EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

11.12.2013

WORKING DOCUMENT 1

on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

1. Mass surveillance of EU Citizens

Recent disclosures have revealed the existence of systems of mass surveillance of citizens by the US and certain EU Member States. Prompted by an increasing focus on security, in particular following the 9/11 attacks these activities were enabled by the growth of internet usage, developments in communication technology and a weak oversight of intelligence services.

In only the past 10 or 20 years, citizens' lives have completely changed through the use of internet, email, communication through social media, online shopping, VoIP "phone calls", information technologies and data storage in the cloud. Whilst these are extremely positive developments, particularly in terms of convenience and cost, they entail an increasing amount of electronically held data, much of which contains personal information and private data. In parallel to this, advancements in technology have increased intelligence agencies' capacity to engage in large scale interception and analysis of such data.

These technological developments seemed to have contributed, along with other factors, to a fundamental shift in the work and practices of intelligence agencies, away from the traditional concept of targeted surveillance as a necessary and proportional counter-terrorism measure, towards systems of mass surveillance. While intelligence services perform an indispensable function in protecting the democratic society against internal and external threats, they have to operate within the rule of law; otherwise they will lose legitimacy and erode the exact democratic society they are trying to protect. This process of increasing mass surveillance has not been subject to any public debate or democratic decision-making, but decisions have largely been taken in small circles and behind closed doors. It appears that legal frameworks, which were put in place at times when technology was not so far advanced as today, are being used to justify systems of mass surveillance even when this was not the intention behind their initial legal interpretation. Due to the fact that oversight mechanisms in many states have not kept up with the increased capabilities of intelligence services, these systems of mass surveillance have continued to develop.

Such a public debate needs to take place now. We need to discuss the purpose and scale of surveillance and its place in a democratic society. We need to discuss the acceptable measures to fight crime and terrorism and where the lines need to be drawn to preserve the right to private life and protection of personal data in a digitalised world. We need to discuss how our intelligence services are supposed to collaborate without undermining the rule of law. We need to discuss how transatlantic business is conducted and how data flowing between countries and continents is kept safe and the governing laws respected.

The availability of proper information is a vital condition for this debate. The inquiry of the LIBE Committee has aimed to collect and assess such information. This working document is one element of this process. It presents an overview of the surveillance activities and discusses the impact of these on EU citizens' fundamental rights.

2. Surveillance Programmes

In recent months revelations were made about numerous different programmes. Several types of alleged surveillance issues can be distinguished as having an impact on the fundamental rights of EU citizens: the mass surveillance of EU citizens by the National Security Agency (NSA), the cooperation of EU Member States authorities in the surveillance programmes operated by the NSA, the surveillance programmes that are conducted by EU Member States themselves as well as surveillance programmes by other third states. Below some of the programmes of the NSA as well as some EU Member States will be presented.

Mass surveillance of EU citizens by the NSA

Several programmes of the NSA[1] focus on online activities. The **PRISM programme** is alleged to give the NSA direct access to the central servers of nine leading US internet companies allowing them to collect customer material including search history, the content of emails, file transfers and live chats.[2] The US administration confirmed the existence of the PRISM programme. However they stated that it was not an undisclosed collection or data mining programme.[3]

According to reports, the **Xkeyscore programme** allows NSA analysts, without prior authorization, to search through vast databases containing emails, online chats and browsing histories of millions of individuals as well as their metadata[4]. It was described as the NSA's widest reaching system that can cover "nearly everything a typical user does on the internet". In response the NSA confirmed the existence of the programme as part of the NSA's lawful foreign signals intelligence collection system saying it was limited to personnel who required access for assigned tasks[5].

BULLRUN is an alleged decryption programme run by the NSA in an effort to break into widely used encryption technologies that would allow the NSA to circumvent online encryption used by millions of people in their online transactions and emails.[6] No response was issued from the NSA in relation to the alleged Bullrun programme. The reports by the Guardian, the New York Times and ProPublica all stated that intelligence officials requested that the story was not published for national security reasons.

