EUROPEAN PARLIAMENT

The ECHELON Affair

The EP and the global interception system 1998 - 2002

STUDY

European Parliament History Series

EPRS | European Parliamentary Reserch Service

Authors : Franco Piodi and Iolanda Mombelli
Historical Archives Unit
November 2014 – PE 538.877

Historical Archives Unit of the European Parliament
European Parliament History Series
November 2014

The ECHELON Affair

The European Parliament and the Global Interception System

Study

EPRS | European Parliamentary Research Service

EUROPEAN PARLIAMENT

Authors: Franco PIODI and Iolanda MOMBELLI

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR PARLIAMENTARY RESEARCH SERVICES

HISTORICAL ARCHIVES UNIT

arch-info@europarl.europa.eu

Cover: http://en.fotolia.com/ - Fotolia_49113209 © Maksym Yemelyanov

Luxembourg: Publications Office of the European Union.

PE 538.877
ISBN: 978-92-823-6260-0
DOI: 10.2861/76176
CAT: QA-02-14-934-EN-N

Printed in Luxembourg

Summary

During the second half of the 1990s press and media reports revealed the existence of the Echelon network. This system for intercepting private and economic communications was developed and managed by the states that had signed the UKUSA and was characterised by its powers and the range of communications targeted: surveillance was directed against not only military organisations and installations but also governments, international organisations and companies throughout the world.

This study recounts the uncovering of the network, notably through the STOA investigations, questions by MEPs, debates in plenary, the setting up of a temporary committee and the final position adopted by the European Parliament. It also takes account of statements by researchers and journalists on the technical aspects and legal implications of the Echelon network. Finally, it considers the views of the political groups in the European Parliament and of the Commission and Council.

Fifteen years after the events, *The Echelon Affair* draws on the European Parliament's archives to describe and analyse a worldwide scandal which had an impact on the history of Parliament and which today is echoed in the revelations of Edward Snowden and Julian Assange and in other cases of spying on a grand scale.

CONTENTS

INTRODUCTORY REMARKS

This Historical Archives study considers the Echelon affair, which took place on the cusp of two millennia, galvanised European politicians and inflamed public opinion in a way achieved by few other parliamentary initiatives. It mainly covers the work of a temporary committee on Echelon, which operated between 2000 and 2001, but also considers the period from 1998 (publication of the first STOA document on Echelon) to 2002, the year in which the European Parliament adopted a resolution at the end of the temporary committee's period of work, criticising the way the Commission and Council had followed up the resolution it had adopted the previous year.

This study is based almost entirely on European Parliament documents, mostly documents produced by the Echelon temporary committee or documents submitted to it from external sources. It should be pointed out that the committee minutes are written in an abridged style and, with a few exceptions, do not allow for reconstruction of the debates. Consequently we have mainly used the documents tabled in plenary.

From the point of view of accessibility, these documents fall into two categories:

- parliamentary debates and minutes, the final report of the Echelon temporary committee (Schmid report), parliamentary questions, motions for resolutions and resolutions (i.e. all the documents tabled or considered in plenary sitting, which are available in the Official Journal of the European Union or on the European Parliament website: http://www.europarl.europa.eu

- records and documents of the Echelon temporary committee and other documents conserved by the European Parliament's Historical Archives. Members of the public can obtain access on request to the documentation service, provided that the author has not classified the documents as confidential and they do not relate to meetings of the Echelon Committee held in camera or are not considered to be confidential at the time the request is made. Some of these documents are also available online on the European Parliament website, where you can find more information about the committee: http://www.europarl.europa.eu/comparl/tempcom/echelon/default.htm

ABBREVIATIONS

CIA	Central Intelligence Agency
COMINT	Communications intelligence
EDD	Group for a Europe of Democracies and Diversities
ELDR	Group of the European Liberal, Democrat and Reform Party
GCHQ	Government Communications Headquarters
GUE/NGL	Confederal Group of the European United Left/Nordic Green Left
NSA	National Security Agency
NATO	North Atlantic Treaty Organisation
CFSP	Common Foreign and Security Policy
PESD	European Security and Defence Policy
PPE-DE	Group of the European People's Party and European Democrats
PSE	Group of the Party of European Socialists
RDE	Group of the Democratic Alliance
STOA	Scientific and Technological Options Assessment
TDI	Technical Group of Independent Members – mixed group
UEN	Union for Europe of the Nations Group
UKUSA	United Kingdom-United States of America Agreement
Verts/ALE	Greens/European Free Alliance

CHAPTER I

THE ECHELON SYSTEM IN STOA STUDIES AND THE FIRST PARLIAMENTARY REACTIONS

1. Echelon: the general context

The name Echelon refers to a system for the interception of telecommunications created and managed by the USA in cooperation with its partners among other Western powers. It is used to intercept telephonic communications (conversations and faxes) and e-mail messages from other countries, including allies.

In 1996, when there were already critical rumours in the press about the existence of the system, the STOA Panel[1], on the proposal of British MEP Glyn Ford, tackled the subject in a general study entitled *An Appraisal of Technologies of Political Control*. This was published in 1998 and led to consideration of the rumours at political level. The study dealt with the subject of interception in general. However, two pages (pp. 19 and 20) on national and international communications interception networks revealed for the first time in a semi-official piece of grey literature the existence of the Echelon system. The key passage was the following:

The Echelon system forms part of the UKUSA system but unlike many of the electronic spy systems developed during the cold war, Echelon is designed for primarily non-military targets: governments, organisations and businesses in virtually every country. The Echelon system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex[2].

In 1999 a second document entitled *Development of Surveillance Technology and Risk of Abuse of Economic Information* was published. This expanded on the topics indicated in the title[3].

These studies enable one to grasp not only Echelon's capacity for the collection and analysis of private communications but also the institutional framework in which the system operated. Institutional framework means the intelligence services and their international networks. The term 'international networks' must be understood in this context as meaning a system of agreements between the services not subject to the normal supervision that national parliaments exercise over their states' foreign policy.

Echelon's intelligence operations covered the collection of technical and secret information in foreign communications by individuals other than the recipients of those communications (COMINT)[4]. Echelon was thus a COMINT system set up under the secret agreement known as UKUSA[5] between the British and American COMINT systems; Canada, Australia and New Zealand later joined the agreement. The most important US framework for COMINT and the management of Echelon was the NSA, the British

---

[1] *Scientific and Technological Options Assessment (STOA)* a department in the European Parliament's Directorate-General for Research that is responsible for drawing up studies on the technical and scientific aspects of Community policies, under the guidance of a group of MEPs.

[2] Wright, Steven, *An Appraisal of Technologies of Political Control – Interim study*, Working document for the STOA Panel, European Parliament, Directorate General for Research - PE 166.499/Int.St. - Luxembourg, 19 January 1998.

[3] *Development of Surveillance Technology and Risk of Abuse of Economic Information – Appraisal of Technologies of Political Control (Volumes 1 to 5)*. Working document for the STOA Panel, European Parliament, Directorate General for Research, PE 168.184 (DG-4-JOIN_ET - 1999).

[4] About 30 states carry out COMINT activities: apart from the USA and its allies, the main one is Russia, but China also operates a powerful system. Mention should also be made of NATO countries outside Echelon that carry out their own independent COMINT operations, such as France and Germany.

[5] The secret agreement was signed in 1947 and made public in 1999 when the Australian Government confirmed its existence.

counterpart of which was GCHQ. In terms of quantity, STOA estimated that the UKUSA system managed 120 data-collecting satellite systems, 40 of them targeting Western commercial communication satellites.

Technically, Echelon's COMINT activities seemed to be characterised by the capacity to select from the messages intercepted those that were important for the users and therefore needed to be analysed. The selection basically consisted of automated processing of control lists, in other words names of people and organisations associated with the intercepted message. Automated processing was needed because of the enormous quantity of intercepted messages; it facilitated the detection of those relating to organisations or topics subject to monitoring. However, at the end of the 1990s, when the STOA documents were being drawn up, searches by key words and the capability to recognise a word in a telephone conversation were impossible, contrary to reports in the press; however, it was possible to carry out searches on the subject of a conversation.

In terms of the uses made of Echelon, industrial espionage attracted the most attention because it also affected private individuals and fair competition – giving companies taking part in Echelon an unfair advantage that was difficult to offset.

The NSA does not conceal the fact that it collects industrial intelligence, using the justification that, as part of the high throughput, civilian communications are mixed in with military and political communications, but it has denied conducting a policy of acting specifically in response to the interests of particular companies. However, each country in the UKUSA authorised its services and ministers to plan and receive economic information not gathered by chance, leading an American authority to advocate industrial espionage as an element in the protection of national security. The UK and Australia also engage in industrial espionage[6].

The 1999 STOA document mentioned some specific cases of industrial espionage that were subsequently communicated to the Advocacy Center, a unit of the US Department of Commerce, which gave US companies an advantage in securing overseas contracts:

- in 1993, the Panavia company was targeted over sales to the Middle East;
- in 1994, the NSA intercepted telephone calls between Thompson CSF and Brazil concerning a contract for a surveillance system for the Amazonian rain forest; bribery was alleged to have taken place; the contract was eventually awarded to a US company that had cooperated on the Echelon system;
- there were reports of a similar interception of communications between Airbus, the Saudi national airline and the Saudi Government in 1995: in this case too, the revelation that bribery had taken place was used to get the contract awarded to the US companies Boeing and McDonnell Douglas Corp;
- reputable sources have also cited occasions when espionage has been used in international negotiations, in particular the interception of communications on emission standards of Japanese vehicles, trade negotiations on the import of Japanese luxury cars, French participation in the GATT trade negotiations in 1993 and the Asian-Pacific Economic Conference (APEC).

[6] STOA, PE 168.184, vol. 2/5, point 5: COMINT and economic intelligence.

2. The first reactions: parliamentary questions and the resolution of September 1998

The first STOA document raised considerable concern amongst MEPs, giving rise to a series of parliamentary questions between 1998 and 1999, mostly questions for written answer, but some for Question Time; apart from one to the Council, all were addressed to the Commission. The content of the questions anticipated the debate on Echelon that would be held in 2000 and 2001. It will be noted that all the questions came from the Italian right, the Greens and the GUE Group, with the exception of two questions from a Dutch Liberal and a French MEP from the RDE Group[7].

The aspects raised in the questions ranged from the existence of Echelon and spying activities by the British intelligence services to the Commission's ability to protect its confidential communications and the Member States, and to whether the public could use advanced encryption systems as a means of protection against spying.

The Commission's replies were evasive and stated that these questions did not fall within its remit, claiming that it could not act on the basis of non-official information. Its replies indicated its unease about Echelon.

Only one question was put to the Council, which replied laconically: *The Council is not aware of the matters mentioned by the Honourable Member*[8].

MEP Nel van Dijck (Netherlands) submits two questions to the Commission for written answer on MI6 and Echelon eavesdropping. © European Union, 1998

[7] Written Questions 1039/98 and 1040/98 by Nel van Dijk to the Commission: *Eavesdropping by MI6 and Echelon*, OJ C 354, 19.11.1998, p. 55. Written Question 1306/98 by Cristiana Muscardini and others to the Commission: *The Echelon system and spying activities directed against EU countries*, OJ C 402, 22.12.1998, p. 9. Written Questions 1775/98 and 1776/98 by Lucio Manisco to the Council and Commission: *Echelon spying system*, OJ C 13, 18.1.1999, p. 81, and OJ C 50, 22.2.1999, p. 90. Written Question 2329/98 by Nikitas Kaklamanis to the Commission: *Echelon network*, OJ C 50, 22.2.1999, p. 142. Written Questions 1894/98 and 2966/98 by Esko Seppänen to the Commission: *EU involvement in covert electronic communications interception*, and *Electronic eavesdropping*, OJ C 142, 21.5.1999, pp. 3 and 63. Written Question 337/99 by Giuseppe Rauti to the Commission: *US espionage system in Europe*, OJ C 341, 29.11.1999, p. 94. Question at Question Time 101 (H-0092/99) by Ioannis Theonas: *Infringement of individuals' privacy*, Debates of the European Parliament, 4-533, 10.2.1999, p. 258. Question at Question Time 69 (H-1067/98) by Patricia McKenna: *Electronic and electromagnetic security of EU institutions*, Debates of the European Parliament, 4-530, 16.12.1998, p. 238.

[8] Written Question 1775/98 to the Council by Lucio Manisco.

The unease was very probably due to the need not to upset relations with the UK, whose involvement in the Echelon system is clear from the STOA documents, or with the USA at a time when transatlantic relations were going through a particularly difficult period. This unease can also be seen in the discussion on the first European Parliament resolution on transatlantic relations/Echelon system, of 16 September 1998, which mentioned Echelon although only incidentally[9].

During the sitting of 14 September 1998, Commissioner Bangemann spoke on transatlantic relations and the Echelon system in a statement deliberately separate from the initial statement on transatlantic relations and the final statement that showed the Commission's degree of interest in Echelon; the Commission said it could base its actions only on information obtained from official sources, not information from press sources or studies. Moreover no Member State, no EU undertaking and no EU citizen had provided any evidence of the existence of the Echelon system nor of the fact that it was still operational.

While the Commission and Council showed caution over Echelon, Parliament also took a cautious stance in a resolution that did not criticise the function of electronic surveillance but recognised its 'vital role' *in stopping and preventing the activities of terrorists, drug traffickers and organised criminals*[10]; it was, however, crucially important to have democratically accountable systems of control. Parliament called for an open debate at both national and EU level and the adoption of a code of conduct in order to ensure redress in cases of malpractice or abuse and, with specific reference to Echelon, *protective measures concerning economic information and effective encryption*.

3. First signs of the debate being reopened in 2000

After the resolution in 1998 and the questions in the first quarter of the following year, the electoral campaign for the 1999 European elections and the start of the new parliamentary term relegated the debate on Echelon to the background but it reopened even more actively at the beginning of 2000. The debate was relaunched by a Committee on Civil Liberties hearing on the European Union and data protection, during which the second STOA text on Echelon was presented, the existence of Echelon having by then been confirmed by American sources[11]. The Committee on Civil Liberties hearing ended with a statement by committee chairman Graham Watson, which made two main points: European companies that had been victims of industrial espionage because of Echelon were invited to make their cases known, as the second STOA document did not contain sufficiently detailed information on this subject; and, with regard to parliamentary business, it was now for the political groups to decide what further action should be taken on Echelon[12].

---

[9] Debates of the European Parliament 4-524 of 14 September 1998, pp. 14-24, and European Parliament resolution of 16 September 1998, OJ C 313, 12 October 1998, p. 98. The resolution was adopted at a time when transatlantic relations were being disturbed by the Helms-Burton Act under which the USA took measures against non-US companies that maintained normal trade relations with Cuba.

[10] European Parliament resolution of 16 September 1998, OJ C 313, 12.10.1998, p. 99.

[11] Report on the hearing on *The European Union and data protection*, 22 and 23 February 2000, Brussels, PE5 AP PV/LIBE.1999 LIBE-20000222-2 0005 and *Hearing in Parliament on 22 and 23 February*, Agence Europe, 5 February 2000. For the STOA text, see p. 9 of this study.

[12] *EP/Privacy – Echelon case creates a stir at the hearing: plenary debate on 30 March 2000*, Agence Europe, 24 February 2000.

The first decision was to hold a debate on the subject (which was scheduled for 30 March 2000) but, around the same time as the hearing, the views of leading politicians became clear. The President of the European Parliament, Nicole Fontaine, said: *One may legitimately feel scandalised that this espionage, which has gone on over several years, has not given rise to official protests. For the European Union, essential interests are at stake. On the one hand, it seems to have been established that there have been violations of the fundamental rights of its citizens, on the other, economic espionage may have had disastrous consequences, on employment for example*.[13]

[13] *EU/'Echelon Affair' – Following EU hearing, Fontaine wonders what comes next,* Agence Europe, 25 February 2000.

