Submission Authored by the German Parliamentary Group BÜNDNIS 90/DIE GRÜNEN (The Greens)
109th Session of the Human Rights Committee, Geneva
14 October 2013 - 01 November 2013

I. Issue Summary

The Alliance 90/The Greens parliamentary group in the Bundestag regards it as a cause for concern that the USA monitors and spies on the internal electronic communications of the German population which in technical terms are routed through the USA. The parliamentary group is particularly anxious to voice its concerns because the communications of its parliamentarians and of the German parliament are also affected. This represents a fundamental attack on democracy in Germany and significantly interferes with the free exercise of the parliamentary mandate and of the process of debate within the parliamentary groups and within parliament. Furthermore the threatened extensive surveillance of electronic communications in Germany by US intelligence agencies interferes with the process of free political debate in Germany and in Europe as a whole. There is at the very least a danger of a widespread chilling effect on democratic debate and culture. Such an attack on the freedom of public and private communications which is the essential basis of a free democracy represents already according to the present legal situation a breach of Articles 17 and 19 of the International Covenant on Civil and Political Rights (below: Covenant). There are, moreover, reasons to fear that the intelligence services of the USA, the UK, Germany and other countries are using a type of organised circular exchange or trade-off to circumvent the legal restrictions to which they are subject under their respective national laws with respect to spying on their nationals. This also amounts to a circumvention of the standard of protection provided for in the Covenant.

The assessment in the first section of this submission is based in particular on the points made in paragraph 2 below. In order to provide a better understanding of the USA's surveillance policy, measures applied inside the USA are outlined in point 1 and the USA's evaluation programs are referred to in paragraph 3.

1. Surveillance inside the USA

Internally the US government is subject to constitutional constraints, especially the Fourth and 14th Amendment to the US-constituion, which can impose restrictions on mass surveillance. Nevertheless the US government has taken measures that in legal terms , including domestically (for the USA), go far beyond what is regarded in Germany as permissible with respect to the retention of data, as reflected in the German Federal Constitutional Court's ruling in relation to the protection of the secrecy of telecommunications [1] . Metadata (contact data) from electronic communication (in

[1] http://www.bverfg.de/pressemitteilungen/bvg12-013en.html; The European Directive in this regard on which German legislation is based is currently being reviewed by the European Court of Justice in terms of its compatibility with fundamental rights (C-293/12 and C-594/12).

particular relating to phone calls) are stored for five years[2]. Since the identity of the parties to these calls can be identified, the retention of these data alone enables comprehensive screening of the population's personal contacts (see paragraph 3 regarding technical means) and hence a policy of social control. The US authorities are already able to ascertain who is in contact with whom and when within the USA.

2. PRISM - Surveillance program for foreign communications

The data disclosed by the whistleblower Edward Snowden reveal that the USA has encroached substantially more radically and extensively on the communication secrecy of foreigners abroad who enjoy fundamental rights (e.g. purely internal German communication) than it does within the USA itself (cf. paragraph 1) and that it also accesses the content of communications. This fact has already been publicly admitted by the USA, hence confirming in principle Snowden's disclosures[3].

While, contrary to what has been said in the international press, the US authorities have sought to put this significant level of surveillance into perspective, the US government's own account proves that this surveillance is more than a case of isolated measures directed against individual terrorists. The US government states[4]:

> "Under Section 702[5], instead of issuing individual orders, the FISC, […], approves annual certification […] that identify broad categories of foreign intelligence which may be collected."

Virtually all the restrictions listed in the document quoted (see "second" to "finally") relate to the protection of US citizens or to internal American communication. The restriction relating to foreign information[6] (under "first")

> "a significant purpose of an acquisition is to obtain foreign information",

does not represent a suitable and clear legal criterion for applying a restriction and ensuring the protection of human rights. It can be assumed that anybody who has at any time communicated with anybody else who has at any time had contact with a person from, for example, a radical Islamist group is a potential subject for surveillance. Since this could apply to virtually anybody, everybody is potentially affected.

