ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Committee on Civil Liberties, Justice and Home Affairs
- The Secretariat -

Background Note

Introduction

This note presents a general description of the different issues made public by the media:

i) Electronic surveillance and interception of communications data by the US authorities (PRISM Programme);

ii) Electronic surveillance programmes implemented by some Member States;

iii) Electronic surveillance of EU institutions and Member States Embassies by the US authorities.

I - The European Parliament resolution of 4 July 2013

1. On 4 July 2013, the European Parliament adopted its Resolution on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy.[1] In the Resolution, the European Parliament instructed *its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter in collaboration with national parliaments and the EU-US expert group set up by the Commission and to report back by the end of the year, by:*

(a) gathering all relevant information and evidence from both US and EU sources (fact-finding);

(b)investigating the alleged surveillance activities of US authorities as well as any carried out by certain Member States (mapping of responsibilities);

(c)assessing the impact of surveillance programmes as regards: the fundamental rights of EU citizens (in particular the right to respect for private life and communications, freedom of expression, the presumption of innocence and the right to an effective remedy); actual data protection both within the EU and for EU citizens outside the EU, focusing in particular on the effectiveness of EU law in respect of extraterritoriality mechanisms; the safety of the EU in the era of cloud computing; the added value and proportionality of such programmes with regard to the fight against terrorism; the external dimension of the area of freedom, security and justice

[1] P7-TA-PROV(2023)0322.

(assessing the validity of adequacy decisions for EU transfers to third countries, such as those carried out under the Safe Harbour Agreement, international agreements and other legal instruments providing for legal assistance and cooperation) (damage and risk analysis);

(d) exploring the most appropriate mechanisms for redress in the event of confirmed violations (administrative and judicial redress and compensation schemes);

(e) putting forward recommendations aimed at preventing further violations, and ensuring credible, high-level protection of EU citizens' personal data via adequate means, in particular the adoption of a fully-fledged data protection package (policy recommendations and law-making);

(f) issuing recommendations aimed at strengthening IT security in the EU's institutions, bodies and agencies by means of proper internal security rules for communication systems, in order to prevent and remedy unauthorised access and the disclosure or loss of information and personal data (remedying of security breaches).

II - Electronic surveillance and interception of electronic communications by the US NSA - The PRISM Programme and the mass and secret surveillance of EU electronic communications

2. On 6 June 2013, The Guardian[2] and Washington Post[3] newspapers published articles revealing that an electronic surveillance system called PRISM had been systematically used by intelligence services in the United States since 2007. The top-secret document leaked to journalists was reportedly used to train intelligence operatives on the functions and scope of the PRISM programme.

3. According to information published, the NSA would have accessed communications and stored data in the servers of nine IT companies (designated as 'special source operations'): Google, Microsoft, Facebook, Yahoo, Skype, Apple, Paltalk, Youtube and AOL. The collected data on 'targeted foreign users' include, among others, email, chat, videos, photos, file transfers, social networking data and 'other special requests'. No further details have been reported regarding the exact nature and scope of this data. Media sources state that the NSA does not appear to have direct (so-called 'root') access to user data, and suggest the handling of requests differs from company to company terminal. However this is cannot be confirmed in the present state of affairs.

4. The US Director of National Intelligence reacted the same day and published a statement[4] criticising the leak and clarifying that the object of this search is not to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States. The Director of National Intelligence stated that the request "*involves extensive procedures, specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targeted, and*

[2] http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data
[3] http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-usinternet-companies-in-broad-secret-program/2013/06/%2006/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
[4] http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa

that minimizes the acquisition, retention and dissemination of incidentally acquired information about U.S. persons." He also alleged that "*information collected under this program is among the most important and valuable foreign intelligence information the US collects and is used to protect the US nation from a wide variety of threats. The unauthorized disclosure of information about this important and entirely legal program was qualified as reprehensible and risking important protections for the security of Americans*".

5. Several companies involved in the Programme (e.g. Apple, Google, Facebook) have first denied having been subjected to the injunctions of the US NSA and disclosed information and data stored by them. Subsequently, after media revealed the issue, they have informed that in order to comply with NSA requests, they should have disclosed information of several thousands of their users (eg: Apple received 4000-5000 requests between December 2012 and May 2013 affecting 9000-1000 users' accounts, similar data have been disclosed by Microsoft or Facebook).

6. In parallel to PRISM, media have also revealed that in April 2013, NSA requested a major US telecom provider (Verizon) to disclose the telephone records of millions of its US customers. Under the terms of a blanket order, the numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls (metadata). The contents of the call conversation itself are not covered. This disclosure would have been based on Section 215 of Patriot Act which requires a judicial order. In a letter on 3 July 2013 to the U.S Congress, the Director of National Intelligence admitted that his first statement of 6 June 2013 (§4 *supra*) was erroneous because he had omitted to refer to Section 215 of the Patriot Act for the collection of metadata of US citizens from the US telecom provider.

III - Surveilloance Programmes in EU Member States - Preliminary Information

7. News reports[5] have also revealed that the United Kingdom's Government Communications Headquarters GCHQ would have developed a programme called TEMPORA which would have enabled it to tape into undersea transatlantic cable where it lands on British shores carrying data from/to Western Europe from telephone exchanges and internet servers in North America and to store internet content for three days and metadata for up 30 days. This would have been done under secret agreements with commercial companies, described in one document as "intercept partners"[6]. The 2000 Regulation of Investigatory Powers Act (RIPA)[7] provides that the tapping of defined targets is to be authorised by a warrant signed by the Home Secretary or the Foreign Secretary. However, a clause allows the Foreign Secretary to sign a certificate for the interception of broad categories of material, as long as one end of the monitored communications is abroad[8].

8. According to media, by May 2012 300 analysts from GCHQ, and 250 from the NSA, had been assigned to sift through the flood of data.

[5] http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa/print
http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet

[6] Some companies would have been paid for the cost of their co-operation and GCHQ would have gone to great lengths to keep their names secret (The Guardian, 21 June 2013)

[7] http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

[8] Regulation of Investigatory Powers Act (RIPA) 2000, Section 7(2)(b).

9. It appears that other Member States would also access transnational electronic communications without a regular warrant but on the basis of special courts, share data with other countries (Sweden), while other may enhance their surveillance capabilities (the Netherlands, Germany, Spain). Concerns have also been expressed in other Member States in relation to the interception powers of secret services (Poland). The French media "Le Monde" published the 4 July 2013[9] that the *Direction générale de la sécurité extérieure (DGSE)* would systematically collect signals data issued by computers and telephones in France and the flows between France and abroad. According to the media, the information collected would be stocked for years and would be accessed by different departments such as the anti-money laundering departments (Tracfin).

IV - Electronic surveillance of EU Institutions and Member States Embassies by the US Authorities

10. On 29 June 2013[10], German newspaper Der Spiegel revealed that US authorities had been spying EU institutions in the EU as well as the EU delegations in Washington and New York. US authorities declined to comment. It is not clear whether or not this secret surveillance have been carried out within the framework of PRISM and FISA or it is rather espionage activity.[11]

V - The EU-US Expters Group

11. At the EU-US Justice and Home Affairs Ministerial of 14 June 2013, the Commission and the US agreed to set up a transatlantic group of experts to clarify matters with regard to the US PRISM programme. At COREPER on 18 July Member States agreed on the establishment of an ad-hoc EU-US Working Group on data protection. The objective of the group is to understand the process and facts in order to assess the proportionality of the programme. The EU side is being co-chaired by the Council Presidency, the Commission and is also composed of the Counter-Terrorism Coordinator, the EEAS, a member of the Article 29 Working Group and Member States experts[12].The group has met on 8/9 July (Washington D.C) and on 22 July in Brussels.

12. Issues relating to "intelligence collection" will be dealt with in a second Working Group with "interested Member States", the EU Institutions and US authorities.

---

[9] http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

[10] Attacks from America: NSA Spied on European Union Offices: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html
http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html

[11] Codename 'Apalachee': How America Spies on Europe and the UN http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html
On 2 September 2013 Brazil and Mexico have both demanded an explanation from the US over claims that the National Security Agency (NSA) spied on their presidents.
http://www.bbc.co.uk/news/world-latin-america-23938909

[12] Letter from the President of the Republic of Lithuania, H. E. Dalia GRYBAUSKAITE to President SCHULZ of 20 July 2013.