CHAPTER II

THE PERIOD LEADING TO THE SETTING UP OF THE ECHELON COMMITTEE

1. The debate in plenary on 30 March 2000

We now come to the debate on 30 March 2000 on the statements by the Council and the Commission on the existence of an artificial intelligence system allowing the United States of America to intercept and monitor all telephone and electronic communications within the European Union, a system called 'Echelon': the debate was wound up by four motions for resolutions. Three motions were tabled calling for the setting up of a committee of inquiry but they were not successful[14].

The President-in-Office of the Justice and Home Affairs Council, Fernando Gomes, made a statement that almost all the Members who spoke after him found inadequate as it did not define a position on specific responsibilities in relation to Echelon and Mr Gomes referred to the 'possible existence of the Echelon system'. However, he was clear on the general principle of interception: *The Council cannot accept the creation or existence of such a system which does not respect the laws of the Member States [...]*.

Members were also unenthusiastic about the Commissioner Liikanen's statement. Mr Liikanen did not even mention Echelon, but reported on a response, in a letter from the Permanent Representative of the UK to the European Union, to the Commission's requests for clarification. The letter stated that the British intelligence agencies worked within a legal framework laid down by the UK Parliament that set out explicitly the purposes for which interception might be authorised, that there was a special parliamentary oversight committee and that the European Commission of Human Rights had held that the system set out under British law was in conformity with the European Convention on Human Rights.

Mr Liikanen also said that the Commission had received a letter from the US Department of State asserting that the US intelligence community was not engaged in industrial espionage and that the US Government and the intelligence community did not accept tasking from private firms.

The ensuing debate primarily revolved around what more could be done in the Echelon case.

Ms Klamt (Germany, PPE-DE), who felt that the Council and Commission had delivered clear opinions, spoke about the proposals to set up a committee of inquiry, which she thought would serve no purpose. She was primarily concerned about industrial espionage and advocated an international approach, with the subject being put on the agenda of the World Trade Conference.

Mr Schulz (Germany, PSE) was not impressed by the Council and Commission statements but was more cautious about the committee of inquiry *because, if such a committee were to be set up, its legal basis would have to be impeccably clarified*.

Speaking on behalf of the ELDR Group, Mr Wiebenga (Netherlands) was also dissatisfied with the statements by Mr Gomes and Mr Liikanen and said the matter must be taken seriously – *because if it is true, then citizens' rights may be violated too.*

---

[14] Debates of the European Parliament, 30 March 2000. The three motions in favour of setting up a committee of inquiry were tabled by the Italian members of the UEN Group (B5-0287/2000), several members of the GUE/NGL Group (B5-0294/2000) and some members of the Verts/ALE Group (B5-0302/2000); the fourth motion (B5-0290/2000) was tabled by members of the TDI Group. A fifth motion, which was never tabled officially (B5-0398/2000) was approved by the Committee on Civil Liberties on 11 April 2000 (see minutes PE5 AP PV/LIBE.1999 LIBE-20000411 0010).

Mr Lannoye, Chair of the Verts/ALE Group, was disappointed by the statements and had no regrets about having taken the initiative, with his group, in calling for a committee of inquiry. *We have ... discovered that this system does exist, but we do not know exactly how it works. There is good reason to believe that ... the United Kingdom ... is collaborating in the system.*

Mr Wurtz, Chair of the GUE/NGL Group, described the statements by the Council and Commission as 'embarrassed' and 'tangled'. On the setting-up of a committee of inquiry, he said: *Whether people like it or not, the Echelon file is now open and it will remain open*.

Mr Berthu (UEN) was *stunned by the Council's statement* and supported his group's call for a committee of inquiry.

Mr Belder (EDD) was exercised less about the existence of techniques for interception than about the legitimacy of their usage: *These techniques must not be used in the pursuit of profit. The right of individuals to privacy must not be contravened at the drop of a hat.*

Mr Martinez (TDI) spoke out strongly to draw a distinction between notions of competition and competitiveness and the practice of industrial espionage, and to contrast the principle of solidarity in the European Community with the transatlantic solidarity practised by the UK.

One voice was raised in defence of the UK. Mr Robert Evans (UK, PSE) said the Council and Commission had made very clear statements and added: *As Mr Liikanen has said, everything done in the United Kingdom is in line with a proper legal framework. Everything is subject to close parliamentary scrutiny in the House of Commons. We have very tight controls, both independent controls and control that emanates from the Secretary of State with the full consent of the United Kingdom Government.*

2. Committee of inquiry or temporary committee?

Voting on the motions for resolutions tabled for the debate on 30 March was held over to the May 2000 part-session and eventually did not take place, but the fundamental question, the setting-up of a committee of inquiry on the Echelon case, was entered on the agenda of three meetings of the Conference of Presidents on 13 April, 11 May and 15 June 2000.

The President of Parliament received two requests to set up a committee on Echelon. The first, seeking the setting-up of a committee of inquiry, came from Mr Lannoye, Chair of the Verts/ALE Group, and obtained 170 signatures.[15]

The reasons given were based on Rule 151 of Parliament's Rules of Procedure, which made provision for committees of inquiry to investigate contraventions of Community law; the Community legislation likely to have been infringed by Echelon was cited. The legal bases were Article 6 of the EU Treaty on respect for fundamental rights, including respect for private life, and Article 286 of the EC Treaty, which makes provision for an independent supervisory body responsible for monitoring the application of Community rules on the processing of personal data[16]; on the basis of this provision, the proposal to set up a committee of inquiry would show that the Community institutions were ready to take the measures needed to ensure the security of the services that they supplied.

[15] Letter of 27 March 2000 to Nicole Fontaine, President of the European Parliament, PE5 OD PV/CPRG CPRG-20000413 0070. The minimum number of signatures required under Rule 151 of the Rules of Procedure was a quarter of the Members, which in 2000 amounted to 157.

[16] Particular reference was made to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, pp. 31-50), and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1997, pp. 1-8).

Another point in justification of setting up the committee was violation of Article 81 of the Treaty, prohibiting practices that had as their object the distortion of competition, which appeared to be the case with Echelon.

The second request was submitted by the Spanish Chair of the PSE Group, Enrique Barón Crespo[17], who proposed the setting-up of a temporary committee[18] with the following mandate:

- *political initiatives to ensure a climate of better trust in cooperation between the Member States;*
- *measures to prevent non-member countries from carrying out any form of interception in the territory of the Union beyond that required by joint measures to combat organised crime; measures required to ensure the protection of privacy*;
- *legislative measures to update and harmonise provisions on the protection of personal data*;
- *appropriate measures concerning the adoption of tools and technologies (cabling, encryption) to counteract interception by non-member countries*.

Thus those requesting a committee of inquiry thought that the Echelon system was in violation of Community law and that the Rules of Procedure made specific provision for investigating the matter.

On the other hand, the reasons given for setting up a temporary committee related to the limitations on the mandate of committees of inquiry: they could investigate violations of Community law under the EC Treaty (Article 93) and could accordingly consider only matters governed by it. Matters falling under Title V and Title VI of the Treaty on European Union (respectively, common foreign and security policy and police and judicial cooperation in criminal matters) would be excluded.

However, it is reasonable to suppose that the concern not to damage relations with the UK – which would inevitably have been accused if a committee of inquiry had been set up – played a role in the choice of the large parliamentary groups in which almost all the British MEPs were concentrated.

Finally, it may be useful to consider the main powers of a committee of inquiry set up on the basis of a 1995 joint decision by the three EU political institutions[19]. Article 3 of that decision regulates arrangements for the appearance before the committee of inquiry of officials of the institutions and Member States who are authorised to appear by the institution or Member State *unless grounds of secrecy or public or national security dictate otherwise by virtue of national or Community legislation*. These restrictions also apply to the obligation on institutions and Member States to provide the committee of inquiry with the documents needed for its work.

In view of the particular nature of the Echelon affair, it is highly likely that a committee of inquiry would have been confronted to a large extent by the restrictions described, and it may thus be presumed that the choice of a temporary committee reflected political considerations, as suggested above, rather than efforts to get round the 1995 decision. On the other hand, whereas a committee of inquiry, despite the restrictions, can see the

---

[17] Letter of 13 April 2000 to Nicole Fontaine, President of the European Parliament, PE5 OD PV/CPRG CPRG-20000615 0070.

[18] Pursuant to Rule 150(2) of its Rules of Procedure, June 1999: '[…] Parliament may at any time set up temporary committees, whose powers, composition and term of office shall be defined at the same time as the decision to set them up is taken'.

[19] Decision of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry (95/167/EC), OJ L 113, 19.5.1995, pp. 1-4. For this study we have consulted Annex VIII to the European Parliament's Rules of Procedure, June 1999.

documents required for its work, a temporary committee can use only documents in the public domain.

At its meeting of 13 April 2000, the Conference of Presidents rejected the proposal to set up a committee of inquiry and approved the creation of a temporary committee: a decision was taken accordingly on 15 June. Both decisions by the Conference of Presidents – rejection of a committee of inquiry and the setting up of the temporary committee – were approved by Parliament on 5 July 2000.

3. The mandate and the members of the temporary committee

On the basis of Parliament's decision[20], the Echelon Committee was set up with the following mandate:

- *to verify the existence of the communications interception system known as Echelon [...];*
- *to assess the compatibility of such a system with Community law, in particular Article 286 of the EC Treaty and Directives 95/46/EC and 97/66/EC, and with Article 6(2) of the EU Treaty, in the light of the following questions:*
- *are the rights of European citizens protected against activities of secret services?*
- *is encryption an adequate and sufficient protection to guarantee citizens' privacy or should additional measures be taken and if so what kind of measures?*
- *how can the EU institutions be made better aware of the risks posed by these activities and what measures can be taken?*
- *to ascertain whether European industry is put at risk by the global interception of communications;*
- *possibly, to make proposals for political and legislative initiatives.*

Carlos Coelho, chairman of the Temporary Committee on the Echelon Interception System, 2000-2001. © European Union, 2011

The mandate was for 12 months, the maximum period permitted under Rule 150. The 36 committee members were[21]:

[20] European Parliament decision setting up a temporary committee on the Echelon interception system (B5-0593/2000/rev.), OJ C 121, 24.4.2001, p. 131.

[21] The names of substitute members, who are not counted among the 36 members, are shown in italics.

14 members from the PPE-DE Group[22]: Banotti, von Boetticher, Cederschiöld, Coelho, Deprez, Dimitrakopoulos, Hernández Mollar, Klamt, Hugues Martin, Oostlander, Palacio Vallelersundi, Pirker, Van Velzen, Zappalà, *Buttiglione*, *Cornillet*, *Gawronski*, *Giannakou-Koutsikou*, *Nassauer*, *Posselt*, *Johan Van Hecke*;

11 members from the PSE Group[23]: Berger, Robert Evans, Karamanou, Catherine Lalumière, Lund, Erika Mann, Medina Ortega, Paasilinna, Gerhard Schmid, Vattimo, Wiersma, *Andersson*, *Caudron*, *Ford*, *Gebhardt*, *Marinho*, *Paciotti*, *Swiebel*, *Swoboda*, *Terrón i Cusí*, *Thielemans*, *Titley*;

3 members from the ELDR Group: Di Pietro, Flesch, Plooij-van Gorsel, *Andreasen*, *Thors*, *Dybkjær*;

3 members from the Verts/ALE Group[24]: Ceyhun, MacCormick, McKenna, *Boumediene-Thiery*, *Ilka Schröder*, *Lambert*;

2 members from the GUE/NGL Group: Di Lello Finuoli, Krivine, *Frahm*, *Papayannakis*;

1 member from the UEN Group: Berthu[25], *Nobilia*;

1 member from the TDI Group: Turco, *Frank Vanhecke*;

1 member from the EDD Group: Belder, *Okking*.

At its constituent meeting on 6 July 2000 the Temporary Committee on the Echelon Interception System elected Carlos Coelho as chairman and Elly Plooij-van Gorsel, Neil MacCormick and Giuseppe Di Lello Finuoli as vice-chairwoman and vice-chairmen. Gerhard Schmid was appointed rapporteur.

Mme Elly Plooij-van Gorsel, vice-présidente de la commission temporaire sur le système d'interception Echelon 2000-2001. © Union européenne, 2003

[22] Apart from the substitutes mentioned below, a later list of members shows some changes of name among the PPE-DE Group's substitute members, but there are no particular references to this in Parliament's archives. Mr Nassauer no longer appears and Mr Bradbourn, Mr Jean-Pierre, Ms Matikainen-Kallström and Ms Oomen-Ruijten appear. In the decision relating to the setting-up of the committee, the PPE-DE Group did not use all the possibilities open to it to provide substitute members.

[23] This number increased to 12 when Mr Ceyhun joined the group.

[24] The Verts/ALE Group had only two members when Mr Ceyhun left to join the PSE Group.

[25] After leaving the UEN Group (30 January 2001), Mr Berthu was replaced by Mr Marchiani whose name does not appear on the later list of members. No trace of this replacement has been found in the European Parliament's archives.

4. The working method and programme

The working method and programme were the focus of discussions at the committee's meetings of 5, 11 and 12 September 2000. We have the minutes, the notes for the chair, draft timetables and work programme, and a working document by the rapporteur that consists of a summary of the work programme and the working methods that were ultimately approved.

The minutes record the chairman reminding the members of the need to ensure that the committee was seen as a credible structure and that its credibility would be a fundamental resource in obtaining the necessary information. That credibility lay primarily in the capacity of the committee as a whole, and the capacity of each of its members, to respect the confidentiality of documents received and points raised at meetings held in camera. The decision to hold meetings in camera would be taken by the Bureau on the chairman's proposal[26]. The committee would provide assurances for people outside Parliament who presented confidential documents that they would be released to committee members or third parties only within limits defined when the documents were forwarded. This guarantee went beyond the provisions of Annex VII to Parliament's Rules of Procedure[27], to which the minutes explicitly referred.

It is in this context that we should consider the nine-point work programme, which mirrors the framework adopted by the rapporteur[28]:

a) What we know with certainty about the Echelon system;

b) Discussion in other Parliaments and on the level of governments;

c) Activities of intelligence agencies;

d) Possibilities of interception of communication systems and their infrastructure;

e) Encryption;

f) Economic espionage;

g) Targets of espionage and their protection measures;

h) Legal questions regarding privacy;

i) Discussion about recommendations and proposals.

The level of detail in working document No 1 contrasts with that in the preliminary draft working programme. This suggests that the committee held a much more detailed discussion than is revealed in the minutes.

[26] The Bureau's role in approving the holding of meetings in camera was decided by the committee, probably by consensus, as the minutes do not mention a vote on the subject.

[27] Procedure for the consideration of confidential documents communicated to the European Parliament.

[28] Aide-memoire: meeting of the Echelon Committee and draft working programme, PE5 AP PV/ECHE.2000 ECHE-20000905 0050.

CHAPTER III

THE COMMITTEE'S CONSULTATIONS

1. Contributions from experts: questions concerning the Echelon system

The Echelon Committee held a number of hearings of experts, who drew on their experience as consultants for public bodies and private firms, as researchers and as journalists who had investigated Echelon. All had used as the basis for their research open, public sources, which, if monitored regularly and analysed correctly, still provided worthwhile information.

Specific mention should be made of three experts, given the part they had already played in the drafting of the STOA documents.

