Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13748
09 April 2015

Mass surveillance

Committee Opinion[1]
Committee on Culture, Science, Education and Media
Rapporteur: Sir Roger GALE, United Kingdom, European Conservatives Group

A. Conclusions of the committee

1. The Committee on Culture, Science, Education and Media considers the report on mass surveillance by the Committee on Legal Affairs and Human Rights (Doc. 13734) as being very timely. This report was originally triggered by the massive disclosure of secret data by Edward Snowden, stemming from national security operations of the United States, Great Britain, Australia and other countries, as well as criminal charges opened against him on 14 June 2013 by a federal prosecutor in the United States and his subsequent change of residence to the Russian Federation since July 2013. However, the political importance of this subject has grown beyond the person and acts of Edward Snowden.

2. Welcoming the general findings of this report on mass surveillance, the committee proposes to further clarify and define the draft resolution contained in that report through a number of amendments.

B. Proposed amendments to the draft resolution:

Amendment A (to the draft resolution)

In paragraph 2, after the words “intelligence services and the”, insert the word “potential”.

Amendment B (to the draft resolution)

Delete paragraph 7.

Amendment C (to the draft resolution)

In the English version, in paragraph 11, first sentence, after the word “terrorists”, delete the word “or” and insert the word “and”.

Amendment D (to the draft resolution)

In paragraph 12, second sentence, delete the word “But” and after the words “founded on”, insert the words “international agreements,”.

1. Reference to committee: Reference 4003 of 30 September 2013. Reporting committee: Committee on Legal Affairs and Human Rights. See Doc. 13734. Opinion approved by the committee on 11 March 2015.

Amendment E (to the draft resolution)

At the end of paragraph 13, after the word “violations”, insert the words “in the public interest and without personal gain”.

Amendment F (to the draft resolution)

Delete paragraph 14.

Amendment G (to the draft resolution)

Replace the second sentence of paragraph 15 by the following text:

> *“Recalling the findings of the Report on the Democratic Control of the Armed Forces adopted by the European Commission for Democracy through Law (Venice Commission) in 2008, the Assembly emphasises that parliaments should have a major role in monitoring, scrutinising and controlling national security services and armed forces in order to ensure respect for human rights, the rule of law, democratic accountability as well as international law. The sub-contracting of security or intelligence operations to private firms should be the exception and must not reduce the democratic oversight of such operations.”*

Amendment H (to the draft resolution)

Delete paragraph 16.1.

Amendment I (to the draft resolution)

After paragraph 16, insert the following paragraph:

> *“The Assembly invites the European Union to accelerate its work towards finalising the General Data Protection Regulation and the Passenger Name Record (PNR) system, to conclude international co-operation agreements based on the Schengen Information System and to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).”*

Amendment J (to the draft resolution)

In the English version, in paragraph 17.1, replace the words “mail secret” by the words “confidentiality of correspondence”.

Amendment K (to the draft resolution)

Replace paragraph 17.3 by the following paragraph:

> *“provide for credible, effective protection for whistle-blowers exposing unlawful surveillance activities, in accordance with Assembly Resolution 1729 (2010) on protection of whistle-blowers;”*

Amendment L (to the draft resolution)

In paragraph 17.4, third sentence, delete the words “political” and “or diplomatic”.

C. Explanatory memorandum by Sir Roger Gale, rapporteur for opinion

1. Introduction

1. On 30 September 2013, as a follow-up to the current affairs debate on “State interference with privacy on the Internet” of 27 June 2013, the committee had held an exchange of views with Lawrence Early, Jurisconsult of the European Court of Human Rights, Dorothee Belz, Vice-President, Legal and Corporate Affairs, Microsoft Corporation Europe, and Duncan Campbell, Journalist, Brighton, United Kingdom.[2] Having

2. https://pace.coe.int/documents/19871/25990/CoECultureCommittee1Oct2013REV.pdf/ee1f16ef-1faf-49a9-8b41-f2767e300b3c.

heard Mr Campbell in Paris on 11 March 2014 again in the framework of the preparation of the report on "Improving user protection and security in cyberspace" by Axel Fischer (Germany, EPP/CD), the committee had decided to ask the Assembly's Bureau to be seized for opinion on the report on mass surveillance.

2. Mass surveillance

2. Mass surveillance is not a recent phenomenon. Starting from direct surveillance of persons at a massive level through huge numbers of neighbourhood wardens ("Blockwart") under the Nazi dictatorship in Germany, communist dictatorship developed mass surveillance further through technological progress, leading to large-scale telephone tapping and the storage of conventional and later electronic data by the notorious KGB of the Soviet Union, especially in the satellite "brother countries" under its control. Such practice has caused a strong popular distrust in authorities of a State spying on its people, as described by George Orwell in his novel *Nineteen Eighty-Four* as well as by the citation of Alexandr Solzhenitsyn describing the situation in the USSR by the words "Our freedom is built on what others do not know of our existences", which opens the report on mass surveillance.