According to section 702 of FISA, a service provider might be required to "immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition" of foreign intelligence information. No clarification has been made on whether this provision could compel disclosure of cryptographic keys.[7]

---

[1] For an overview of the US legal situation see the Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection http://register.consilium.europa.eu/pdf/en/13/st16/st16987.en13.pdf

[2] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1

[3] http://online.wsj.com/public/resources/documents/prismfactsheet0608.pdf

[4] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[5] http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml

[6] http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[7] The US surveillance programmes and their impact on EU citizens' fundamental rights
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

Boundless Informant is a powerful data-mining tool deployed by the NSA to record and analyse global electronic information. It details and even maps by country the vast amount of information, mainly metadata, which it collects from computer and telephone networks. According to the reports, "the tool allows users to select a country on a map and view the metadata volume and select details about the collections against that country."[1] In March 2013, 97bn pieces of intelligence were collected from computer networks worldwide.

MUSCULAR, as reported by the Washington Post on 31 October[2], is a joint programme operated by the NSA with the GCHQ to intercept, from private links, data traffic flowing between the servers of Yahoo, Google, Microsoft Hotmail and Windows Live Messenger, amongst others. The access point, DS-200B is located outside the US, which renders the programme out of jurisdiction of the FISC court, and relies on an unnamed telecommunications provider to provide a secret access to a cable or switch through which the communications traffic passes. NSA documents about the effort refer directly to "full take," "bulk access" and "high volume" operations on Yahoo, Google and Microsoft networks. It was reported that numerous analysts working on the programme had complained that MUSCULAR produces too much data, much of which with low intelligence value.

In October 2013, media reports in France, Spain and Italy alleged that the NSA was intercepting huge volumes of **telephone calls**. For example, it was alleged that the NSA collected 70.3 million phone records in France from 10 December 2012 to 8 January 2013. In response General Keith Alexander, Chief of the NSA, stated the data was collected jointly by the NSA and the individual Member State intelligence agencies for purposes of defence and support of military operations[3].

Surveillance activities of EU Member States

According to press reports, the UK intelligence agency, **GCHQ**, was alleged to have access to communications collected through the PRISM programme allowing them to circumvent the national legal framework on accessing personal material from an internet company based outside the UK. Reports have also pointed to the joint involvement of GCHQ with the NSA in the MUSCULAR programme. The Intelligence and Security Committee (ISC) of the UK Parliament confirmed the use by the GCHQ of surveillance material obtained from the US PRISM programme but found that the GCHQ had not circumvented UK law by doing so.

GCHQ is alleged to engage in an upstream surveillance activity known as the **Tempora programme** which allows them access to large fibre optic cables that carry huge amounts of internet users' private communications and share it with the NSA. Due to the sheer volume of data collected, the content of the information is said to be deleted after 3 days, and metadata are usually kept for 30 days[4].

[1] http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining
[2] http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
[3] http://www.washingtonpost.com/world/national-security/top-intelligence-officials-called-to-testify-on-nsa-surveillance-programs/2013/10/29/e9e9c250-40b7-11e3-a751-f032898f2dbc_story.html
[4] http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

GCHQ is alleged to be operating a corresponding decryption programme to BULLRUN known as **Edgehill**. The programmed aims at decoding encrypted traffic used by companies to provide remote access to their systems and to "continue to work on understanding" major communication providers.

Reports on the activities of the **National Defense Radio Establishment (FRA), Sweden** have alleged that they are collecting/receiving data from fibre optic cables crossing Swedish borders from the Nordic and Baltic States and Russia and forwarding the data to the USA[1]. They also, allegedly, intercept and routinely monitor the Norwegian phone and internet cables that pass through Sweden as well as intercept mobile phone data and calls of other Nordic countries where the signal is transmitted through Swedish GSM links.

Allegations have emerged in **France that the General Directorate for External Security (DGSE)** intercepts and collects metadata from email, text messages and phone bills by use of a supercomputer capable of collecting, processing and storing data. The data is intercepted and collected by both satellite stations and interception of fibre-optic submarine cables. Also, the database is alleged to be accessed by six other intelligence services including the customs service and the anti-money laundering service[2].

In **Germany**, press reports have alleged that the **Bundesnachrichtendienst (BND)** has set up offices at the DE-CIX (German Commercial Internet Exchange) to divert incoming traffic, copy the data and analyse it later in the BND headquarters[3]. Reports also indicate strong cooperation between the German intelligence services and their US counterparts with reports of millions of metadata collected by the BND were being transferred to the NSA via data collection sites on German territory[4].

