on the basis of terror legislation, and legal threats made by the British government to retrieve and destroy material. On this point, he explained that the US laws gave more robust protection to journalists than legislation in Europe, since prior restraint of publishing was not possible in the US. Such journalism in the public interest of course generated enormous legal bills and required partnerships with NY Times and La Repubblica.

In the last 15 years partnership between states and corporations had been created, involving massive harvesting of electronic devices enabling surveillance of individuals, without any consent ever having been given by the people for such activities. Even President Obama recognised the need to have a debate on this issue; however, this was not possible without information. Of course, a balance had to be found between security, privacy, freedom of speech and freedom of association, but for the time being only the security aspects and arguments seemed to be heard. Technical experts will always be ahead of laws and achieving meaningful oversight was very important.

In reply to questions, Mr Rusbridger said it was of the utmost importance to preserve investigative journalism, as threats of the use of anti-terrorist legislation and restraining orders had a chilling effect. He called for the protection of whistle-blowers and journalists. Journalism itself was threatened by such surveillance activities. It was also questionable whether existing special courts and parliamentary oversight could provide effective and meaningful control. Lawmakers should protect journalism.

SESSION II

Follow-up of the Temporary Committee on the ECHELON Interception System

Carlos COELHO (MEP), former Chair of the Temporary Committee on the ECHELON Interception System

Mr Coelho (EPP, PT) explained that the Echelon inquiry at the time proved that the Five Eyes had a global network to intercept communications and share the information retrieved. After the end of the Cold War the US reoriented its spy network from military to civil and commercial targets. The report proved such activities, unfortunately it was adopted just 2 months before 9/11, and for obvious reasons of solidarity with the US nobody was willing to confront the US on the issue of spying on its own allies. He stressed that it was the EP's role to debate these issues and make political recommendations. Many Echelon report recommendations were still valid.

Gerhard SCHMID (former MEP and Rapporteur of the ECHELON report 2001)

Mr Schmid, former MEP and rapporteur on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), emphasised that there was still work to be done in order to understand the exact details of the working of interception systems. Only when the capabilities of these systems were fully understood could political conclusions be drawn. He recommended carefully checking information sources and their plausibility. Furthermore, it was important to verify the origin of these sources. He recommended using the expertise of the US Congress and the British Parliament. He stressed the importance of clarifying the existing legal framework regarding extend intelligence services' use of interception systems.

He recommended fully studying the technical processes behind interception systems and surveillance equipment. With regard to the technical aspect, he recommended examining which companies put what machines on the market and inviting those companies to discuss what could be done with regard to data mining. He also pointed out that that the NSA outsourced approximately 70% of its operations to private companies, which raised security concerns. He doubted national governments or national parliaments would share their information with the EP. He said investigative journalists could be helpful to give hints and tips.

With reference to the security within the EU institutions and the bugging of the EU representation in Washington DC, he said that not enough had been done to prevent spying within the EU institutions. With regard to the legal aspect, he stressed how important it was that EU law was in alignment with national legislation. He believed that national legislation could be used as a safeguard for EU legislation. On the matter of how data were processed, Schmid argued that data processing could be outsourced to American companies, meaning that American legislation applied to these metadata.

Duncan CAMPBELL, investigative journalist and author of the STOA report "Interception Capabilities 2000"

Mr Campbell said that in the past 10 years a number of revelations had unveiled the extraordinary interception capabilities possessed by the US and the UK, along with Canada, New Zealand and Australia. The Snowden revelations confirmed the existence of various surveillance programmes which were in place and functioning. He showed various photos of facilities around the world used for communications collection. The input to the systems was fed by satellites and direct access to optical cables (coerced or voluntary), as well as interception centres around the world. Metadata provided the map of virtually all humanity; however, the protection offered by the US constitution of course applies only to US citizens, not to European citizens.

In his concluding remarks, Rapporteur Moraes (S&D, UK) explained he was fairly optimistic about the next four months and said that he intended to prepare the report for the vote in the Plenary in January 2014. It was too soon to draw any conclusions, but he said he felt ambitious and that much could be achieved through this inquiry. He would certainly built on the Echelon recommendations.

Next meeting(s)

- ***12 September 2013, 10.00 – 12.30 (Strasbourg)***