3. While non-democratic States used mass surveillance in order to control and stifle political opposition, surveillance technologies have also been used by democratic States in order to combat large-scale crime and terrorism. In the wake of the terrorist attacks by the "Red Army Fraction" in West Germany in the 1970s, the European Court of Human Rights held in *Klass and others v. Germany* (Application No. 5029/71) that "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. … The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law".[3]

4. The growth in mobile telephony since the end of the 20th century has enabled secret services to intercept such telephone communications widely. The practice by the United States and its allies was the object of the report by the European Parliament of 11 July 2001 "on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)".[4] At the same time, the European Court of Human Rights developed further its jurisprudence in this field: "In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."[5]

5. Through the rapid growth of Internet communication and the technological simplicity in intercepting and monitoring such communication, mass surveillance has entered a new and so far unknown scale. While the manner of the disclosures made by Edward Snowden through a British national newspaper and the consequent risk posed to the lives of those engaged in counter-terrorism is highly questionable, those disclosures have nevertheless also shed light on the practice of national security services of the United States and countries co-operating with the United States. It can be assumed, however, that third countries also possess the technological equipment and skills in order to pursue mass surveillance of Internet and mobile communications of their citizens and foreigners abroad. In addition, mass surveillance or profiling of Internet users is also used by multinational commercial companies specialising in targeted advertising. The latter phenomenon has been addressed by the Committee of Ministers in its Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling and its Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines.

---

3. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510.
4. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN.
5. *Liberty and others v. the United Kingdom* (Application No. 58243/00) citing its decision in *Weber and Saravia v. Germany* (Application No. 54934/00), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207.

6. Mass surveillance measures have to be assessed with proper regard to their purpose. While private or commercial mass surveillance is generally not covered by the exceptions to the right to protection of private life under Article 8 of the European Convention on Human Rights (ETS No. 5), mass surveillance by law-enforcement authorities must respect the safeguards established by the European Court of Human Rights.[6] National security is specifically mentioned in Article 8 of the Convention and obviously allows for restrictions of the right to private life, but it is essential that national security is carefully defined by domestic law and that such measures are not used by governments in order to persecute democratic political opposition.[7] As regards a narrow definition of the term national security, reference can be made to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information of 1995.[8]

7. Following the terrorist attacks in Paris, the ministers of the interior of several countries in Europe as well as Canada and the United States made a declaration on 11 January 2015 in Paris which called for greater international, and in particular transatlantic, co-operation in the fight against international terrorism. This was echoed by the informal meeting of Justice and Home Affairs Ministers of EU member States in Riga on 29 and 30 January 2015.[9] Such co-operation had led to the arrest of Islamist terrorists informally called "Sauerland Group" in Germany in autumn 2007, based on telephone and email communications between Germany and Pakistan that had been intercepted by the National Security Agency of the United States, which had subsequently informed the German authorities. Although Russian security services had intercepted telephone calls of Tamerlan Tsarnaev with his mother and had informed the intelligence services of the United States, Tsarnaev and his brother were able to launch the bomb attack on the Boston Marathon in 2013, thus highlighting the potentially disastrous and lethal consequences of inefficient co-operation.[10]

8. In 2013, the European Parliament blocked the proposal to exchange cross-border passenger data between the European Union and the United States. Shortly after the attacks on *Charlie Hebdo* on 7 January 2015, the President of the EU Council called on the European Parliament to speed up work on the EU Passenger Name Record (PNR) system. On 11 February 2015, the European Parliament finally agreed to expedite work on the PNR before the end of 2015.[11] Such work should be linked to the finalising of the General Data Protection Regulation of the European Union and its accession to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

9. Edward Snowden, who was working with a private company sub-contracted by the National Security Agency of the United States, stated in *The Guardian*: "The government has granted itself power it is not entitled to. There is no public oversight. The result is people like myself have the latitude to go further than they are allowed to."[12] This self-critical statement illustrates the problem that private security firms are legally responsible solely under a given contract and the general laws of a country, whereas democratic oversight by parliaments is applicable to public authorities and public security services only. Outsourcing should generally be avoided in order not to circumvent parliamentary control functions recommended by the European Commission for Democracy through Law (Venice Commission) in its 2008 report on the democratic control of the armed forces.[13]

10. As rapporteur of the Committee on Legal Affairs and Human Rights, Pieter Omtzigt (Netherlands, EPP/CD) is also preparing a report on "Improving the protection of whistle-blowers"[14] in parallel to this report on mass surveillance. Both reports reflect largely on a legal analysis of the acts committed by Edward Snowden. Besides the huge amount of copied intelligence data Mr Snowden took with him when leaving the United States for China and finally Russia at the end of June 2013, he would obviously be of great strategic value for the Russian security services because of his personal experience and knowledge as a key collaborator of US intelligence services. This knowledge has probably already been used in order to expose international intelligence structures and improve Russian intelligence operations in cyberspace. Given the dismal record of the Russian authorities in relation to transparency and access to information, it is unlikely that general support for whistle-blowing and altruism guided the Russian authorities when granting Edward Snowden asylum, a residence permit, housing and remunerated work in Russia.

---

6. See, for example, Weber and Saravia v. Germany (Application No. 54934/00), op. cit.
7. See the analysis of case law by the European Court of Human Rights of 2013, published by the Court's Registry, www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20(final).pdf.
8. www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.
9. https://eu2015.lv/images/Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf.
10. www.bbc.com/news/world-us-canada-26975845.
11. http://ecrgroup.eu/news/european-parliament-agrees-to-reach-passenger-name-records-agreement-this-year/.
12. *The Guardian*, 11 June 2013, www.theguardian.com/world/2013/jun/10/obama-pressured-explain-nsa-surveillance.
13. www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2008)004-e.
14. See the corresponding motion for a recommendation by Andrej Hunko (Germany, UEL) and others, Doc. 13278**.**

11. In conclusion, it is worth recalling in the current context another citation from the judgment of the European Court of Human Rights in *Klass and others v. Germany* (Application No. 5029/71): “The Court, in its appreciation of the scope of the protection offered by Article 8 [of the European Convention on Human Rights], cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction.” This citation is timelier today than ever before.

3. Specific explanations of the amendments

(A) The draft resolution speaks in paragraph 2 of “the lack of adequate legal regulation and technical protection at the national and international level”, but the report does not provide evidence for such a harsh and categorical judgment. In fact, the Council of Europe has produced international treaties which offer legal protection, such as the European Convention on Human Rights and the Convention on Cybercrime (ETS No. 185).

(B) Paragraph 7 presents an unsupported series of assertions. They must either be substantiated or this paragraph must be deleted.

(C) Paragraph 11 of the English version speaks of “effective, targeted surveillance of suspected terrorists or other organised criminal groups”. It is important to have targeted surveillance of suspected terrorists AND suspected members of organised crime.

(D) Trust among the transatlantic partners can only be established by concluding adequate legal frameworks. The Council of Europe offers a number of relevant legal treaties which are open to signature by non-member States, in particular the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30), the European Convention on the Suppression of Terrorism (ETS No. 90), the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141) and on the Financing of Terrorism, the Convention on Cybercrime and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. It is therefore necessary to base future co-operation on mutual agreements rather than mere trust.

(E) The right to “whistle blow” cannot be afforded unqualified protection as this could lead to the sale of confidential and sensitive information in self-interest. This amendment is based on Assembly Resolution 1729 (2010) on protection of whistle-blowers.

(F) Following the Snowden disclosures, the US President announced in January 2014 that the NSA practice would be changed and procedures amended regarding the US Foreign Intelligence Surveillance Court. The US Congress started an inquiry into the facts as did the governments of France, Germany, Spain and other countries. In addition, there is no indication of “harsh treatment” of Edward Snowden. As he is in Russia since the end of June 2013, such harsh treatment cannot *de facto* be pursued outside Russia, and the report does not provide details of his treatment in Russia.

(G) While there is no reason for the Assembly to believe that the inquiry committee of the German Parliament would not be capable of assuming its parliamentary role, reference should instead be made to the need for democratic parliamentary oversight of the security services and armed forces in member States. The latter was thoroughly analysed and recommended in the report on the democratic control of the armed forces adopted by the Venice Commission in 2008. In addition, it is important to remind governments of the potential risk of out-sourcing intelligence operations to private firms which are not under such democratic control.

(H) Through its resolution of 12 March 2014, the European Parliament had invited the Secretary General of the Council of Europe to launch a procedure against States Parties under Article 52 of the European Convention on Human Rights. I assume that such an inquiry has not been initiated for good reasons, because several national parliaments and governments in member States have since held debates about their co-operation with the US National Security Agency and other foreign intelligence services. In this field, a lot depends also on progress in co-ordination of EU policies and legislation. Therefore, we should not insist on this request to the Secretary General

(I) In 2013, the European Parliament had blocked the proposal to exchange cross-border passenger data between the European Union and the United States. Shortly after the attacks on *Charlie Hebdo* on 7 January 2015, the President of the EU Council called on the European Parliament to speed up work on the EU

Passenger Name Record (PNR) system. This call on the EU institutions was also made by the ministers of the interior meeting in Paris on 11 January 2015. Such work should be linked to the finalising of the General Data Protection Regulation of the European Union and its accession to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

(J) Article 8 of the European Convention on Human Rights contains the right to the protection of the confidentiality of correspondence, but the term “mail secret” does not exist and may be misleadingly narrow.

(K) In its Resolution 1729 (2010) on protection of whistle-blowers, the Assembly thoroughly dealt with the issue of whistle-blowing in view of the standards of the Council of Europe. Therefore, it is necessary for the Assembly to recall this resolution in this context. The granting of asylum to Edward Snowden has been refused by several countries on legal grounds. Even Russia has changed his status from asylum seeker to resident of Russia. Finally, most countries in the world would not grant asylum to people on the basis that they claim to be possibly subjected to unfair prosecution, especially if agreements on mutual legal assistance exist such as between the United States and many European countries

(L) There can be circumstances where, for political or diplomatic reasons, surveillance is justified. That justification cannot, however, be extended to industrial espionage.