3. Impact on fundamental rights in the EU

Developments in technology have enabled states to know more about citizens than was ever possible in history. While previously it required considerable efforts and physical proximity to spy on a person, the technology of today allows such action on a scale and depth impossible before.

The systems of mass and indiscriminate surveillance impact significantly on the fundamental rights of citizens. While legal frameworks are in place, questions still remain as to whether the various programmes respect the spirit and were intended by the relevant legal frameworks; including International and European law notably with regards to the question of whether such programmes may be considered proportionate, necessary and appropriate in democratic societies.

---

[1] Source: M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', Nordic Yearbook of Law and Information Technology, Bergen 2010, pp. 96-134
Source: Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013

[2] Source: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' Le Monde, 4 July 2013.

[3] http://www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html

[4] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

The systems of mass surveillance described above have first and foremost an impact on citizens' privacy. By being able to collect data regarding the content of communications, as well as metadata, and by following citizens' electronic activities, in particular their use of smartphones and tablet computers, intelligence services are de facto able to know almost everything about a person. They can know where people are with advanced location programmes[1], with whom they speak and for how long, what they do, what they buy, what they read and even what they most probably think.

Surveillance, therefore, has also an effect on other fundamental rights such as freedom of expression, of opinion, of religion, of association, data protection, right to fair trial, access to an effective remedy etc. Of particular concern, as highlighted during the inquiry, is the impact on the freedom of the press, in particular through the chilling effect created for journalists providing information needed for an informed debate, through techniques used either to intimidate or to slow down reporting.

While intelligence services are essential in protecting against internal and external threats they have to operate at all times within the rule of law. Even the existence of a threat to national security is not a sufficient reason for an intelligence service to break the law. Illegal activities on the part of an intelligence services not only undermine the same democratic society that the services aim to protect, but also erode the legitimacy and democratic trust and support that the intelligence services need.

A key question which has been discussed during the inquiry is of whether the surveillance programmes violate the law, in particular international law and the European Convention on Human Rights. While obviously only courts are able to answer this question in a definitive manner, there have been strong statements indicating that we are indeed in a scenario where human rights and the rule of law have been violated.

3.1 The protection of privacy under international law

In terms of international law, testimonies were submitted to the Inquiry concluding that the US is in breach of its obligation under Article 17 of the UN International Covenant on Civil and Political rights (ICCPR) to prohibit arbitrary or unlawful interference with anyone's privacy or correspondence as it fails to comply with the permissible limitations test.[2]

In this regard the Inquiry awaits the assessment of the US compliance with Article 17 of the ICCPR by the Human Rights Committee and supports calls for an update to the ICCPR to tackle the transparency and proportionality concerns raised by mass surveillance practices be it by means of a new General Comment introducing a rigorous test for permissible limitations upon privacy rights (including data protection) or a new Additional or Amending Protocol to the ICCPR.

[1] NSA gathering 5bn cell phone records daily, Snowden documents reveal
http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden

[2] See testimony by Professor by Martin Scheinin (EUI), formerly UN Special Rapporteur on human rights and counter-terrorism and Douwe Korff, Professor of International Law, London Metropolitan University, London (UK) in the LIBE Committee on the Electronic Mass Surveillance of EU Citizens on 14/10/2013

All EU Member States to the ICCPR are also covered as far as their own surveillance activities are concerned whether targeting their own or other Member States' citizens. As to the cooperation of Member States authorities in the surveillance programmes operated by the NSA, the Human Rights Committee states in its General comment, that "State parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant", therefore such cooperation is also unlawful under the ICCPR.

3.2 The protection of privacy under the European Convention on Human Rights (ECHR)

The European Court of Human Rights (ECtHR) has consistently ruled that national security and intelligence agencies are bound to respect the rights and freedoms as laid down in the ECHR. Not only this, but there is a positive obligation on Member States to protect their citizens from surveillance undertaken by third parties, be they states or private entities[1].

Given the extent of the mass collection of personal data that are collected through the surveillance programmes, serious concerns have been raised as to whether these activities respect EU citizens' right to private life and privacy of their communications under the ECHR[2]. Whilst the right to privacy is not absolute, this does not infer an automatic suspension on grounds of national security. According to the ECtHR, the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied and thereby may amount in itself to an interference with the exercise of individuals' rights under Article 8, irrespective of any measures actually taken against them[3].