The first is Duncan Campbell, the journalist who revealed the Echelon affair and who had been involved in the drafting of the STOA documents. He emphasised the role played by Echelon in the context of industrial espionage, and commercial espionage in particular, highlighting the links with the activities of the US Department of Commerce and the damage caused to the European economy. Echelon was not used to intercept all data; instead, the focus was on pre-defined priorities and requests from 'clients'. In particular, he drew attention to the many successes scored by the US Government's Advocacy Center, whose remit was to support US firms in their commercial dealings abroad, which apparently included making use of the Echelon system[29].

The second expert, James Bamford[30], gave a detailed account of the US espionage system. The NSA was a larger espionage agency than the CIA. Its task was to collect intelligence and, in Mr Bamford's view, it represented a more serious threat to the privacy of individuals than to the activities of firms. He said that the information about non-US firms which the NSA sought to obtain related primarily to attempts to circumvent the economic sanctions imposed on certain countries and that he had no proof that the NSA passed on information to US firms.

The third expert, Nicky Hager, a researcher and investigative journalist from New Zealand, analysed the situation as regards interceptions in the South Pacific region and relations between the USA, the UK, Canada, Australia and New Zealand from the point of view of industrial espionage. He said that, according to his sources, his country, as a member of the UKUSA alliance, carried out monitoring on the grounds that if it failed to play its role it might gradually be excluded from the agreement. On the basis of the information he had collected, and by analogy, he concluded that the situation in Europe was comparable to that in the South Pacific[31].

---

[29] Mr Campbell produced a number of documents which were included in the file for the meeting held on 22 and 23 January 2001, PE5 AP PV/ECHE.2000 ECHE-20010122.

[30] American investigative journalist and author of two books, one on the NSA, which appeared in 1982, and the other, *Body of Secrets*, which was published after his hearing on 23 April 2001. As regards his hearing, we have the minutes of the Echelon Temporary Committee, PE5 AP PV/ECHE.2000 ECHE-20010423 0010, which are more detailed than the other documents, and an aide-mémoire from the committee secretariat, see PE5 AP PV/ECHE.2000 ECHE-20010423 0025.

[31] Nicky Hager has written a number of books, including *Secret Power: New Zealand's Role in the International Spy Network*, Nelson 1996, quoted in the 1998 STOA document. He was heard by the Echelon Committee on 23 April 2001 and a record of his statement is available in English, PE5 AP PV/ECHE.2000 ECHE-20010423 0026.

The minutes of the meeting of 12 October 2000, at which a first group of experts were heard, are rather succinct, but another document[32] gives an overview of the way the Echelon system was used to carry out industrial espionage to the benefit of US firms and, more generally, of the system and the methods employed by the USA in order to monitor flows of economic information, sometimes for the purpose of fighting international crime and corruption.

Another external source document which is worthy of mention is the *Rapport complémentaire d'activités 1999* (*Additional activity report 1999*) of the Standing Control Committee for the Belgian Intelligence Services[33], which is not a study of the activities of the Belgian intelligence services, but instead considers the documents drawn up on Echelon, in particular by STOA, and places the US interception system in the relevant technological and legal context. According to that document, *Echelon can intercept all satellite traffic to Europe* and its *decryption capacity is enormous, although this is played down as far as possible by the US intelligence services*. What is more, *any US technology (software and hardware) legally exported to Europe is regarded as intrinsically and deliberately vulnerable to discreet, remote surveillance by the US intelligence services*.

According to the same document, surveillance of non-encrypted emails and satellite-supported fax traffic could be carried out using a dictionary of key words; no such surveillance of satellite telephone communications (which made up roughly 1% of international telephone communications) was possible, *but individual speakers can be identified on the basis of their voiceprint*.

In January 2001, the committee heard a number of independent journalists and researchers who gave their thoughts on Echelon and, more generally, on the issue of electronic espionage. In particular, two Danish researchers described Denmark's interception capacities and outlined that country's relations with certain other countries which were signatories to the UKUSA[34].

The document entitled *Espionnage industriel – intelligence économique et stratégique (Industrial espionage – economic and strategic intelligence)* takes a different tack, addressing the issue from the point of view of users of industrial espionage, whose philosophy is set out in a quote from a former CIA Director, William Webster: *Our political and military allies are also our economic rivals and the ability of an economic rival to create, win or control markets in the future has security implications for the United States*. The document shows that Japan and China also have industrial espionage services[35].

Another document, *L'Europe face au défi de l'intelligence stratégique (Europe and the strategic intelligence challenge)*, bemoans the way in which Europe had fallen behind in the area of strategic intelligence and criticises the Commission for its refusal to enter into any discussion about the use of information in the sphere of geo-economics[36].

---

[32] Von Coester, S., *Système Echelon – éléments de réflexion – sources ouvertes*. PE5 AP PV/ECHE.2000 ECHE-20001012 0080. The author is the head of the Salamandre strategic consultancy (France).

[33] *Rapport complémentaire sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau Echelon d'interception des communications* http://www.crid.be/pdf/public/4226.pdf,

[34] Minutes of the Echelon Temporary Committee of 22 and 23 January 2001, PE5 AP PV/ECHE.2000 ECHE-20010122 0010.

[35] Document submitted at the committee meeting of 6 March 2001 by Mr La Fragette, of the French firm Circé, which provides advice in the area of industrial espionage, PE5 AP PV/ECHE.2000 ECHE-20010305 0075.

[36] Document submitted by Mr Harbulot, Director of the École de guerre économique (School of Economic Warfare), meeting of the Echelon Temporary Committee of 5 March 2001, PE5 AP PV/ECHE.2000 ECHE-20010305 0060.

2. Contributions from outside experts: legal questions

A comprehensive and detailed account of the legal aspects of the Echelon affair is given in the document entitled *Echelon et Europe (Echelon and Europe)*, submitted to the committee by Dimitri Yernault at the hearing of experts held on 22 March 2001. The document outlines the way in which Echelon represented a breach of the laws of various countries[37].

Under **international law**, the starting point is the generally accepted concept of the territorial extent of the sovereignty of a state: a legal power can only be exercised extraterritorially with the consent (known as 'exequatur') of the state on whose sovereign territory the location of the activity in question is situated. Interceptions carried out using the Echelon system whose targets were persons and entities situated outside the state in which the installations were located must therefore be deemed a breach of international law.

As regards **accountability**, although a state cannot be held accountable for the conduct of international bodies, even if the latter are operating on its territory, it nevertheless has an obligation to monitor what is happening on its territory and to take any precautions required to prevent violations of international law. That obligation becomes important in the context of Echelon, because it concerns the accountability of countries which authorised the USA to use bases situated on their territory[38].

As regards the **European Convention on Human Rights (ECHR)**, it is important to quote Article 8(1) (Right to respect for private and family life):

Everyone has the right to respect for his private and family life, his home and his correspondence. Here, the term 'correspondence' must be understood as meaning the full range of telecommunications services[39]. Under Article 8(2), no public authority may carry out an interception except where this is in accordance with the law and only for the purposes stated in that paragraph. It follows, therefore, that the interception must be both lawful and necessary.

The principle of lawfulness has been defined by the European Court of Human Rights as meaning that the interception must be provided for in a law which is accessible to the individual concerned and whose consequences for him or her are foreseeable[40]. The laws governing the Echelon system were not readily accessible, in either the USA or the UK, and the agreements governing the use of the Menwith Hill base were likewise not accessible, including to Members of the UK Parliament.

The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued. On the basis of that notion,

---

[37] Notice to Members forwarding a document by Mr Dimitri Yernault entitled *Echelon et Europe (Echelon and Europe)* - PE 300.134, PE5 AP PV/ECHE.2000 ECHE-20010322 0082. This document reproduces an article of the same name published in the *Journal des Tribunaux – Droit européen* (Brussels), October 2000, pp. 187-196. The minutes of the meeting of 22 March 2001, PE5 AP PV/ECHE.2000 ECHE-20010322 0010, contain a summary of Mr Yersault's remarks.

[38] The document refers to the specific case of Germany, which allegedly gave permission for its Bad Aibling base to be used, although it played no part in the activities conducted there.

[39] Council of Europe – Recommendation No R (95) 4 F of 7 February 1995 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services.

[40] In the judgment quoted, the notion of 'accessibility' seems to be broader that the standard notion of 'publication'. Foreseeability means that the law must be sufficiently clear in its terms to give an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to carry out interceptions; the persons concerned must also be familiar with the relevant instructions or administrative practices. Leander v Sweden, Application No 9248/81, judgment of the European Court of Human Rights of 26 March 1987.

the European Court of Human Rights affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate[41].

A system such as Echelon, used to carry out a large number of exploratory interceptions, is clearly not consistent with the principle of necessity and the document in question points out that, outside the context of the ECHR, the United Nations Human Rights Committee also emphasises that interceptions must be authorised on a case-by-case basis.

After situating the Echelon system in the context of the ECHR, to which the USA is not a signatory, the document entitled *Echelon et l'Europe* considers whether the ECHR can apply to Echelon. It addresses that issue from the point of view of the applicability of the ECHR to state activities conducted in the context of international relations and, in the light of the relevant international case law, the document states that it is, whether on the basis of the organ of government theory – which argues that states may be held accountable for acts committed by organs of their government which have effects outside their territory[42] – or on the basis of the obligation which states have to monitor activities undertaken on or from their territory, an obligation to which reference has already been made[43].

The document also considers the issue of the admissibility of actions against Echelon before the European Court of Human Rights. Although the relevant case law rules out actions brought by private individuals not directly affected, some judgments have found that actions may be brought by potential victims who are regarded as such simply by virtue of the existence of secret surveillance measures or of a law which authorises such surveillance, there being no need to prove that the measures in question are specifically directed against the victim[44].

3. The position of the Commission and Council

The executive expressed its views at hearings of Antonio Vitorino, Commissioner for Justice and Home Affairs, and Erkki Liikanen, Commissioner for Enterprise and the Information Society, held on 11 and 12 September 2000[45], and Christopher Patten, Commissioner for External Relations, which took place on 3 April 2001.

As had been the case when the Commission made statements during the debate held on 30 March, Commissioners Vitorino and Liikanen dealt with general telecommunications security issues which fell within their respective remits, without discussing Echelon

---

[41] Klass and other v Germany, Application No 5029/71, judgment of the European Court of Human Rights of 6 September 1978.

[42] Drozd and Janousek v France and Spain, Application No 12747/87, judgment of the European Court of Human Rights of 26 June 1992.

[43] It follows that the ECHR takes precedence over the other international agreements concluded by a state and thus, as regards Echelon, over the UKUSA.

[44] Klass and others v Germany, Application No 5029/71, judgment of the European Court of Human Rights of 6 September 1978, and Rotaru v Romania, Application No 28341/95, judgment of 4 May 2000. The document referred to above is more detailed and more comprehensive than the legal documents submitted at the meeting of 22 March 2001. Other important documents should also be cited: *Cyber-rights vs Cyber-crimes* (PE 300.135), submitted by the UK association Cyber-Rights & Cyber-Liberties; *Protection de la vie privée et droits de l'homme (Protection of privacy and human rights)*, submitted by M. Nataf, lawyer, and M. Coste, an IT security expert, *The interception of communications and unauthorised access to information stored on computer systems in the light of the European Convention on Human Rights*, submitted by M. Dossow, Council of Europe official.

[45] Mr Vitorino answered a question about the existence of Echelon by making a joke: *I believe in God and in Echelon, but I have never met either. EP/Espionage - The European Parliament's temporary committee on the Echelon system has started work*, Agence Europe, 13 September 2000.

directly. Mr Vitorino focused on the protection of privacy in the context of EU Directive 95/46/EC on data protection. For his part, Commissioner Liikanen focused on encryption, which he said should be reliable and provide a high level of protection, and on cryptographic systems, which he said should continue to be controlled by the public authorities, in order to make the fight against crime effective.

Commissioner Patten stated that, although the activities of the US intelligence services were not part of the New Transatlantic Agenda, the issue of Echelon was to be addressed at a meeting of justice and home affairs ministers. As regards the more specific issue of information security, Mr Patten said that, following the approval of the Council regulation on security, the Commission was in the process of approving its own regulation which would lay down detailed arrangements for the processing of the various forms of classified EU information and afford the Commission a level of security commensurate with its role in the context of the CFSP and the ESDP[46]. At least some of the members of the committee were dissatisfied with Mr Patten's answers in particular.

Christopher Patten, Commissioner for External Relations, who took part in a hearing with the Echelon Committee on 3 April 2001. © European Union, 1999

The Council's position was outlined to the committee by Hervé Masurel, President-in-Office of the Council, on 28 November 2000[47]. The Council took the view that interceptions were an important weapon in the fight against crime, but that their use in order to obtain commercial advantages was unacceptable. As regards the specific issue of Echelon, although its existence was now accepted, there was no proof that it was being used for commercial purposes or in a manner which breached the rights of EU citizens. He emphasised in particular the importance of encryption and of establishing a security architecture for IT systems.

Brian Crowe, Director-General of External Relations[48], also spoke on behalf of the Council. He was at pains to emphasise the distinction between the powers of states and those of

[46] In addition to the minutes of the meeting, two other documents dealing with the statement made by Commissioner Patten are available: Contribution by Commissioner Chris Patten to the European Parliament's Temporary Committee on Echelon, PE5 AP PV/ECHE.2000 ECHE-20010403 0026, and Note setting out a transcription of the questions put to Mr Patten and his answers – meeting on Echelon of 3 April 2001 – Strasbourg, PE5 AP PV/ECHE.2000 ECHE-20010403 0028.

[47] Transcription of the statements by Hervé Masurel and Arthur Paecht, PE5 AP PV/ECHE.2000 ECHE-20001128 0020.

[48] Mr Crowe was heard on 23 April 2001. His statements are set out in the minutes of the committee meeting, PE5 AP PV/ECHE.2000 ECHE-20010423 0010, and in an aide-memoire drawn up by the secretariat, Record of

the Council: intelligence was a state matter. He also said that the Council was making significant progress in setting up a secure telecommunications system and was negotiating an agreement on this issue with NATO.

The Swedish Presidency, represented by Ambassador Lund, was heard on 29 May 2001. Mr Lund did no more than outline the measures taken by the Council on issues falling within the Union's sphere of responsibility, referring in particular to the 'Security Sphere' for the protection of personal data[49].

At least two members of the committee were not satisfied with the Council's statements and, in particular, the contribution by Mr Masurel[50].

4. Contributions from the national parliaments

In addition to the Council statement, the committee meeting of 28 November 2000 was devoted to a hearing of representatives of the national parliaments and, more specifically, of the national parliament bodies responsible for monitoring national intelligence services or MPs who had considered or were considering the Echelon case. Only four parliaments sent representatives: the Irish Parliament, the Belgian Senate, the Austrian Nationalrat and the French National Assembly. The documents for the chair show that Finland, Norway and the Netherlands had stated they were unable to send representatives, but they provide no explanation as to why the representatives of Luxembourg and Spain, whose attendance was 'to be confirmed', were not at the meeting; the minutes of the meeting of 22 January 2001 show that Denmark refused to send a representative. No information is available concerning participation by representatives of the other national parliaments.[51]

The minutes provide no insight into the statements made by three of the four representatives, but give extensive details of the contribution by the representative of the French National Assembly, and rapporteur on Echelon, Arthur Paecht. Mr Paecht gave a mordant and at times sarcastic account of his meetings with the US authorities. He put forward his own ideas as to why attention was suddenly being paid to the Echelon affair, given that the relevant documents had been available for some time on the internet. He put his finger on the key issue when he stated that there was no proof of Echelon being used for industrial espionage purposes, but that this was irrelevant because *it is technically possible and when something is possible [...] the important thing in my view is to protect oneself. France, Germany or the Netherlands will not be protecting themselves individually – this is a European Union problem [...]*[52].

---

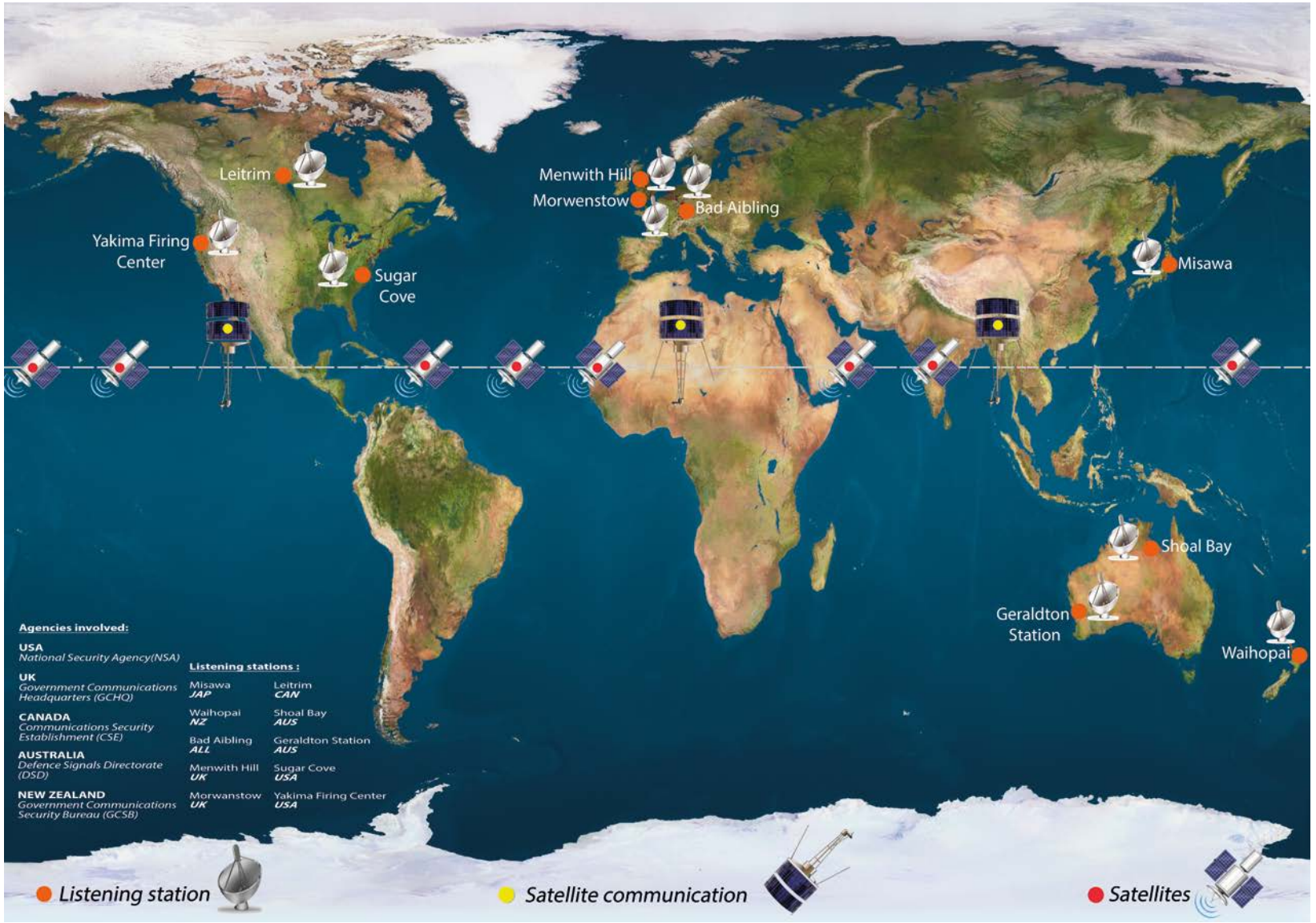
the statement made by and the exchange of views with Mr Crowe, PE5 AP PV/ECHE.2000 ECHE-20010423 0027.

[49] The principles underpinning the Security Sphere are those concerning the confidentiality of personal data adopted by the US Administration on 21 July 2000. The Commission decision of 26 July 2000 on this matter (OJ L 215, 25.8.2000, p. 7) refers to these principles. Minutes of the Echelon Temporary Committee of 29 May 2001, PE5 AP PV/ECHE.2000 ECHE-20010529 0010.

[50] Minutes of the meeting (held in camera) of the Echelon Temporary Committee of 28 November 2000, PE5 AP PV/ECHE.2000 ECHE-20001128 0010.

[51] The file available in the Historical Archives contains the following documents: Documentation concerning the legislation on the bodies responsible for monitoring intelligence services in Germany, PE5 AP RP/ECHE.2000 A5-0264/2001 0110, Documentation on the legislation in force in Germany: parliamentary monitoring of the intelligence services, PE5 AP RP/ECHE.2000 A5-0264/2001 0120, Documentation concerning legislation on the bodies responsible for monitoring intelligence services in Austria, PE5 AP RP/ECHE.2000 A5-0264/2001 0140, and Synoptic table of intelligence services and parliamentary control bodies in the Member States (draft), PE5 AP PV/ECHE.2000 ECHE-20001128 0030.

[52] Transcription of the statements by Hervé Masurel and Arthur Paecht of 28 November 2000, p. 4, PE5 AP PV/ECHE.2000 ECHE-20001128 0020.



A global electronic surveillance system: Echelon eavesdrops on all e-mail, telephone, fax and telex transmissions carried by satellite worldwide. Illustration: Historical Archives © European Union, 2014

CHAPTER IV

THE COMMITTEE'S WORK AND THE FINAL REPORT

1. Missions to Paris, London and Washington

Alongside its other consultations, the committee sent delegations to Paris, London and Washington: the success of these missions varied.

The main focus of the mission to **Paris** on 18 January 2001 was a meeting between committee chairman Mr Coelho and rapporteur Mr Schmid and the French Secretary-General for National Defence, Jean-Claude Mallet, with five members of his staff. The committee delegation was also received at the Ministry of Foreign Affairs and the Defence Ministry.

The Secretary-General for National Defence outlined his view on the available information about Echelon and its potential implications. He also talked about encryption and about intelligence cooperation in the context of a European security and defence identity.[53]

At the Ministry of Defence, Mr Perraudau, advisor to the Minister, outlined the arrangements France was putting in place to protect both government ministries and companies from interception, and spoke of the need to pool Member States' information sources in certain specific strategic fields.

The mission to **London** between 24 and 26 January 2001 included several meetings, one of which was with Mr King, chair of the House of Commons Intelligence and Security Committee: he described the tasks of that committee, which has access to all secret documents other than those concerning ongoing operations and to all intelligence service databases. There was also an exchange of views on the interception of satellite communications.

At a subsequent meeting, the UK Home Secretary, Mr Straw, highlighted the Convention on Mutual Assistance in Criminal Matters and the UK legislation on interception, which he compared to that of certain European countries; he also explained his own duties in relation to authorising interception[54].

During the mission to **Washington** from 6 to 11 May 2001, a number of US intelligence agencies, as well as the Departments of State and Commerce, refused to meet the delegation members.

In the end, the mission entailed a meeting with the Congressional Permanent Select Committee on Intelligence, which Mr Coelho later described as very useful and constructive, a meeting with former CIA director James Woolsey and several meetings with non-government bodies. The overall assessment of what this mission achieved and the political considerations with regard to the US authorities' attitude are clear from the minutes of the meeting of 15 May 2001 at which the chairman reported back to the committee: he *deplored the last-minute cancellation, with no satisfactory explanation, of the*

---

[53] The relevant available documents are to be found in the document file for the Echelon Committee meeting of 22-23 January 2001, PE5 AP PV/ECHE.2000 ECHE-20010122. This file includes an aide-mémoire on which the authors of this study drew extensively, a letter of thanks from committee chairman Coelho to the Secretary-General for National Defence and the list of members of the two delegations.

[54] The relevant available documents are to be found in the document file for the Echelon Committee meeting of 5-6 February 2001, PE5 AP PV/ECHE.2000 ECHE-20010205, which includes a note to the Presidency of Parliament, several contributions from experts and a note from the head of the committee secretariat, Mr Lowe, concerning one of the preliminary visits which he made.

meetings that had been scheduled with the US Department of State, the Advocacy Center of the Department of Commerce, the CIA and the NSA, adding that *the objective of the delegation had at no point been the collection of more information,* and regretting *the fact that the institutions which had cancelled the meetings had lost an opportunity to clear up the uncertainties over their role in the matter by rejecting the possibility of debate*[55].

Carlos Coelho and Gerhard Schmid (with David Lowe on the left) at the press conference on 16 May 2001, following the visit by an Echelon Committee delegation to the USA. © European Union, 2001

The treatment of the delegation in Washington provoked reaction. Firstly, the President of Parliament, Nicole Fontaine, said she found it deeply regrettable that the main US government bodies concerned had refused to meet the delegation, thus preventing the Echelon Committee from carrying out its work properly. At the same time, however, she thanked the Congress members for being prepared to engage in dialogue. A few days later, the House took a similar position in a resolution on the state of the transatlantic dialogue[56].

[55] Statement by Mr Coelho during the visit to Washington, PE5 AP PV/ECHE.2000 ECHE-20010515 0040, and minutes of the meeting of the Echelon Committee of 6 May 2001, PE5 AP PV/ECHE.2000 ECHE-20010515 0010.
[56] Statement by the Presidency of the European Parliament on the refusal by US government authorities to meet the EP delegation, PE5 AP PV/ECHE.2000 ECHE-20010515 0050, and European Parliament resolution on the state of the transatlantic dialogue (joint resolution B5-0345/2001) of 17 May 2001, OJ C 34E, 7.2.2002, pp. 255-359. In the debate on 16 May 2001, little mention was made of the issue.

2. The Schmid report: characteristics of the Echelon system[57]

On 3 July 2001, the committee adopted the weighty Schmid report with its accompanying motion for a resolution by 27 votes to five, with two abstentions; the votes against and the abstentions were explained in four minority opinions.

The report details all the information obtained about Echelon (including through confidential contacts by the rapporteur) as well as interception activities undertaken outside the Echelon system, the legal and practical implications of industrial espionage and the types of technology used, and it addresses the question of encryption, which is seen as the major potential defence against interception.

The report starts by asserting the existence of a global system for intercepting communications, known as Echelon. A significant section – Chapter V entitled *Clues to the existence of at least one global interception system* – considers the sources on the basis of which it was concluded that Echelon and the UKUSA agreement were a reality. Chapter VI is entitled *Might there be other global interception systems?* and answers that question in the affirmative, focusing in particular on France, Germany, Russia and China.

The main feature of Echelon was its global reach, achieved through collaboration between a number of countries under the UKUSA agreement. A further feature of note was Echelon's technological capacity to intercept virtually all forms of telecommunications, despite the various means of access and degrees of difficulty involved in doing so.

While **satellite communications** were not overly challenging for a network with interception centres in the relevant regions of the globe, the interceptibility of **radio transmissions** depended on the range of the electromagnetic waves employed. If the radio waves ran along the surface of the earth (so-called *ground waves*) their range was restricted, as was the scope for intercepting them; the range of *indirect* or *space waves*, reflected off layers of the ionosphere, was greater and it was thus easier to intercept them. Intercepting **cable transmissions** – used in all types of telecommunications – required physical access at a cable terminal, so a state through which a cable transited would always be capable of practicing interception, whereas a foreign state would be able to gain the requisite access only with the transit state's cooperation or by unlawful means. Intercepting **underwater cable transmissions** posed problems of a different order: it was possible using submarines – obviously very costly – but not in the case of new-generation fibre optic cables.

The UKUSA countries therefore had excellent resources for intercepting satellite transmissions, few for the interception of radio transmissions and very limited resources for intercepting cable transmissions, the UK being in practice the only UKUSA state with capability in that field.

Given that international interception operations, unlike interception practiced within a country for law-enforcement purposes, were not targeted, there was the further difficulty – apart from that of restricted access to the various forms of telecommunications – of sifting relevant communications from the huge quantity of transmissions intercepted. At the time the report was compiled, the identification of specific voices was technically possible using systems 'trained' to recognise them. However, automatic recognition of specific words spoken by any voice was not yet possible to a sufficient degree of accuracy.

---

[57] European Parliament report on the existence of a global system for the interception of private and commercial communications (Echelon interception system), PE5 AP RP/ECHE.2000 A5-0264/2001 0010, p. 26. The following paragraphs offer an outline of the report, focusing on its politically most important aspects.

3. The Schmid report: legal aspects[58]

Another feature of the Echelon system was the fact that it operated outside any legal framework. It is useful to quote the report directly on this point:

Possible threats to privacy and to businesses posed by a system of the Echelon type arise not only from the fact that is a particularly powerful monitoring system, but also that it operates in a largely legislation-free area. Systems for the interception of international communications are not usually targeted at residents of the home country. The person whose messages were intercepted would have no domestic legal protection, not being resident in the country concerned. Such a person would be completely at the mercy of the system. Parliamentary supervision would also be inadequate in this area, since the voters, who assume that interception 'only' affects people abroad, would not be particularly interested in it, and elected representatives chiefly follow the interests of their voters. That being so, it was hardly surprising that the hearings in the US Congress concerning the activities of the NSA were confined to the question of whether US citizens were affected by it [...].

The absence of any legal framework governing Echelon did not prevent consideration of its status with regard to the law. The report seeks to identify a basis in law for penalising espionage systems and pinpoints Article 10 of the EC Treaty, applied in circumstances which it describes thus:

If a Member State were to promote the use of an interception system, which was also used for industrial espionage, by allowing its own intelligence service to operate such a system or by giving foreign intelligence services access to its territory for this purpose, it would undoubtedly constitute a breach of EC law. Under Article 10 TEC, the Member States are committed to acting in good faith and, in particular, from abstaining from any measure which could jeopardise the attainment of the objectives of the Treaty.

The report concludes:

[...], it can therefore be said that the current legal position is that in principle an Echelon type intelligence system is not in breach of Union law because it does not concern the aspects of Union law that would be required for there to be incompatibility. However, this applies only where the system is actually used exclusively for the purposes of state security in the broad sense. On the other hand, were it to be used for other purposes and for industrial espionage directed against foreign firms, this would constitute an infringement of EC law. Were a Member State to be involved in such action, it would be in breach of Community law.

4. The Schmid report: protecting the public against interception activities[59]

Protecting members of the public against interception operations carried out by public bodies was an exclusively national responsibility subject to different rules depending on whether the interception was initiated, on the one hand, as part of a police or judicial investigation or, on the other, by the intelligence services, which in democratic systems operated solely in pursuit of lawful aims.

In the case of interception operations as part of a police or judicial investigation, all the Member States had fairly similar safeguards in place, including as standard the requirement of prior authorisation by a judicial authority. In the case of interception activity by the intelligence services targeting, as a rule, not individual users but rather

[58] Report A5-0264/2001, points 1.6, 7.3 and 7.4.
[59] Report A5-0264/2001, points 9.3 and 9.4.

groups seen as potentially dangerous, the safeguards differed significantly from one Member State to another.