Thus even according to the US government's own account, it is evident that it extensively accesses the content of foreign (including purely internal German) communications. In addition to PRISM, which uses servers in the USA through which purely foreign (e.g. internal German) communications

[2] According to the US government, Robert S. Litt, ODNI General Counsel, PRIVACY, TECHNOLOGY AND NATIONAL SECURITY, July 19, 2013: "bulk collection of telephony metadata".
[3] See evidence on http://icontherecord.tumblr.com/ and footnote 2 above.
[4] Annex to letter of 4 May 2012 to the United States Senate Select Committee on Intelligence, p. 2; published on http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf [highlighting not in original].
[5] Foreign Intelligence Surveillance Act (FISA).
[6] See footnote 3 above.

are also routed, foreign internet-based information is also swept up as it transits other communication channels in the USA[7].

3. XKeyscore

The NSA uses Xkeyscore,[8] a data collection and in-depth analysis program which enables real-time storage and analysis of any internet communication (connection and content data) due to the worldwide server infrastructure. The program enables the intercepted data to be screened, which could lead to a further significant encroachment on the right to privacy.

The NSA has only partially refuted the reports on XKeyscore. While the agency denies that analysts have practically unrestricted access to information, the former NSA director, Michael Hayden, stated that XKeyScore was "good news" as it enabled intelligence agents to "find the needle in the haystack".[9]

4. Circular exchange

There are a number of indications that German intelligence services are working with and using the results of communications surveillance by the NSA and the British Government Communications Headquarters (GCHQ). This gives rise to suspicions of a circular exchange to circumvent respective national restrictions on the surveillance of nationals:

- An interview with the former US intelligence chief, Michael Hayden (1999-2005 Director of the NSA, 2006-2009 Director of the CIA,) reveals very open and close cooperation between the intelligence services post 9/11 including the exchange and pooling of large amounts of data, although he provided no details.[10]
- In a lecture on 19.7.2013 the current NSA Director, Keith Alexander, stated that every nation acts in its own self-interest and we all have intelligence services. He said it was an honour to work with the German intelligence services. "We don't tell them everything we do, or how we do it [....] Now they know. And we go through a court process that's probably more rigorous than anybody's in the world".[11]
- Following a report in the press[12] that Germany, with 500 million data sets (in a given month), was the country subject to the most surveillance by the USA, a German government minister sought to pacify the public by saying that it was not the USA who had collected this data, but rather the data were a product of German foreign surveillance which was passed to the Americans [13].

---

[7] Footnote 3, p. 3, 4: "in addition to collection directly from ISPs, NSA collects telephone and electronic communication as they transit the Internet "backbone" within the United States".
[8] http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
[9] NSA press statement 30 July 2013 http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml
[10] http://www.heute.de/Ex-NSA-Chef-spottet-%C3%BCber-deutsche-Politiker-28928066.html.
[11] http://www.heute.de/NSA-Chef-Jetzt-wissen-die-Deutschen-Bescheid-28912874.html.
[12] http://www.spiegel.de/netzwelt/netzpolitik/prism-und-tempora-fakten-und-konsequenzen-a-909084.html
[13] http://www.bundesregierung.de/Content/DE/Mitschrift/Pressekonferenzen/2013/08/2013-08-12-pofalla.html : „Die Daten, über die in den letzten Wochen teilweise hitzig diskutiert worden ist, stammen also nicht aus der Aufklärung der NSA oder des britischen Nachrichtendienstes. Sie stammen aus der Auslandsaufklärung des [deutschen] BND [Bundesnachrichtendienst]. Diese Daten erhebt der BND im Rahmen

II. Concluding Observations by the Human Rights Committee and other case law of the Human Rights Committee under the International Covenant on Civil and Political Rights

The Human Rights Committee, in its General Comment No. 16 on Article 17 of the Covenant in 1988, already determined that Article 17 also covers new forms of electronic communication and that interferences in the right to privacy not only require a legal basis but also in particular have to be reasonable in the particular circumstances.[14] The Committee also made it explicitly clear that what amounted to mass surveillance of electronic communication was not compatible with Article 17 of the Covenant and that only surveillance on a case-by-case basis was permissible:

> "8. Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[15]

The Committee also refers to the need for legal protection against interception measures:

> "10. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. […] In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."[16]

The Human Rights Committee already addressed the monitoring practices of the US intelligence services on an earlier occasion (CCPR/C/USA/CO/3/Rev.1, S. 6 f., sec. 21) and, despite certain specific improvements to the legal situation, expressed concern about compliance with the provisions of Article 17 of the Covenant. The Committee expressed particular concerns about the limited possibilities of people under surveillance to be informed about such measures and to receive protection under the law in this respect. Furthermore the Committee, referring to Article 2

---

seiner Gesetze und leitet sie auch auf der Grundlage des Abkommens vom 28. April 2002 an die NSA weiter." (These data which have been the subject of such intense debate in recent weeks are not the result of surveillance by the NSA or British intelligence services. They are a product of the foreign surveillance of the [German] BND [Federal Intelligence Service]. The BND collects the data under its laws and passes the information on to the NSA on the basis of the Agreement of 28 April 2002)

[14] CCPR General Comment No. 16, para. 4.