Any interference with this right, by means of surveillance practices, should be prescribed by law, limited, necessary, proportionate and subject to continual assessment. Given that telecommunications technologies have rapidly developed to allow the indiscriminate mass collection of communication data, it is imperative that EU Member States adopt precise legislative frameworks that will ensure effective legal scrutiny to safeguard private information[4].

More particularly, any surveillance must be "in accordance with law". The ECtHR has interpreted this element as accessibility of the relevant provisions and foreseeability of their consequences. The relevant legal rules shall always define categories of offences or persons likely to be subject to surveillance measures[5]. Further, there must be strict limits on the duration of any ordered surveillance[6]. Further, interference shall serve a "legitimate aim in a democratic society", while being "necessary" and "proportionate" in relation to that aim. "Necessary" means corresponding "to a pressing social need"[7] while "proportionate" shall be

[1] *Van Hannover v Germany*, Judgment of 24 June 2004, (2005) 40 EHRR 1, *X & Y v Netherlands ,* Judgment of 26 March 1985, (1985) 8 EHRR 235, see also the Council of Europe's Human Rights Handbook No. 7 on Positive obligations under the European Convention on Human Rights, by Jean-Francois Akandji-Kombe, available at: http://www.coehelp.org/file.php/54/resources/Handbooks/pos_obl_eng.pdf
[2] Article 8 of the ECHR
[3] Weber and Saravia, para. 78
[4] Uzun v Germany (2012) 54 EHRR 121 at [61], in Weber v Germany (2008) 46 EHRR SE5 at [93]
[5] *Kennedy v. The United Kingdom,* judgment of 18 May 2010, application no. 26839/05
[6] *Weber and Saravia v. Germany, Liberty and Others v. UK*
[7] *Leander v. Sweden,* judgment 26 March 1987, § 48, Series A no. 116

defined by reference to the legitimate aim pursued. In the same regard, adequate guarantees must be laid down to prevent any misuse of power[1]. Thus, mere usefulness or desirability is not sufficient justification. The ECtHR has also found in several cases that, for instance, rules should provide that the duration of the interception[2] and of the storage of information[3] is limited or, at least, that adequate safeguards are put in place to control the discretion of authorising authorities in this regard[4].

3.3 The protection of personal data

The European data protection framework is founded on a list of core principles including; data must be processed fairly and lawfully, personal data must be obtained for a specific and lawful purpose, personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed and appropriate measures should be taken against unauthorised processing of personal data.

The alleged practices of mass surveillance as described above without any specific, targeted justification are at odds with these founding principles. There is a positive obligation on the EU and its Member States to protect the personal data of their citizens and to ensure that any international transfer of data respects these core principles.

3.4 The right to effective remedy

An effective remedy is a fundamental right under the EU Charter and the ECHR, awarded to all persons, regardless of their nationality, also applicable to cases where data privacy rights have been violated. The ECJ has also established, as a basic principle, that remedies must be available in all cases of breach of EU law. All these EU safeguards are in direct contrast to the legal framework in the US which reciprocally denies European citizens, who are not resident in the US, the right to an effective remedy.

If EU citizens are under surveillance for any lawful reason they must have the right to challenge the information by intelligence authorities. Given the mass international transfer of data of EU citizens to US authorities, the lack of appropriate redress mechanism for European citizens is an issue of extreme concern. As a step towards reciprocity, the US must explore the most appropriate mechanisms to extend at least the legal protection afforded to persons within the US also to EU citizens outside the US, in order to provide an effective legal redress mechanism for EU citizens whose data has been held or accessed by the US authorities.

3.5 The protection against discrimination of EU citizens

[1] Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no.176-A, and Eur. Court HR, Huvig v. France judgment of 24 April 1990, Series A no.176-B
[2] Eur. Court HR, Kruslin v. France judgment of 24 April 1990, Series A no.176-A, and Eur. Court HR, Huvig v. France judgment of 24 April 1990, Series A no.176-B
[3] Eur. Court HR, Rotaru v. Romania judgment of 4 May 2000, application no. 28341/95, Eur. Court HR, Amann v. Switzerland judgment of 16 February 2000, application no. 27798/95
[4] Eur. Court HR, Kennedy v. The United Kingdom, judgment of 18 May 2010, application no. 26839/05.