One essential tool for protecting members of the public against interception operations by intelligence services was the system whereby those services were monitored: monitoring arrangements in the various Member States differed but were generally the responsibility of special committees. The report's conclusions on this point are far from satisfactory from the European citizen's point of view, for the powers of intelligence services varied substantially. *The adverse impact is felt above all by nationals of other states, since foreign intelligence services, by their very nature, carry out their work abroad. Individuals are essentially at the mercy of foreign systems, and here the need for protection is greater still.*

5. The Schmid report: protection against industrial espionage[60]

The term 'industrial espionage' describes espionage activities by a state intelligence service targeting companies – as a rule, foreign companies. It is not the same as 'competitive intelligence', or 'industrial intelligence', which is something that goes on between companies, usually rivals, or in the context of trade relations.

In many respects, the report does not observe this distinction: it deals in a general way with espionage practised against companies. The information on the damage caused by industrial espionage is based on controversial and non-uniform assessments and the only conclusion one can safely draw is that it was taking a heavy toll.

The report does focus on industrial espionage as defined above for purposes of identifying the states which engaged in such activities on the basis of their technology. The countries most advanced in industrial espionage were using it for purposes of tailoring their economic or industrial policies or for gathering information useful to national companies trading abroad. The least advanced countries were concerned with acquiring know-how on the cheap.

One of the main types of industrial espionage, and one that fell within the remit of the Echelon Committee, entailed tapping into computer networks or stealing data from electronic storage media. The risks of industrial espionage were high because, outside big public and private-sector organisations, they were under recognised, which meant that even elementary precautions were rarely taken.

The report goes on to consider risk awareness in various situations, particularly in the EU institutions. The solution it proposes is encryption as a means of self-defence and it discusses the question of the legal restrictions which some states had placed on encryption. The report comes down against such restrictions, which could impede the development of e-commerce and of electronic banking services.

6. Key points of the report

The Schmid report can be summed up as follows:

- a global system for intercepting communications, probably known as Echelon, indeed existed and was managed on the basis of a secret agreement (the UKUSA agreement) between five countries, the USA (as lead partner), the UK, Canada, Australia and New Zealand; the system also made use of bases in other countries, e.g. the Bad Aibling base in Germany;

[60] Report A5-0264/2001, points 10.2, 10.5.2 and 10.11.

- for technical reasons, the system did not have the capability to intercept all or even most communications, and it could analyse only a limited number of communications;
- the system had indeed been used to intercept European companies' telecommunications, for the stated purpose of combating international corruption, and there was therefore a risk that information gathered in this way could be used to place US companies at an advantage;
- other states possessed comparable interception systems[61].

Gerhard Schmid, rapporteur on the existence of a global system for the interception of private and commercial communications (Echelon interception system) (Document A5-0264/2001), at the committee meeting of 12 October 2000. On the left, Reino Paasilinna, member of the te
mporary committee. © European Union, 2000

The report is accompanied by 44 recommendations on various matters. Almost all of these also feature in the motion for a resolution and in the resolution as adopted. Of the recommendations not included in the resolution the most important was No 16, which – logically in accordance with the principle of Member State responsibility under Article 10 TEC as interpreted in the report with reference to industrial espionage – called on *the authorities of the United Kingdom [...] to explain their role in the UK/USA alliance in connection with the existence of a system of the 'Echelon' type and its use for the purposes of industrial espionage*. This is the only place where the report, albeit cautiously, reminds the UK of its accountability[62].

[61] These four points sum up the report's conclusions. Report A5-0264/2001, point 13.1.

[62] Recommendation No 21, which is included in the resolution, calls on the UK and Germany to make the authorisation of further communications interception operations by the USA on their territory conditional on their compliance with citizens' rights.

The report is accompanied by four opinions, one from each of the European Parliament minority groups represented on the Echelon Committee: GUE/NGL, Verts/ALE, UEN and TDI. The content of these minority opinions was reflected in speeches made during the debate on the subject on 5 September 2001.

7. The Perkins affair

An account of the Echelon Committee's work is not complete without mention of an episode which, while not recorded in the report, caused a stir within the committee and in the press.

One of the people invited by the committee to a hearing of encryption experts was Desmond Perkins, head of the unit responsible for encryption at the Commission: he told the members: *I have always had very good contacts with the National Security Agency in Washington, and they usually check our [encryption] systems to see that they are being well looked after and not being misused*[63].

This statement provoked rapporteur Gerhard Schmid to ask precisely what the checking by the NSA entailed.

After initially avoiding the question as to why the NSA was involved, Mr Perkins said: *Because I have relatives working in there. It is as simple as that. You have got to remember, as I am sure all of you around this room know, the Americans read everything, no matter what is going on inside here, they read everything, with their satellites that are lined up [...] The NSA is a huge organisation. It has got thousands of staff just listening all the time and reading all the time.*

Mr Perkins' statements led rapporteur Schmid to write to Commissioner Patten asking him to explain the Commission's relationship with the NSA[64]. Mr Perkins, meanwhile, felt it necessary to clarify, in a note to his director-general, what he had said about the Americans reading everything. He said that what he had meant by 'read' was simply that *the Americans intercept all sorts of traffic. This does not mean that they can necessarily de-encrypt everything that they intercept*; he added that he was not certain *whether the Americans are able to de-encrypt cypher traffic from the Commission's Delegation in Washington,* but that in his professional experience it was unlikely.[65]

In reply to Mr Schmid's letter, Commissioner Patten forwarded Mr Perkins' note to him, and the incident was described by a Commission spokesperson as a misunderstanding[66].

However, Mr Perkins' note and the spokesperson's statement were not the end of the matter: two Commission officials attended the committee's next meeting to offer clarification about what Mr Perkins had said[67]. The minutes of the meeting of 6 March 2001, this part of which was held in camera, record the explanations they gave as follows: *Mr Briet said that he accepted responsibility for Mr Perkins' remarks, and stressed the*

---

[63] Contribution from Desmond Perkins on the Commission's encryption system, PE5 AP PV/ECHE.2000 ECHE-20010205 0100.

[64] Letter of 7 February 2001 concerning a contribution made at the meeting of 5-6 February 2001 which gave rise to misunderstandings, PE5 AP PV/ECHE.2000 ECHE-20010305 0080, p. 4.

[65] D. Perkins, note à Mr Legras of 8 February 2001, concerning a contribution made at the meeting of 5-6 February 2001 which gave rise to misunderstandings, PE5 AP PV/ECHE.2000 ECHE-20010305 0080, p. 2.

[66] *EU/Spying - European Commission denies Americans are testing EU encryption system*, Agence Europe, 2 March 2001.

[67] The attendance list for the meeting of 5-6 March 2001 includes the names of two Commission officials, who are quoted in the minutes in relation to the Perkins affair: Mr Briet, a deputy director in the Directorate-General for External Relations and thus Mr Perkins' superior, and Mr De Baenst, Protocol Director of the Commission's Security Service, PE5 AP PV/ECHE.2000 ECHE-20010305 0010.

Commission's willingness to guarantee access to communications[68]*. He added that the notion that the NSA should want to monitor the Commission's communications was absurd: in his view there had been no contacts between the Commission and the NSA*. He added that *both Mr Perkins and other security officials had been subjected to the requisite checks.*

That may have concluded the matter at committee level[69], but the Perkins affair also created ripples further afield: the Green Group called for a debate in plenary on the grounds that the matter went beyond the remit of the temporary committee and ought to be discussed by the full House, with the Commission being required to make a statement on any NSA access to the EU executive's encryption system[70]. At Parliament's sitting of 12 March 2001, the Greens put forward a proposal to this effect, with the support of the GUE/NGL Group. Mr Swoboda (Germany, PSE) took a different position, disagreeing with the Greens' proposal on the grounds that, while Mr Perkins' statements had been alarming, it was the task of the Echelon Committee – possibly with an extended remit – to examine them. The proposal was rejected.[71]

[68] The minutes are vague here and this sentence is open to more than one interpretation. To whom does the Commission guarantee access to communications?

[69] In reply to a specific question at a press conference, rapporteur Schmid echoed Mr Briet in stating that there was no documentation attesting to NSA intervention as described by Mr Perkins. *EP/Echelon - Schmid discusses work of temporary Echelon Committee,* Agence Europe, 8 March 2001.

[70] *EP/Espionage - Lannoye wants debate in plenary*, Agence Europe, 3 March 2001.

[71] European Parliament proceedings of 12 March 2001, Order of business.

Carlos Coelho and Gerhard Schmid at the press conference on 11 July 2001. © European Union, 2001

CHAPTER V

THE ECHELON RESOLUTION AND WHAT HAPPENED AFTERWARDS

1. The debate in plenary

On 5 September 2001, the Schmid report was debated in plenary; the atmosphere was calm[72] but opposing positions emerged. A large majority of the Members, however, said they were in favour of the resolution.

The committee chairman, Mr Coelho, summarised the committee's work thus: *Echelon exists, whether under this name or any other. The European Parliament should be in no doubt about this.* He pointed out that *Echelon runs a risk, a serious risk of its network being abused. This is a commercial risk, which compromises the concept of fair trade, but also presents a risk for civil liberties. ... Europe and the United States must cooperate fairly ... for the sake of the common values that they most definitely share.* He also emphasised *the need to strengthen the European Convention on Human Rights with regard to protecting privacy in the information society, the need for parliamentary and judicial control over the activity of the secret services, the need to extend defence practices such as the use of cryptography and electronic signatures, and the need for the European institutions themselves to set an example by using these technologies.*

The rapporteur, Mr Schmid, was aware of the political nature of the various views expressed and raised the question of how to respond to European public opinion, particularly with regard to mistrust of the Americans:

[...] the United States is considered capable of such measures. The political problem highlighted by this whole issue is the prevalence of profound mistrust. This mistrust has to be weeded out.

The Socialist rapporteur was supported by the PPE-DE Group in the person of Mr von Boetticher who thanked *the rapporteur and his team for resisting the attempts of the Greens, as well as those from the Left of this chamber, to have him write a cloak-and-dagger thriller*. He found the report to be responsible and objective, even if the conclusions, which exhausted the available legal options, might not go far enough for some.

Mr Wiersma (PSE Group) considered what constituted an appropriate relationship between the secret services and the public, and stressed the importance of having *rules to protect the privacy of all European citizens in all EU countries [...].*

The rapporteur also received full support from the ELDR Group; Ms Flesch commented that it was misleading and futile to suggest abolishing the secret services. *They exist and they will continue to exist. We should, therefore, draw political conclusions and seek solutions [...].*The view of the Verts/ALE Group was diametrically opposed and Ms McKenna asked whether it was appropriate to uphold the existence of secret services. Her group's fundamental criticism of the report was that it focused *mainly on the threat to European industrial competition and the threat posed by industrial espionage. The real issue at stake ... is that nobody can communicate in confidence any more.*Mr Di Lello Finuoli (GUE/NGL) agreed and said that because of its technical capabilities Echelon *nullifies the relationship of proportionality which, precisely within the meaning of Article 8 of the European Convention on Human Rights, has to exist between interference in people's private lives and the benefits of interception for protection purposes.*

---

[72] Debates of the European Parliament, 5 September 2001.

Mr Marchiani (UEN) also opposed the report, but for different reasons, the main one being that *most of the Members in this House from the United Kingdom have put solidarity with the US before solidarity with Europe*.

Mr Turco was critical of the way the committee's work had been carried out: *it was necessary to organise the work in this way not in the interests of European security [...] but in order to conceal the responsibility of the Member States of the Union*. The report stated quite clearly *that Echelon does exist [...] and that the United Kingdom is part of the system,* but it did not condemn this fact openly because Germany was already carrying out interceptions and the Netherlands was planning to.

Mr Belder (EDD) supported the report but urged adoption of an amendment he had tabled *to protect communication against interception where supervision is lacking*.

2. The resolution

The motion for a resolution was adopted[73] with only two amendments, on the same day as the debate, with 367 votes for, 159 against and 34 abstentions: there was no consistent pattern in group voting, with the exception of the GUE/NGL and UEN, where all members voted against.

In substance the resolution followed the temporary committee's recommendations. Some points covered international treaties that needed to be concluded or amended and the particular importance of an agreement between the European Union and the USA whereby each party would apply to the other the rules governing the protection of privacy and the confidentiality of business communications which were valid for its own citizens and firms.

The Member States were asked to adapt their legislation on the intelligence services to the European Convention on Human Rights, by providing appropriate guarantees not only for their own citizens but also for those from third countries on the basis of a common code of conduct, and to negotiate a similar code of conduct with the USA. They were also asked *to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission*.

Member States were asked collectively not to abuse the intelligence services for economic ends but, in view of their involvement in the Echelon system, the United Kingdom and Germany were asked to *make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR*.

The other points were intended to encourage self-protection on the part of the public and firms by the development of encryption and open-source software to ensure no 'backdoors' were built into programs. The Commission was asked to strengthen its encryption system.

---

[73] European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) – A5-0264/2001 (2001/2098 INI) 5 September 2001, OJ C 72E 21.3.2002, pp. 221-229. The resolution did not include recommendation No 16 in the report, which called on *the authorities of the United Kingdom to explain their role in the UK/USA alliance in connection with the existence of a system of the 'Echelon' type and its use for the purposes of industrial espionage*.

In conclusion, one of the most significant comments in the report and resolution was to point to the lack of scrutiny and to recommend the creation of a parliamentary body to monitor intelligence activities.

3. Statements by the Council and Commission one year on[74]

On 23 October 2002, the Council and Commission reported to Parliament on action taken on the resolution of 5 September 2001. Speaking on behalf of the Danish Presidency, Mr Haarder said the Schmid report had done a lot to contribute to awareness of issues surrounding telecommunications security and that the Danish Presidency was working to strengthen security of communications for the individual. He particularly mentioned the directive of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.[75] He commented on the work that still needed to be done to increase the use of encryption and to boost IT security, which would be a top priority in the common European action plan *eEurope 2005*.

Commissioner Liikanen said the Commission's policy focused on network and information security as set out in the *eEurope 2005* plan, which aimed *to strengthen the exchange of information and good practice, to establish a European centre of competence, to create a culture of security and to establish a secure communication environment*. Like Mr Haarder, Mr Liikanen mentioned the directive of 12 July 2002: this would *provide a high level of protection for processed personal data* by means of a provision that required *Member States to guarantee confidentiality of communications and to prohibit any form of interception*.

Neither statement aroused great enthusiasm. Ms Flesch, on a point of order, said that the statements had nothing to do with the subject on the agenda. Mr von Boetticher asked Mr Liikanen several questions on progress on the project to protect against interception; he finished by saying that if the Commission continued to take no action, Parliament might take this into account when considering the forthcoming Commission discharge.

Mr Wiersma took a more moderate tone but was equally firm on substance; he concurred with what Mr von Boetticher had said and deplored the fact that Commissioner Patten was not present, as he could have provided more information about the international aspects of the Echelon affair.

Mr Coelho, the chairman of the temporary committee, regretted that the report seemed to have been forgotten; indeed Parliament's Bureau had chosen not to promote publication of the report. The situation had not changed and he deplored the suggestion that *the fight against international crime and terrorism is necessarily undertaken at the cost of our freedoms.*[76]

The Liberal Group's view was set out by Ms Plooij-van Gorsel. She thought there was a need for a legal framework to curb unlawful practices and to *clearly define legal interception with effective control at European level.* The Liberal Group had opted for a dual-track approach to protect the rights and privacy of the individual citizen, on the one hand, and to safeguard the EU's economic interests by means of measures to prevent industrial espionage, on the other.

---

[74] Debates of the European Parliament, 23 October 2002.
[75] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, OJ L 201, 31.7.2002, p. 37.
[76] Combating terrorism. Debates of the European Parliament, 23 October 2002.

Speakers from groups that had not approved the resolution the previous year were equally critical. Mr Di Lello said the real message of the Echelon Committee was that citizens and their privacy needed to be protected, and that *the failure of the institutions and Parliament itself to take any practical steps regarding Echelon [...] damages their legitimacy*.

Ms McKenna expressed the Verts/ALE view opposing the *actions taken by the Council with a view to bringing telecommunications interception capabilities into line with the new technologies* and the *adoption of the directive under which Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period*.

Mr Turco criticised the failure to act following the Schmid report and said that there was a continuing focus on the Anglo-American system, while continuing to ignore the fact that these systems were also being used in EU countries.

Mr Schmid was equally dissatisfied but concentrated more on the specific issues of open-source software and the Commission's IT security. He wanted open source to be promoted as a basis for the encryption software so there was definite knowledge of what the software did.

4. Resolution of 7 November 2002

The dissatisfaction shown during the October debate manifested itself in a resolution adopted a fortnight later[77]. Parliament regretted that the Council and Commission had failed to react adequately to the recommendations it had made, and it urged them to take all the measures necessary to fully implement the recommendations contained in its earlier resolution, highlighting the main points of the resolution of 5 September 2001, which called for measures to *protect citizens and firms against the abuse and illegal use of interception of communications, the introduction and use of systems and techniques to protect privacy and the confidentiality of communications and the introduction of measures against industrial espionage and the abuse of competitive intelligence*.

The resolution referred to the events of 11 September 2001, which had stalled the debate: *whereas the events of 11 September 2001, other recent terrorist attacks and the international efforts to combat terrorism have further emphasised the importance of the recommendations contained in its resolution* [of 5 September 2001], the European Parliament reiterated *its request to the Member States to collaborate, cooperate and coordinate amongst themselves and on a multilateral level in the exchange of information ... in the fight against terrorism and against international crime* and called for the conclusion of international agreements and for greater cooperation and coordination between Member States' intelligence services under the common security and defence policy.

[77] European Parliament resolution on Echelon (B5-0528/2002), 7 November 2002, OJ C E16, 22.1.2004, pp. 88-89.

CONCLUSIONS

As a policy initiative, the European Parliament's temporary committee on the Echelon affair was a focus for contemporary concerns about telecommunications security and confidentiality, examining whether these had been breached by the Echelon system. Parliament took the step of setting up the committee on the basis of research carried out by one of its own internal bodies, the STOA Panel, which had distilled the available information in the international media about an interception programme involving allies of the EU and Member States and had also stimulated initial reaction among MEPs, triggering the political debate about the matter.

The Echelon affair came to the forefront in Parliament at a time when transatlantic relations were under strain as the result of trade rows and the determination of the US administration to penalise companies that had links with countries subject to the US trade embargo (Helms-Burton Act). It was therefore not surprising that the first mention of Echelon was in a resolution largely devoted to transatlantic economic relations.

This context goes some way to explaining a degree of embarrassment on the part of the EU institutions and the major political groups in Parliament: how could they investigate the Echelon system without harming the already strained relationship with their American ally and putting the UK in an awkward position? While the legal logic behind the establishment of a temporary committee – as opposed to a committee of inquiry – is sound, it also reflects a desire to pre-empt any polemics. The dropping of recommendation No 16 of the Schmid report, which called on the UK authorities to explain their role in the UKUSA alliance, also speaks volumes.

Despite the cautious approach, Gerhard Schmid produced a report that confirmed the existence of the Echelon system and attempted to determine what it entailed. The report also raised the general question of the security of telecommunications in the EU and how to protect them effectively under the law.

What has been the legacy of the Echelon affair and how has it affected the EU's position on the questions of data interception and protection? The affair itself would seem to have been largely forgotten: it is no longer referred to in the press, and websites about it have ceased to be updated.

However, the EU has undertaken wide-ranging reform to protect access to its citizens', institutions' and companies' data: it has introduced a comprehensive approach to data protection, has strengthened rights to the protection of privacy on line and has ended the situation whereby these matters were governed by 28 separate sets of national laws. The words of Justice Commissioner Viviane Reding are worth recalling here: *Following the US data spying scandals, data protection is more than ever a competitive advantage. [...] we need a uniform and strong European data protection law, which will make life easier for business and strengthen the protection of our citizens*[78].

[78] European Commission Memo 14/186 of 12 March 2014, Progress on EU data protection reform now irreversible following European Parliament vote.

In March 2014, Parliament confirmed its support for Ms Reding's approach and for the Commission's proposed framework reform by adopting reports by MEPs Jan Philipp Albrecht and Dimitrios Droutsas on, respectively, the protection and the free movement of personal data.[79]

Nonetheless, the issues at stake are still current following the revelations by WikiLeaks and Edward Snowden and the recent eavesdropping on German Chancellor Angela Merkel and on French diplomats posted to the USA.

[79] Report by the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), A7-0402/2013 - COM(2012)0011 – C7 0025/2012 – 2012/0011(COD), rapporteur Jan Philipp Albrecht; Report by the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - A7-0403/2013 - COM(2012)0010 – C7 0024/2012 – 2012/0010(COD), rapporteur Dimitrios Droutsas; Commission Memo 14/186 of 12 March 2014, 'Progress on EU data protection reform now irreversible following European Parliament vote'.

INDEX

A

B

C

D

E

F

G

APPENDICES

'Radomes' at the encryption operations centre, Misawa airbase, Japan. The portmanteau word 'radome' is derived from 'radar' and 'dome' and describes a weatherproof enclosure that protects an antenna. © Preston Keres - Source: www.kereskreatives.com.

Wednesday 16 September 1998

17. Transatlantic relations/Echelon system

B4-0803, 0805, 0806 and 0809/98

Resolution on transatlantic relations/Echelon system

The European Parliament,

— having regard to its resolution of 15 January 1998 on transatlantic trade and economic relations ([1]),

— having regard to the Commission communication to the Council, the European Parliament and the Economic and Social Committee on a New Transatlantic Market,

— having regard to the conclusions of the EU-US Summit in London (18 May 1998),

A. considering the importance of defending and sharing the same values in the new era of globalisation,

B. pointing out that transatlantic relations are the most intense in the world, both at political and economic level,

C. whereas the progress and deepening of EU/US relations will lead to an increase in political and economic stability,

D. recalling the strong stand Parliament has taken concerning the extraterritorial effects of the Helms-Burton and d'Amato Acts,

E. aware of the recent interim study 'An appraisal of technologies of political control' produced by the STOA unit for the Civil Liberties Committee,

1. Stresses the importance of EU-US relations, which are based on common economic, political and security interests, as well as a common perception of responsibilities and needs at world level;

2. Considers that common political objectives include promoting peace, stability, democracy and development, as well as responding to global challenges through enhanced cooperation;

3. Recalls that the transatlantic economic relationship is underpinned by the most important trade and economic links in the world, and that the EU and the US have the world's largest and most complex economic relationship;

4. Welcomes the highly significant achievements obtained within the New Transatlantic Agenda (NTA) and recognised in the statement agreed at the EU-US summit; in this context, the Transatlantic Economic Partnership (TEP) would constitute a key instrument for developing the bilateral relationship;

5. Considers that the prospective agreement, to be negotiated within the TEP, in particular on mutual recognition agreements (MRAs) and 'equivalent standards', on government procurement and on intellectual property should drastically reduce bilateral conflicts on regulatory matters, and induce a process of 'regulatory convergence';

6. Supports the People-to-People initiative which, through its fostering of contacts in the business world, makes an important contribution to dismantling barriers in transatlantic trade;

7. Stresses however that US extraterritorial legislation, and in particular the Helms-Burton and d'Amato Acts, remain unacceptable to the European Union; asks the US Congress to act speedily in order to eliminate such legislation and, in any case, to grant the waivers requested;

([1]) OJ C 34, 2.2.1998, p. 139.

8. Asks to be fully informed about the implications of the Understanding with respect to further negotiations of the MAI, as the Understanding codifies some of the core principles of the MAI project, such as expropriation and compensation;

9. Welcomes the joint declaration issued by the Delegation for relations between the European Parliament and the US Congress on the strengthening of interparliamentary dialogue in order to develop a balanced and mutually advantageous transatlantic partnership; considers therefore that existing interparliamentary exchanges should be greatly reinforced;

10. Recognises the vital role of international cooperation with regard to electronic surveillance in stopping and preventing the activities of terrorists, drug traffickers and organised criminals;

11. Further recognises, however, the vital importance of having democratically accountable systems of control with respect to the use of these technologies and the information obtained;

12. Asks for such surveillance technologies to be subject to proper open debate both at national and EU level as well as procedures which ensure democratic accountability;

13. Calls for the adoption of a code of conduct in order to ensure redress in case of malpractice or abuse;

14. Considers that the increasing importance of the Internet and worldwide telecommunications in general and in particular the Echelon System, and the risks of their being abused, require protective measures concerning economic information and effective encryption;

15. Instructs its President to forward this resolution to the Commission, the Council and the US Congress.

---

18. Waste management

A4-0235/98

Resolution on the communication from the Commission to the European Parliament and the Council concerning the application of Directives 75/439/EEC, 75/442/EEC, 78/319/EEC and 86/278/EEC on waste management (COM(97)0023 – C4-0368/97)

The European Parliament,

– having regard to the communication from the Commission (COM(97)0023 – C4-0368/97),

– having regard to Article 5 of the EC Treaty,

– having regard to its resolutions of 8 April 1992 [1] on the application of Community environment law and 14 May 1997 [2] on the Commission communication on the application of Community environment law,

– having regard to the report of the Committee on the Environment, Public Health and Consumer Protection (A4-0235/98),

A. having regard to its commitment to sustainable development as one of the European Union's priority objectives,

B. whereas effective application of Community environment law is a *sine qua non* for achieving sustainable development,

[1] OJ C 125, 18.5.1992, p. 122.
[2] OJ C 167, 2.6.1997, p. 92.

Brussels, 27 March 2000

Dear Mrs Fontaine,

On behalf of the signatories of the attached text, I hereby request that a temporary committee of inquiry be set up to investigate the alleged contravention of Community law (pursuant to Rule 151 of the Rules of Procedure) arising from the existence and presumed instances of use of the Echelon system.

The list of signatories is currently limited to 170 (i.e. more than the quorum of 157) but as it has not yet been possible to contact all the Members it goes without saying that it should remain open until this application has been considered by the Conference of Presidents.

Thank you for considering this request.

Yours sincerely,

Paul Lannoye
Chairman Verts/ALE

Request for the constitution (by virtue of article 151 of the Rules of Procedure) of a temporary committee of inquiry to *investigate alleged contraventions of Community law* due to the presumed existence and utilisation of the *Echelon* system

Grounds

A report of STOA (Scientific and Technological Options Assessment), carried out at the request of the commission for civil liberties, published in October 1999 entitled. *"Development of surveillance technology and risk of abuse of economic information"* mentions the existence of a system called *Echelon* which would allow the NSA *(National Security Agency)* of the United States to intercept, at a worldwide level, private telecommunications (fixed wire and portable telephones, fax machines and electronic mail) One of the main surveillance posts, which concerns Europe, is located at Menwith Hill, Yorkshire in the United Kingdom. This espionage system, originally created for military purposes, would appear to have been converted and directed at political and economic targets to the benefit, not only of the United States, but also of Canada, New Zealand, Australia and the United Kingdom

The information contained in this report was recently confirmed, thanks to publication by the NSA of declassified top secret documents. The contents represent, at the very least, *"alleged contraventions of Community law"*, according to the definition given in article 151 of the Rules of Procedure relating to the constitution of provisional committees of inquiry.

In fact, article 286 of the Treaty establishing the European Community submits to the *control of an independent supervisory body* the application of *Community acts on the protection of individuals with regard to the processing of personal data* and confirms the obligations of the Member States, by virtue of the secondary legislation, in this instance, directives 95/46/EC and 97/66/EC.

Thus, directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free circulation of such data (OJ L 281 of 23/11/1995), specifies in article 1, paragraph 1: *"In accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".*

Directive 97/66/EC, concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 024 of 20/01/1998), is even more clearly implicated. *"service providers must take appropriate measures to safeguard the security of their services"*, (recital 15); *"measures must be taken to prevent the unauthorised access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicy available telecommunication services.*(recital 16), *"where the rights of users and subscribers are not respected, national legislation must provide for judicial remedy; (...) sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive"* (recital 25). With regard to the purpose of the directive, it consists of *"the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector ..."* (article 1, paragraph 1) With regard to the confidentiality of communications, article 5, paragraph 1 of

this directive stipulates: *"Member States shall ensure, via national regulations, the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with article 14 (1)".*

Although it is true that the above-mentioned directives are only applicable to policies and activities governed by Community law, it is legitimate to consider that Community institutions and agencies, inasmuch as they are service providers, have failed in their duty to *"take appropriate measures to safeguard the security of their services".* In addition, it would also be legitimate to consider that the existence of an economic espionage system which benefits, in particular, a member State, to the detriment of other member States, would be a contravention of Community law, specifically with regard to article 10 of the Treaty establishing the European Community. *"Member States shall take all appropriate measures, whether general or particular to ensure fulfillment of the obligations arising out of this Treaty or resulting from action taken by the institutions of the Community. They shall facilitate the achievement of the Community's task. They shall abstain from any measure which could jeopardise the attainment of the objectives of this Treaty."* Likewise, Chapter VI (previously entitled Chapter V) of the Treaty of the European Community "common rules on competition, taxation and approximation of laws" provides in article 81.1 (previously 85 1) *"shall be prohibited as incompatible with the common market : all agreements between undertakings, decisions by associated of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the common market..."* Thus, the allegations of industrial espionage practised via the *Echelon* system to the detriment of companies in Europe, who will have lost major contracts to Anglo-Saxon companies because of this, represent a distortion of competition within the internal market and, consequently, a violation of Community law.

Moreover, article 6.2 of the European Union Treaty stipulates that *"the Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms",* of which article 8 in particular recognizes the respect of the right to privacy. In this regard, the approximation of national laws relating to the processing of personal data, which is the objective of directive 95/46/EC *"must not result to any lessening of the protection that they afford but must, on the contrary, seek to ensure a high level of protection in the Community"* (Directive 95/46/EC, recital 10)

Furthermore, according to the same directive, *"the principles of protection of rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data."* (recital 11). These principles are also protected by Convention 108 of the Council of Europe relating to the *protection of individuals with regard to automatic processing of personal data.*

Articles 11 and 12 (previously J1 and J2) of the European Union Treaty can also be invoked: *"the Member States shall work together to enhance and develop their mutual political solidarity. They shall refrain from any action which is contrary to the interests of the Union or likely to impair its effectiveness as a cohesive force in international relations. The Council shall ensure that these principles are complied with."*

It should be noted that article 151 of the Regulation, relating to the constitution of a committee of inquiry mentions *"alleged contraventions of Community law"*. In other words, the said contravention does not necessarily have to be established. This is the very reason for the constitution of a committee of inquiry, to establish whether the allegations in question can be authenticated or are groundless. In the case in question, the existence of *Echelon* can hardly be denied since it has now been established by recently declassified top secret documents issued by the National Security Agency NSA.

Moreover, the principle of proportionality - ratified by the jurisprudence of the European Court of Human Rights - appears at the very least to be disparaged because of the lack of balance between the means being implemented by the *Echelon* network and its objectives

Finally, and following the precautionary principle, it appears to us not only legitimate but also indispensable, in the light of information in our possession regarding the existence of *Echelon* and the real or potential risks that this system can bring to bear on the European Union, its institutions and bodies, on certain Member States and companies, not forgetting individuals and organisations, that an investigative inquiry should be set up to distinguish truth from falsehood and, where applicable, to use the necessary legal and technical means to provide effective protection for fundamental freedoms and rights and to obtain full respect for Community law. Commissioner Bangemann, called upon by the Parliament, declared on behalf of the Commission in a plenary session on 14 September 1998, in response to concern expressed by several MEPs from all parties regarding the existence and capacity of Echelon *If the system existed in such a form, that would naturally represent a blatant violation of rights, the individual rights of citizens, and of course an attack on the security of the Member States. That is absolutely clear. The Council, and naturally the Commission and the Parliament as well, would have to respond the instant something of that kind was officially confirmed.* "

The European Parliament, which has moreover played a major role in issuing information about *Echelon*, must shed light on the existence of this network and on how it is being used in order to respond to growing concern and to the legitimate questions of European citizens To this end, it is therefore proposed that a committee of inquiry be constituted which will also enable us to distinguish the responsibilities involved and to highlight any possible gaps and shortcomings.

Groupe V/Ale 48/48

Ahern Nuala
Auroi Danielle
Bautista Carlos
Boumedine-Thiery Alima
Bouwman Theo
Breyer Hiltrud
Buitenweg Kathalijne
Celli Giorgio
Ceyhun Ozan
Cohn-Bendit Daniel
De Roo Alexander
Echerer Mercedes
Evans Jill
Flautre Hélène
Frassoni Monica
Gahrton Per
Graefe zu Baringdorf FW
Hautala Heidi
Hudghton Ian
Isler-Beguin Marie Anne
Jonckheer, Pierre
Knorr Gorka
Kreissl-Dorfler Wolfgang
Lagendijk Joost
Lambert Jean
Lannoye Paul
Lipietz Alain
Lucas Caroline
MacCormik Neil
Maes Nelly
McKenna Patricia
Messner Reinold
Noguira Camilo
Onesta Gérard
Ortuondo Josu
Pietrasanta Yves
Rod Didier Claude
Ruehle, Heide
Schorling Inger
Schroder Ilka
Schroedter Elisabeth
Sorensen Patsy
Staes Bart
Turmes Claude
Vander Taelen Lucas
Voggenhuber Johannes
Wyn Eurig
Wuori Matti

Groupe GUE 42/42

Ainardi Sylviane
Alavanos Alexandros
Alyssandrakis Konstantinos
Bakopoulos Emmanuouil
Bertinotti Fausto
Bordes Armonia
Boudjenah Yasmine
Brie Andreas
Cauquil Chantal
Cossutta Armando
Di Lello Giuseppe
Eriksson Marianne
Fiebiger Christel
Figueiredo Ilda
Frahm Pernille
Fraisse Geneviève
Gonzalez Laura
Hue Robert
Jove Salvador
Kaufmann Sylvia-Yvonne
Korakas Efstratios
Koulourianos Dimitrios
Krivine Alain
Laguiller Arlette
Manisco Lucio
Markov Helmut
Marset Campos Pedro
Meijer Erik
Miranda Joaquim
Modrow Hans
Morgantini Luisa
Papayannakis Michail
Puerta Alonso
Schmid Herman
Seppanen Esko
Sjostedt Jonas
Sylla Fodé
Theonas Ioannis
Uca Feleknas
Vachetta Roseline
Vinci Luigi
Wurtz Francis

Groupe PSE 15/180

Caudron Gérard
Dehousse Jean-Maurice
Desir Harlem
Duhamel Olivier
Ferreira Anne
Garot Georges
Gui-Quint Catherine
Hazan Adeline
Ilvari Ulpu
Lienemann Marie-Noelle
Myller Riitta
Nair Sami
Roure Martine
Savary Gilles
Seguro Antonio

Groupe PPE 11/232

De Mita Ciriaco
Deprez Gérard
Ebner Michl
Grosch Mathieu
Hansenne Michel
Kauppi Piia-Noora
Korhola Eija-Riitta
Matikainen Marjo
Thyssen Marianne
Vatanen Ari
Wijkman Anders

Groupe ELDR 4/51

De Clerck Willy
Di Petro
Ries Frédérique
Stercks Dirk

Groupe UEN 28/30

Abitbol
Andrews
Angelilli
Berlato
Berthu
Camre
Caullery
Collins
Coûteaux
Crowley
de La Perriere
Fini
Fitzsimon
Gallagher
Hyland
Kuntz
Marchiani
Montfort
Muscardini
Musumeci
Nobilia
Pasqua Charles
Poli Bortone
Queiro
Ribeiro e Castro
Segni
Souchet
Varaut
Thomas-Mauro
Turchi

Groupe EDD 12/16

Bernié Jean-Louis
Belder Bas
Esclopé Alain

Blokland Johannes
Bonde Jens-Peter
Farage Nigel
Holmes Michael
Krarup Ole
Mathieu Véronique
Okking Jens Dyhr
Sandbaek Ulla
Saint-Josse
Titford Jeffrey
van Dam Rijk

Groupe TDI 6/18

Bonino Emma
Cappato Marco
Dell'Alba Gianfranco
Della Vedova Benedetto
Dupuis Olivier
Turco Maurizio

****

Signatures effectives : 170
Quorum : 157

Parlement Européen
La Présidente

Monsieur Romano PRODI
Président de la Commission européenne
Rue de la Loi, 200
B-1049 BRUXELLES

302946 30.III.2000

Monsieur le Président,

Le 30 mars prochain, le Conseil et la Commission présenteront au Parlement Européen leur position quant à la question de l'interception des télécommunications évoquée lors de l'audition sur la protection des données qui s'est déroulée les 22 et 23 février dernier.

Cette question ayant déjà fait l'objet de nombreuses questions écrites et orales au cours des deux dernières années, je vous saurai gré, dans l'intérêt d'un meilleur débat, si la Commission pouvait développer essentiellement les points suivants, à savoir la nécessité :

1. d'assurer aux citoyens européens, indépendamment de leur nationalité, une protection conforme à l'art. 8 de la Convention européenne sur la protection des droits de l'homme et aux dispositions pertinentes adoptées sur la base des Traités communautaires et de l'Union ;

2. de s'assurer que toute activité d'interception des télécommunications respecte la jurisprudence de la Cour des droits de l'homme quant à la nécessité d'une proportionnalité entre l'ingérence dans la vie privée et l'intérêt public, ce qui justifierait l'interception des communications des citoyens de l'Union ;

3. d'établir sur la base des principes cités aux paragraphes précédents une norme européenne assurant que les exigences de la « sécurité européenne » soient compatibles avec celles de la « citoyenneté européenne » et prévoyant que toute forme d'interception soit notifiée aux Etats membres où se trouvent les personnes interceptées ;

4. que toute mesure adéquate soit prise par les institutions européennes pour éviter des interceptions par des pays tiers et pour établir des rapports périodiques sur les problèmes éventuellement rencontrés ; ceux-ci seraient soumis au Parlement européen conformément à l'annexe 7 de son règlement ;

5. de rendre plus simple et efficace l'action des autorités qui assurent la protection des données au niveau de l'Union par l'unification progressive des structures (Autorité prévue par l'art. 286 du TCE, Autorité Schengen, Europol, Convention douanière, ...) et le renforcement au plus haut niveau possible des standards de protection ;

6. d'adopter les mesures technologiques (câblage, cryptographie,...) pour contrecarrer les interceptions en provenance de l'extérieur de l'Union ainsi que les mesures législatives et financières nécessaires pour développer les outils et le savoir-faire informatique européens dans ce domaine ;

7. de s'assurer que chaque Etat de l'Union, conformément aux obligations de coopération loyale prévues par les articles 10 du TCE et 11, par. 2 et 29 du TUE, informe les autres Etats membres ainsi que les Institutions de l'Union de la portée de ses accords avec des pays tiers en matière d'interception des télécommunications.

Convaincue, Monsieur le Président, que vous partagez nos préoccupations quant à la nécessité que l'Union se dote dans les meilleurs délais d'un cadre législatif qui puisse, d'une part, renforcer la confiance entre ses Etats membres et, d'autre part, protéger d'avantage la vie privée de ses citoyens, je vous remercie de l'attention que vous voudrez bien accorder à cette question.

Je vous prie d'agréer, Monsieur le Président, l'expression de ma haute considération.

Nicole FONTAINE

Annexe

Letter of 13 April 2000 from Mr Enrique Barón Crespo, chairman of the PSE Group, to Mrs Nicole Fontaine, President of the European Parliament

---

Translation

Dear Madam President,

Subject: Proposal to set up a temporary committee pursuant to Rule 150(2) of the Rules of Procedure

The hearings held in the Committee on Citizens' Freedoms on 22 and 23 February 2000 concerning the protection of personal data revealed the following facts:

1. Confirmation of the existence of a communications interception system known as Echelon, the operation of which is described in the STOA report entitled 'Development of Surveillance Technology and Risks of Abuse of Economic Information';

2. The participation of at least one Member State in the Echelon system;

3. The possibility that this system is being used for interception and surveillance activities for purposes other than those authorised by Article 8 of the European Convention for the Protection of Human Rights and, consequently, in violation of Articles 6(2), 11 and 12 of the EU Treaty and Article 286 of the EC Treaty and the principles set out in EP and Council Directives EC/1995/46 and EC/1997/66 on the processing of personal data and the protection of privacy in the telecommunications sector;

4. The vulnerability of systems and means of communication and the inadequacy of devices for transmitting and encrypting data, given the possibility of misuse by public authorities or private entities;

5. The inadequacy of data protection legislation and the lack of consistency in provisions relating to cooperation between the Member States in this sphere.

Bearing in mind the statements made by the Council and Commission on 23 March 2000:

- Given that there is a need for a broad range of measures at different levels to deal with the risks highlighted by the Echelon system and to safeguard the fundamental rights of European citizens,

- I propose that the Conference of Presidents recommends the setting up of a temporary committee pursuant to Rule 150(2) of the Rules of Procedure which, by pooling the competences of the committees on Citizens' Freedoms, Foreign Affairs and Industry, could examine without delay all the problems revealed by the report on the Echelon system.

The temporary committee should be instructed to propose:

political initiatives to ensure a climate of better trust in cooperation between the Member States, which will have to be called upon to publish their agreements with non-member countries on this matter (particularly important with a view to enlargement);

measures to prevent non-member countries from carrying out any form of interception in the territory of the Union beyond that required by joint measures to combat organised crime; measures required to ensure the protection of privacy in terms of both commercial policy and in the area of combating organised crime;

legislative measures to update and harmonise provisions on the protection of personal data and to simplify and step up action by the supervisory authorities, within the framework of an appropriate strategy to guarantee the fundamental rights of citizens more effectively, even by ending the Union's dual system for protecting data, i.e. at Community level and at the level of police and judicial cooperation in criminal matters (Third Pillar), and the proliferation of supervisory authorities (Schengen, Europol, customs conventions, etc.);

appropriate measures concerning the adoption of tools and technologies (cabling, encryption) to counteract interception by non-member countries; legislative and financial measures subsequently to develop European informatics tools and know-how in this sector.

Having regard to the provisions of Rule 152 of the Rules of Procedure, the temporary committee could be composed of 21 members, including 12 from the Committee on Citizens' Freedoms, 4 from the Industry Committee, 4 from the Foreign Affairs Committee and the President. Representatives of the Legal Affairs Committee might also be included.

The temporary committee will be required, within one year, to propose the measures necessary to deal with the risks posed to citizens' fundamental rights and the interests of European firms as a result of the possible misuse of systems for the widespread interception of communications beyond national frontiers.

The temporary committee will report to the European Parliament on its activities by the end of July 2000 and will draw up a detailed report on the topics listed by the end of its mandate.

(Closing formula and signature)

EUROPEAN PARLIAMENT

TEMPORARY COMMITTEE ON THE ECHELON INTERCEPTION SYSTEM

MINUTES

of the constituent meeting

6 July 2000

STRASBOURG

The meeting was opened at 10.42 a.m. with Mrs Lalumière, Oldest Member, in the chair.

1. Election of chairman

The chairman announced the purpose of the meeting, viz. to elect the committee's chairman and three vice-chairmen, and to appoint the rapporteur. She noted that a quorum had been reached.

Mr Schmid nominated Mr Coelho. The committee approved the nomination unopposed with one abstention.

The chairman congratulated Mr Coelho on his election and invited him to take the chair.

2. Election of the committee bureau

The chairman called on members to submit nominations for vice-chairmen.

Mr Wiersma nominated Mrs Berger.

Mr Ceyhun nominated Mr MacCormick.

Mrs Thors nominated Mrs Plooij-van Gorsel.

Mr Krivine nominate Mr di Lello.

The chairman pointed out that the number of nominations exceeded the number of posts to be filled.

The following spoke: Frahm, Krivine, Ceyhun, Dimitrakopoulos, McKenna, Wiersma and Schröder. The chairman drew attention to the provisions of the Rules of Procedures and called on members to submit nominations for first vice-chairman.

Mr Wiersma nominated Mrs Berger.

Mrs Thors nominated Mrs Plooij-van Gorsel.

The chairman announced that the election would have to be held by secret ballot and called on members to appoint two tellers. Mr Thielemans and Mr Dimitrakopoulos were nominated. The committee agreed to their appointments unanimously. The chairman suspended the meeting at 10.58 a.m. The meeting was resumed at 11.07 a.m.

Mr Wiersma proposed that voting be adjourned. The chairman pointed out that voting was in progress and could not be interrupted. Mrs Banotti spoke on a point of order. Members then voted by secret ballot.

Mrs Plooij-van Gorsel was elected by 24 votes to 11 cast for Mrs Berger.

The chairman and Mrs Berger congratulated Mrs Plooij-van Gorsel on her election.

The chairman called on members to submit nominations for second vice-chairman.

Mr Ceyhun nominated Mr MacCormick.

Mr MacCormick was elected by acclamation.

The chairman called on members to submit nominations for third vice-chairman.

Mr Krivine nominated Mr di Lello.

Mr di Lello was elected by acclamation.

3. Appointment of rapporteur

The chairman proposed that Mr Schmid be appointed as rapporteur, and invited members to submit other nominations.

Mrs McKenna and Mr Vattimo nominated Mrs Berger. Mrs Berger declined to be nominated.

Mr Vattimo spoke.

Mr Turco agreed to be nominated.

Mr Wiersma and Mr Pirker seconded Mr Schmid's nomination.

Seven members called for the vote on the appointment of the rapporteur to be held by secret ballot. The chairman suspended the meeting at 11.21 a.m. The meeting was resumed at 11.35 a.m.

Members voted by secret ballot.

Mr Schmid was appointed by 27 votes to 7 cast for Mr Turco, with one blank vote.

4. Chairman's announcements

The chairman outlined the committee's mandate, informed members of the practical arrangements for the committee's work, and drew attention in particular to the importance of complying with the rules in force on the treatment of confidential information.

5. Statement by rapporteur, followed by exchange of views

The rapporteur set out his guidelines for drawing up a programme of activities that would be considered at the committee's next meeting.

Mrs McKenna and Mrs Plooij-van Gorsel spoke.

6. Date and place of next meeting

The next meeting would be held in Strasbourg on 5 September 2000 at 5.30 p.m.

The meeting was closed at 11.54 a.m.