[15] CCPR General Comment No. 16, para. 8.

[16] CCPR General Comment No. 16, para. 10.

paragraph 3 and Article 17 of the Covenant, was concerned that the NSA in particular monitors the phone, e-mail and fax communications of people both inside and outside the USA without any judicial or other independent control.

The Committee recommended that the USA revise Sections 213, 215 and 505 of the Patriot Act in order to ensure that they fully comply with the provisions of Article 17 of the Covenant. In particular it is required to ensure that any interference in the individual's right to a private life remains restricted to what is strictly necessary and is duly authorised by law. There is also a requirement to respect the individual rights arising from this.

In its case law to date not specifically related to the USA, the Committee has clearly established that it is incompatible with the provisions of Article 17 for national laws to provide for interferences in private life. The Committee moreover regularly states that any interference may not be arbitrary. The Committee understands arbitrary in the meaning of Article 17 paragraph 1 of the Covenant to mean in essence that the interference must be reasonable and in other respects accord with the other objectives and provisions of the Covenant.[17]

In particular with respect to surveillance by intelligence services and similar, the Committee requires that legal regulations for those affected must guarantee the right to be informed of measures affecting them, that they must have the right to request rectification of incorrect data and where necessary to ensure the elimination of data collected about them. The law must also provide for effective control mechanisms.[18]

III. U.S. Government Report

In the current and previous List of Issues, the Committee called on the USA to comment on NSA surveillance of phone, email and fax communications both within and outside the USA and steps taken in this regard.

In its report of 2 July 2013 the USA reported that the President acknowledged in the 2011 periodic report that in 2005 the NSA had been intercepting international communications without a court order where the government had a reasonable basis to conclude that one party was a member of or affiliated with al-Qaida or a member of an organisation affiliated with al-Qaida. It reported that this practice had now been brought under the supervision of the FISC. In 2008 the legislation had been amended and FISC's role solidified. This had enhanced judicial and Congressional oversight and oversight by Congress and the protection of individual rights.[19] In general, without naming details, the USA stated that there was oversight of intelligence activities by Congress and that the executive branch also exercised extensive oversight.[20]

[17] Cf. Sarah Joseph/Melissa Castan, The International Covenant on Civil and Political Rights, 3rd ed. 2013, p. 535 ff.; Jakob Th. Möller/Alfred de Zayas, United Nations Human Rights Committee Case Law 1977-2008, 2009, p. 339 ff. Each with numerous references to the corresponding case law of the Human Rights Committee.
[18] General Comment 16/32, para. 10; Manfred Nowak, CCPR Commentary, 2nd ed. 2005, Art. 17 note. 23.
[19] United States Written Responses to Questions From the United Nations Human Rights Committee Concerning the Fourth Periodic Report, para. 115: http://www.state.gov/j/drl/rls/212393.htm.
[20] ebd. para 119.

While the above comments by the USA to the Committee suggest that surveillance is directed exclusively at members of al-Qaida and persons affiliated with this group, this is cannot be reconcilded with the published material (see I.2.).

IV. Other UN Body Recommendations und European Court of Human Rights

In his report of 17 April 2013[21] to the UN General Assembly the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, expresses concern that state surveillance and the interception of electronic communications can have a substantially negative impact on individual freedom and on freedom of expression, which is fundamental to democracy:

> "23. In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. Anonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation."

The Rapporteur particularly emphasizes the chilling effect that surveillance can have on free democratic discourse:

> "24. The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization. In this regard, article 17 of ICCPR refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communication, both online and offline. As the Special Rapporteur noted in a previous report, the right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties." [internal footnotes omitted]

The case law of the Committee, as outlined above (II.) is in line with the corresponding decisions with respect to the European Convention on Human Rights made by the European Court of Human Rights in Strasbourg. This case law also calls for a clear delimitation of powers to store information and also clear rules on the examination, transmission and destruction of collected material[22].