Reciprocity is a crucial element of international relations and something that has been fundamentally lacking in the EU-US relationship. Whereas US legal protection concerning communication data applies only to US citizens and residents, in the EU, regardless of their nationality, everyone's personal data and the confidentiality of their communications are protected as fundamental rights.

According to the US legal framework the provisions of the First and Fourth Amendment do not protect EU citizens and it seems that relevance requirements are very low in case of US surveillance activity directed at EU citizens. For instance, under section 702 of the FISA Amendments Act, no probable cause seems to be required in order to target foreign citizens, as targeting and minimisation guidelines do not apply in the case of non-US persons.

European citizens have no right to be informed, nor can they challenge the surveillance activities conducted by US authorities in any way, despite the principle of non-discrimination and equality before the law, as laid down in Article 26 ICCPR.

3.6 Surveillance programmes and their compatibility with the Presumption of Innocence

The practice of untargeted, mass surveillance and the collection of bulk data of EU citizens may at least risk violating the fundamental principle of justice, notably in criminal proceedings, of "presumption of innocence", which again covers all persons, irrespective of nationality[1].

The role of mass surveillance leads to a shift in criminal law from its role of sanctioning specific acts on the basis of personal responsibility to reducing risks and identifying possible offenders, which can lead to all citizens, under continuous surveillance, being considered as suspects.

3.7 Freedom of Expression – impact on Journalism and Whistleblowers

There is a consensus on the need for transparency and for an informed debate on the extent of mass surveillance activities, and their impact on privacy. Such a debate is only possible if media freedom is respected. In particular, when supervisory mechanisms fail to prevent or rectify mass surveillance, the role of media and whistleblowers in unveiling eventual illegalities or misuses of power, notably when these infringe upon fundamental citizens' rights, is extremely important.

Throughout the Inquiry, the LIBE Committee has heard several statements by journalists, whistleblowers and the civil society on the need for strong protection of freedom of information and of media freedom in the sensitive area of intelligence activities. Furthermore the Editor of the Guardian, Alan Rusbridger, stated that the reactions from the US and UK authorities to the disclosures by Edward Snowden have had a chilling effect on journalism and he urged the European Parliament to do more to protect the media.

[1] The presumption of innocence is considered to be a fundamental principle of criminal law and is recognised both in the ECHR and the Charter of Fundamental Rights of the European Union.

Freedom of expression and information, including media freedom, is protected both under the EU Charter of fundamental rights (Article 11) and the ECHR (Article 10). These were further substantiated by recent reports from the European Parliament[1], EctHR case-law, the Parliamentary Assembly of the Council of Europe (PACE) and various UN texts which all require Member States to protect freedom of expression, interferences being allowed only under restrictive conditions similar to those on privacy, including in the field of surveillance. Journalists must also be protected against intimidation tactics to ensure freedom of the press.

Throughout the Inquiry, it has become evident that whistleblowers play a crucial role in unveiling serious violations of fundamental rights and as a result are extremely vulnerable to retaliation attacks. The ECtHR has upheld whistleblowers' rights under the same conditions governing protection of the freedom of expression, ruling against interferences by the State/their employer[2]. The important role of the whistleblowers and the need for protecting them against dismissals and the related chilling effect has also been confirmed by the Court[3].

Whistleblowers' right to freedom of expression has also been substantiated with several other recent initiatives from the Council of Europe[4], PACE[5], the European Parliament[6] and civil society, including Transparency International[7]advocating for stronger whistleblower protection. Whilst the European Commission has adopted sectoral provisions on whistleblowing, it is clear that a more comprehensive approach could be envisaged at the EU level.

[1] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0203+0+DOC+XML+V0//EN
[2] See for instance, Heinisch v. Germany, App. No. 28274/08, Eur. Ct. H.R. (2001)
[3] Guja v. Moldova, Application no. 14277/04, Judgment of 12 February 2008
[4] http://www.coe.int/t/DGHL/STANDARDSETTING/CDcj/Whistleblowers/CDCJ%20(2012)9E_Final.pdf
[5] http://assembly.coe.int/main.asp?link=/documents/adoptedtext/ta10/eres1729.htm
[6] European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report) (2013/2107(INI))
[7] Transparency International, "Whistleblowing in Europe, Legal protections for whistleblowers in the EU", 2013 http://www.transparency.org/whatwedo/pub/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu