ARTICLE 29 Data Protection Working Party

Brussels, 13 August 2013

Viviane Reding
Vice President
Commissioner for Justice, Fundamental Rights and Citizenship
European Commission
B - 1049 BRUSSELS Belgium

Dear Vice President Reding,

The recent Prism controversy and related disclosures on the collection of and access by the American intelligence community to data on non-US persons[1] are of great concern to the international data protection community, including the members of the Article 29 Working Party (hereafter: WP29). Especially alarming are the latest revelations with regard to the so-called XKeyscore, which allegedly allows for the collection and analysis of the content of internet communication from around the world. Even though some clarifications have been given by the United States' authorities[2], many questions as to the consequences of these intelligence programs remain. Let me stress that the WP29 understands that on national security grounds different countries make different decisions on what information can or should be used to find leads and prevent, investigate or detect attacks against a country, or even for purposes of political and economic surveillance. At the same time, also in case of the protection of national security, due consideration should be given to the protection of individuals' fundamental rights irrespective of their nationality.

The joint EU – US working group that was established - and in which the WP29 is represented[3] - may be able to shed some light on the issues at stake, notably by establishing the facts with regard to the disclosed intelligence programs. However, the WP29 considers it is its duty to also assess independently to what extent the protection provided by EU data protection legislation is at risk and possibly breached and what the consequences of PRISM and related programs may be for the privacy of our citizens' personal data. In order to be able to do so we have, in addition to my previous letter dated 7 June 2013 and your letter to US Attorney-General Eric Holder dated 10 June 2013, identified the following issues of concern and questions that need to be answered as soon as possible.

[1] http://www.theguardian.com/world/the-nsa-files
[2] Privacy, Technology and National Security: An Overview of Intelligence Collection by Robert S. Litt, ODNI General Counsel – Brookings Institution Washington D.C. - 19 July 2013
[3] http://www.eu2013.lt/en/news/statements/presidency-statement-on-outcome-of-discussions-on-euus-working-group

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/13.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

First of all, it needs to become clear what information is actually collected through the intelligence programs following section 215 of the USA PATRIOT Act, section 702 of the FISA Amendment Act, Executive Order 12333 and adjacent legislation. News reports indicate that both the metadata[4] and contents of communications of non-US persons are collected, but as yet it is not fully clear which data are collected to what extent and what safeguards are in place before they are accessed. Neither has it become clear thus far if (meta)data on non-US persons collected as a by-product when investigating a US person under section 215 may subsequently be used for investigation of these non-US persons under section 702, and if so, under what legal provisions. Allegedly the collection of personal data takes place both on a very large scale as well as on a structural and/or systematic basis, allowing the NSA, FBI, CIA and/or other intelligence and law enforcement agencies continuous access.

One point that has been revealed is that data may only be accessed if they originate from non-US persons and are collected from sources within the US. The WP29 would however like to know when US authorities consider personal data to be inside the US, especially given the continuously increasing use of the internet for processing personal data, where much information currently is stored in the cloud, without knowing the exact location of the datasets, and following the global scale of backbone networks and their inherent capability to convey a wide range of communication services. It needs to be determined whether data on communication networks that are only routed through the United States (data that are in transit) are also subject to collection for the aforementioned intelligence programs. To this end, WP29 has so far considered that European law does not apply to personal data that is only in transit in the European Union, following article 4(1)c directive 95/46/EC. Applying the same reasoning would suggest that US law should not apply to data that is only in transit on its territory. It thus needs to become clear whether the intelligence services or other relevant bodies have to prove that the data are physically and legally available on US soil (i.e. stored on servers on US territory) or if it is sufficient that data are processed by or through an American company or subsidiary. Finally on this point, clarity is necessary over whether personal data is also collected on European territory, as is suggested in the media.[5]

Next, clarification is needed about the involvement of the FISA Court, both in terms of procedures and the moment it is seized, as well as the conditions and criteria the Court applies in its decisions to allow surveillance orders of non-US persons under the US legislation mentioned above. The WP29 wants to be able to assess to what extent these orders are narrowly targeted enough and substantiated sufficiently to allow for a limitation of individuals' fundamental rights on national security grounds. Additionally, it needs to be determined if this processing of personal data is in line with the data protection principle of purpose limitation and if the purposes for processing stated by the United States are indeed in line with the concept of national security as defined in the EU acquis. This can only be done in detail once the facts of the various intelligence programs are known. The US authorities

[4] WP29 understands the American notion of metadata corresponds to the categories of data retained in the European Union under article 5 of the data retention directive 2002/58/EC, except for the collection of location data

[5] http://www.reuters.com/article/2013/07/07/usa-security-germany-idUSL6N0FD0FV20130707

should be encouraged to disclose several NSA request and FISA Court orders to allow for this assessment to take place.

News reports suggest that the FISA Court has developed what is believed to be a secret body of law on surveillance and has set rules for the collection, use and access of data on the basis of the various intelligence programs. While it is always good if criteria limiting the processing of personal data are in place, it may prove problematic if these criteria are kept secret. Furthermore, the information that has been made public to date suggests that the FISA Court takes no decisions in individual cases, in which it weighs the national security interest against the fundamental rights of the individuals concerned, but the Court merely has to approve the procedures in place for the collection (and possibly use) of personal data from non-US persons. Moreover, the other safeguards in place do not seem to include scrutiny on the level of individual cases, except to ensure that the minimisation procedures (the procedures intended to ensure US persons are not targeted) are respected.

A third issue at stake is the relation between the intelligence programs following section 215 of the USA PATRIOT Act, section 702 of the FISA Amendment Act and Executive Order 12333 on the one hand and compliance by organisations with the conditions for the third country transfer of personal data (including standard contractual clauses, binding corporate rules and the Safe Harbour Principles) on the other hand. The Safe Harbour Principles indeed do allow for a limitation of adherence to the Principles "to the extent necessary to meet national security (…) requirements". However, the WP29 has doubts whether the seemingly large-scale and structural surveillance of personal data that has now emerged can still be considered an exception strictly limited to the extent necessary. Furthermore, the WP29 recalls that the Article 3.1 (b) of the Commission Decision on the Safe Harbour principles (Decision 2000/52/EC of 26 July 2000) gives to the competent authorities in Member States the possibility to suspend data flows in cases where there is a substantial likelihood that the Principles are being violated and where the continuing transfer would create an imminent risk of grave harm to data subjects.

It also needs to be clarified if these American intelligence programs are in line with European and international law. This includes the International Covenant on Civil and Political Rights, which lays down the right to privacy in a general way. More importantly, the necessity and proportionality of these programs according to the Council of Europe Convention 108 needs to be further assessed. WP29 therefore considers it is likely that the current practice of apparent large-scale collection and accessing of personal data of non-US persons is not covered by the Council of Europe Cybercrime Convention. This is particularly relevant in light of the on-going discussion within the Council of Europe Cybercrime Convention Committee (T-CY) on the preparations for an additional protocol meant to facilitate trans-border data flows in this field.[6] Such a draft protocol would appear to legitimise the current practice of the US intelligence community by allowing access to data stored on computers abroad by applying the law (or the definitions of consent) of the searching party.[7]

[6] (Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding trans-border access to data, T-CY (2013)14 - version 9 April 2013

[7] WP29 understands cybercrime is very often considered to be an issue of national security by the US authorities

Consequently, individuals including those in the EU Member States would not benefit from the protection afforded by their domestic privacy and data protection legislation.

Another issue that needs to be addressed is the possibility for redress for non-US persons. Currently, individuals affected are offered no possibility to assert their fundamental rights in court or before an independent oversight body. Admittedly, in general individuals will not be (made) aware that they are of interest to the intelligence services. However, if a suspicion arises, for example because an individual is wrongly arrested or limited in his freedom of movement, the individual needs to be able to effectively challenge the information provided by the intelligence services, as is the case in many European countries.

Finally, the WP29 wishes to stress that it will not only focus its attention on the intelligence programs used by the United States, but will also make an effort to assess any impact of PRISM, including the use of PRISM-derived information on European territory, to the extent possible within the WP29's mandate. Furthermore, the WP29 intends to examine compliance with EU data protection principles and legislation of possible similar intelligence programs on the territory of the Member States, such as Tempora, in its continuous endeavour to uphold the fundamental rights of all individuals.

I trust the European Commission will to the best of its ability contribute in finding the answers to the questions raised above, both within and outside the framework of the joint EU - US working group.

Yours sincerely,
On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman

A copy of this letter was sent to:
- *Cecilia Malmström, Commissioner for Home Affairs*
- *Martin Schulz, President of the European Parliament*
- *Juan Fernando López Aguilar, Chairman of the LIBE Committee of the European Parliament*