[21] A/HRC/23/40.

[22] See in particular Liberty vs. UK (http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207)and Weber and Saravia vs. Germany (http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-76586)

V. Recommended Questions

1. Please explain the scope of interception measures involving nationals (US citizens and "US persons") and foreigners abroad in an average month and during recent years and what percentage of internet, phone and fax communications that in technical terms transit the USA and servers or communication channels there are affected. Please specify whether the intercepted and stored data are solely metadata or also include the content of communications, and what intelligence services and government agencies have access to the data as a whole or parts of it.

2. Please explain for what period metadata and the content of intercepted communications are stored and according to what criteria and processes stored data are deleted and/or according to what criteria and processes storage periods are extended.

3. Please explain

a) the steps taken in practice with reference to nationals and foreigners abroad to ensure that interception measures comply with the requirements of Article 17 of the Covenant with respect to the proportionality of the measures and what measures are taken to avoid as far as possible and

b) a chilling effect on communications relating to public and private affairs in the USA and other countries affected by US surveillance.

4. Please explain how foreigners whose communication abroad with foreigners, e.g. communication in Germany between two German nationals, has been intercepted on the basis of Section 702 of the FISA or another legal basis can

a) obtain information from government agencies in the USA about this process,

b) proceed against the incorrect storage of their data and, where appropriate, have this data deleted and

c) obtain legal protection before the courts in the USA or other independent supervision bodies in the USA against interception measures.

5. Please explain the legal conditions under which personal information obtained by the NSA or other intelligence services in the USA, e.g. on the basis of Section 702 of the FISA or measures to intercept internet, phone or fax communications on another legal basis, can be passed on to services in other countries such as the United Kingdom or Germany.

6. Please explain the legal requirements for the receipt, storage and processing of personal information by the NSA or other intelligence agencies in the USA received from intelligence services in Germany or the United Kingdom and which they know or suspect originates from the surveillance activities of the intelligence services in these countries.

7. Please explain whether and how it is ensured that the electronic communications of the parliamentarians of other countries who are not themselves suspected of committing terrorist acts against the USA or of supporting such acts are not intercepted, stored or used and what legal protection foreign parliamentarians have against this in the USA.

80. Please explain the legal conditions under which the NSA or other US intelligence agencies may be in receipt of personal information about US citizens or US persons which has been intercepted in the USA by the intelligence services of other countries and which the NSA or other US intelligence agencies would not have been permitted to intercept under Section 702 of the FISA or another American legal provision.

VI. Suggested Recommendations

1. Creation of legislation to ensure that the interception of the communications of foreigners abroad where the surveillance is technically carried out in the USA also complies in full with Article 17 and the other objectives of the Covenant. This includes in particular compliance with the principle of proportionality which prohibits any – even de facto – mass or virtually mass surveillance and avoiding data preservation. Furthermore it also includes safeguarding the information rights of foreigners affected by surveillance who live abroad, as well as providing comprehensive legal protection in the USA which enables effective enforcement of the right to have incorrect or wrongly collected data rectified or eliminated.

2. Creation of legislation governing the passing on of personal information to the intelligence services or other government agencies of other countries by the NSA or other intelligence agencies in the USA which has been acquired by interception or other intelligence activities in full compliance with Article 17 and the principle of proportionality derived from this, as well as the other objectives of the Covenant. This includes in particular safeguarding the rights of those affected by surveillance to be informed and comprehensive legal protection in the USA which enables the effective enforcement of the right to have incorrect or wrongly collected personal data rectified or eliminated.

3. Creation of legislation governing the receipt, storage and processing of personal information which the intelligence agencies in the USA receive from the intelligence services or other government agencies of other countries which is in full compliance with Article 17 and the principle of proportionality derived from this, as well as the other objectives of the Covenant. This includes in particular safeguarding the rights of those affected by surveillance to be informed and comprehensive legal protection in the USA which enables effective enforcement of the right to have incorrect or wrongly collected personal data rectified or eliminated.

Renate Künast MdB

Volker Beck MdB

Ingrid Hönlinger MdB

Dr. Konstantin von Notz MdB