DELTAGERLISTE/ANWESENHEITSLISTE/ΚΑΤΑΣΤΑΣΗ ΠΑΡΟΝΤΩΝ/LIITE RECORD OF ATTENDANCE/LISTA DE ASISTENCIA/LISTE DE PRESENCE/ELENCO DEI PRESENTI/PRESENTIELIJST/LISTA DE PRESENÇAS/LÄSNÄOLOLISTA/DELTAGARLISTA

Til stede	Formandskabet/Vorstand/Προεδρείο/Bureau/Ufficio di Presidenza/Mesa/Puhemiehistφ/J L. Presidium. (*)
Anwesend	COELHO (P), PLOOIJ-VAN GORSEL (1st VP), MacCORMICK (2nd VP), DE LELLO FINUOLI (3rd VP)
Παρόντες	Medlemmer/Mitglieder/Μέλη/Members/Diputados/Diputis/Deputati/Leden/Deputados/jδsenet/ Ledamöter:
Present	BANOTI, VON BOETTICHER, CEDERSCHIÖLD, DEPREZ, DIMITRAKOPOULOS, HERNANDEZ, KLAMT, MARTIN,
Presentes	OOSTANDER, PIRKER, ZAPPALA,
Présents	BERGER, EVANS R , KARAMANOU, LALUMIERE, LUND, MANN, PAASILINNA, SCHMID, VATTIMO, WIERSMA, CEYHUN, McKENNA, KRIVINE, TURCO, BELDER
Presenti	
Aanwezig	Stedfortrædere/Stellvertreter/Αναπληρωτές/Substitutes/Suplentes/Suppliants/ Membri supplenti/Plaatsvervangers/Membros suplentes/Varajäsenet/Suppleanter:
Lasna	CORNILLET, GAWRONSKI, GIANNAKOU-KOUTSIK, MATTIKAINEN-KALLSTRÖM, NEWTON DUNN, NIEBLER, OOMEN-RUIJTEN, ROVSING, VAN HECKE
Närvarande	ANDERSSON, CAUDRON, GEBHARDT, MARINHO, PACIOTTI, SWIEBEL, SWOBODA, TERRON I CUSI, THIELEMANS, TITLEY
	ANDREASEN, THORS, BOUMEDIENE-THIERY, SCHRÖDER I , LAMBERT, FRAHM, PAPYANNAKIS,

Art 153,2	GEBHARDT, FIORI
Art 166,3	
Art 162,6 Endv. Deltog/Weitere Teiln / Συμμετείχαν επίσης/Also present Participaron igualmente/ Participaient également/ Hanno partecipato altresi'/ Andere deelnemers/ Outros participantes/ Muut osallistujat/ Dessutom deltog	

* (P) =Formand/Vorsitzender/Πρόεδρος/Chairman/President/Presidente/Voorzitter/Presidente/Puhemies/Ordfφrande
(VP) =Næstform /Stellv. Vorsitz /Αντιπρόεδρος/Vice-Chairman/Vice-President/Vicepresidente/Varapuhemies
Ondervoorz /Vice-Pres /Vicepres/Vice ordförande.

Til stede den/Anwesend am/Παρών στις/Present on/Present le/Presente il/Aanwezig op/Presente em/Presente el/Lδsnδ/Nδrvarande den

Efter indbydelse fra formanden/Auf Einladung d Vorsitzenden/Με πρόσκληση του Προέδρου/At the invitation of the Chairman/Por invitación del presidente/Sur l'invitation du président/Su invito del presidente/Op uitnodiging van de voorzitter/A convite do presidente/Puhemiehen kutsusta/ På ordförandens inbjudan· Radet/Rat/Συμβούλιο/Council/Consejo/Conseil/Consiglio/Raad/Conselho/Neuvosto/Rådet· (*) Kommissionen/Kommission/Επιτροπή/Commission/Comisión/Commissione/Commissie/Commissão/Komissio/ Kommissionen (*) Cour des comptes: CES:		
Andre deltagere/Andere Teilnehmer Επίσης Παρόντες/Also present Otros participantes/Autres participants/Altri partecipanti Andere aanwezigen/Outros participantes Muut osallistujat/Övriga deltagare		
Gruppernes sekretariat Sekretariat der Fraktionen Γραμματεία των Πολ Ομάδων Secretariat political groups Secr. De los grupos politicos Secr. Groupes politiques Segr. Dei gruppi politici Secr. Van de fracties Secr. Dos grupos políticos Puolueryhmien sihteeristö Gruppernas sekretariat	PPE-DE PSE ELDR Verts/ALE GUE/NGL UEN TDI EDD NI	SCRIBAN, SALAFRANCA VAN DE WATER VAN DEN BROUCKE ROBERT JEAN LUC BATTISTINI
Cab Du Président		DE VICENTE, LAGARDE
Cab. Du Secrétaire Général		
Generaldirektorat Generaldirektion Γενική Διεύθυνση Directorate-General Dirección general Direction générale Direzione generale Directoraat-generaal Direcção general Contrôle financier Service juridique Pääosasto Generaldirektorat	I II III IV V VI VII	NICKEL, LIBERATO BARAGIOLA SILVESTRO SCHOO, KARAMARCOS
Udvalgssekretariatet Ausschubsekretariat Γραμματεία επιτροπής Committee secretariat Secretaria de la comisión Secrétariat de la commission Segretariato della commissione Commissiesecretariaat Secretaria de comissão Valiokunnan sihteeristö Utskottssekretariatet		LOWE, JACOB, HELMBERG
Assist /Βοηθός		MALOUTA

* (P) =Formand/Pres /Πρόεδρος/Chairman/President/Voorzitter/Puhemies/Ordförande
(VP) =Næstform /Vize-Pres /Αντιπρόεδρος/Vice-Chairman/Vice-President/Ondervoorz /Vice-pres/Varapuhemies/Vice ordförande.
(M) =Medlem /Mitglied/Μέλος/Member/Miembro/Membre/Membro/Lid/Membro/Jäsen/Ledamot
(F) =Tjenestemand/Beamter/Υπάλληλος/Official/Funcionario/Fonctionnaire/Funzionario/Ambtenaar/ Functionário/Virkamies/Tjänsteman

27. Urges the Member States to ratify the Montreal Convention as soon as possible to improve the protection of passengers in the event of accident and to enable the updating of Council Regulation (EC) No 2027/97; in this regard, stresses the importance of clear and easily accessible information to air passengers on applicable liability limits, including the relevant time limits for issuing complaints, which should be automatically provided by airline companies whilst booking;

28. Considers that accessibility of air travel must be improved for all passengers, including for disabled passengers, children and the elderly;

29. Welcomes the efforts made by airlines to implement staff training activities in the field of assistance to passengers in general, and those with reduced mobility in particular;

30. Calls on the Commission to bring forward legislative proposals to prohibit any European Union airline or airport from charging an extra fee to persons with reduced mobility for being assisted onto or off any aeroplane in the European Union;

Health aspects

31. Considers that health should be given a higher profile and that the air passengers and crew should be sufficiently informed about the health aspects of air travel;

32. Recommends that the airlines give pre-take-off health briefing on long-haul flights comparable to the safety briefing already required and that such information be available to passengers on their tickets, in particular concerning preventative action;

33. Calls on the Commission as a matter of urgency to allocate monies from the EU research budget to carry out an independent evaluation of the possible public health risks for air passengers who travel on long-haul flights, including carrying out a comprehensive study into the whole issue of deep vein thrombosis; calls on the Commission to carry out this independent research in consultation with EU airline companies and with EU consumer groups;

34. Calls on European Union airlines to inform passengers of the percentage degree seat pitch available to passengers travelling in economy class;

*

* *

35. Instructs its President to forward this resolution to the Council and the Commission.

---

21. Echelon

A5-0264/2001

European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) (2001/2098(INI))

The European Parliament,

— having regard to its decision of 5 July 2000 to set up a Temporary Committee on the Echelon Interception System and the mandate issued to the Temporary Committee [1],

— having regard to the EC Treaty, one objective of which is the establishment of a common market with a high level of competitiveness,

---

[1] OJ C 121, 24.4.2001, p. 131.

Wednesday 5 September 2001

— having regard to Articles 11 and 12 of the Treaty on European Union, which impose on the Member States a binding requirement to enhance and develop their mutual political solidarity,

— having regard to the Treaty on European Union, in particular Article 6(2) thereof, which lays down the requirement that the EU must respect fundamental rights, and Title V thereof, which sets out provisions governing the common foreign and security policy,

— having regard to Article 12 of the Universal Declaration of Human Rights,

— having regard to the Charter of Fundamental Rights of the EU, Article 7 of which lays down the right to respect for private and family life and explicitly enshrines the right to respect for communications, and Article 8 of which protects personal data,

— having regard to having regard to the European Convention on Human Rights (ECHR), in particular Article 8 thereof, which governs the protection of private life and the confidentiality of correspondence, and the many other international conventions which provide for the protection of privacy,

— having regard to the work carried out by the Temporary Committee on the Echelon Interception System, which held a large number of hearings and meetings with experts of all kinds, and in particular with senior representatives of the public and private sectors in the sphere of telecommunications and data protection, with employees of intelligence and information services, with journalists, with lawyers with expert knowledge of this area, with members of the national parliaments of the Member States, etc.,

— having regard to Rule 150(2) of its Rules of Procedure,

— having regard to the report of the Temporary Committee on the Echelon Interception System (A5-0264/2001),

The existence of a global system for intercepting private and commercial communications (the Echelon interception system)

A. whereas the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the US, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt; whereas it seems likely, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that its name is in fact Echelon, although this is a relatively minor detail,

B. whereas there can now be no doubt that the purpose of the system is to intercept, at the very least, private and commercial communications, and not military communications, although the analysis carried out in the report has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed,

C. whereas, therefore, it is surprising, not to say worrying, that many senior Community figures, including European Commissioners, who gave evidence to the Temporary Committee claimed to be unaware of this phenomenon,

The limits of the interception system

D. whereas the surveillance system depends, in particular, upon worldwide interception of satellite communications, although in areas characterised by a high volume of communications only a very small proportion of those communications are transmitted by satellite; whereas this means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals, something which — as the investigations carried out in connection with the report have shown — is possible only to a limited extent; whereas the numbers of personnel required for the final analysis of intercepted communications imposes further restrictions; whereas, therefore, the UKUSA states have access to only a very limited proportion of cable and radio communications and can analyse an even more limited proportion of those communications, and whereas, further, however extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice,

The possible existence of other interception systems

E. whereas the interception of communications is a method of spying commonly employed by intelligence services, so that other states might also operate similar systems, provided that they have the required funds and the right locations; whereas France is the only EU Member State which is — thanks to its overseas territories — geographically and technically capable of operating autonomously a global interception system and also possesses the technical and organisational infrastructure to do so; whereas there is also ample evidence that Russia is likely to operate such a system,

Compatibility with EU law

F. whereas, as regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios: if a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP), although at present that title lays down no provisions on the subject, so that no criteria are available; if, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyal cooperation and with the concept of a common market based on free competition, so that a Member State participating in such a system violates EC law,

G. having regard to the statements made by the Council at the plenary sitting of 30 March 2000 to the effect that 'the Council cannot accept the creation or existence of a telecommunications interception system which does not respect the laws of the Member States and which violates the fundamental principles aimed at protecting human dignity',

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

H. whereas any interception of communications represents serious interference with an individual's exercise of the right to privacy; whereas Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference; whereas interference must be proportionate, so that competing interests need to be weighed up and, under the terms of the case law of the European Court of Human Rights, it is not enough that the interference should merely be useful or desirable,

I. whereas an intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and would not be compatible with the ECHR; whereas it would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable, or if the interference was not proportionate; whereas most of the rules governing the activities of US intelligence services abroad are classified, so that compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and foreseeability laid down by the European Court of Human Rights probably occur,

J. whereas the Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance,

K. whereas, in addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus; whereas the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, so that there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services,

Wednesday 5 September 2001

Are EU citizens adequately protected against intelligence services?

L. whereas the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and whereas in some cases parliamentary monitoring bodies do not even exist, so that the degree of protection can hardly be said to be adequate; whereas it is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services; whereas even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens; whereas it would be an encouragement for proportionate interference practices, if intelligence services were obliged to notify a citizen whose communications have been intercepted of this fact afterwards, for example five years after the interception took place,

M. whereas, in view of their size, satellite receiving stations cannot be built on the territory of a state without its consent,

N. whereas, in the event of cooperation between intelligence services under the CFSP or in the areas of justice and home affairs, the institutions must introduce adequate measures to protect European citizens,

Industrial espionage

O. whereas part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc., and whereas, for these reasons, the firms concerned are often subject to surveillance,

P. whereas the US intelligence services do not merely investigate general economic facts but also intercept detailed communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery; whereas detailed interception poses the risk that information may be used for the purpose of competitive intelligence-gathering rather than combating corruption, even though the US and the United Kingdom state that they do not do so; whereas, however, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled,

Q. whereas an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications,

R. whereas the situation becomes intolerable when intelligence services allow themselves to be used for the purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country, and whereas it is frequently maintained that the global interception system has been used in this way, although no such case has been substantiated,

S. whereas, during the visit by the delegation from the Temporary Committee to the US, authoritative sources confirmed the US Congress Brown Report, indicating that 5 % of intelligence gathered via non-open sources is used as economic intelligence; whereas it was estimated by the same sources that this intelligence surveillance could enable US industry to earn up to USD 7 billion in contracts,

T. whereas sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering in particular involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more commonly, by hacking

into internal computer networks; whereas only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering; whereas this applies systematically in the following three cases:

- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the firm's head office,

U. whereas risk and security awareness in small and medium-sized firms is often inadequate and the dangers of economic espionage and the interception of communications are not recognised,

V. whereas security awareness is not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations) and action is therefore necessary,

Possible self-protection measures

W. whereas firms can only make themselves secure by safeguarding their entire working environment and protecting all communications channels which are used to send sensitive information; whereas sufficiently secure encryption systems exist at affordable prices on the European market; whereas private individuals should also be urged to encrypt e-mails; whereas an unencrypted e-mail message is like a letter without an envelope; whereas relatively user-friendly systems exist on the Internet which are even made available for private use free of charge,

Cooperation among intelligence services within the EU

X. whereas the EU has reached agreement on the coordination of intelligence-gathering by intelligence services as part of the development of its own security and defence policy, although cooperation with other partners in these areas will continue,

Y. whereas in December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP; whereas the European Council decided furthermore that, in order to achieve this goal, by the year 2003 the Union should be able to deploy rapidly units of about 50 000-60 000 troops which should be self-sustaining, including the necessary command, control and intelligence capabilities; whereas the first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee,

Z. whereas cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense, and, secondly, it would have numerous professional, financial and political advantages; whereas it would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR; whereas the European Parliament would of course have to exercise appropriate monitoring,

AA. whereas the European Parliament is in the process of implementing European Parliament and Council Regulation (EC) No 1049/2001 of 30 May 2001 on public access to European Parliament, Council and Commission documents [1] by amending the provisions of its Rules of Procedure as regards access to sensitive documents,

[1] OJ L 145, 31.5.2001, p. 43.

Wednesday 5 September 2001

Conclusion and amendment of international agreements on the protection of citizens and firms

1. States, on the basis of the information obtained by the Temporary Committee, that the existence of a global system for intercepting communications, operating with the participation of the United States, the United Kingdom, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt;

2. Calls on the Secretary-General of the Council of Europe to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account;

3. Calls on the Member States — whose laws governing the interception capabilities of the secret services contain provisions on the protection of privacy which are discriminatory — to provide all European citizens with the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence;

4. Calls on the Member States of the European Union to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of the report of the European Parliament's temporary committee, and in particular Section 8.3.4.; emphasises the need to draw up joint standards which are better suited to the requirements of protecting the fundamental rights of EU citizens and more stringent than those guaranteed by Article 8 of the ECHR;

5. Calls on the Member States to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act at the next Intergovernmental Conference in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy;

6. Calls on the member countries of the Council of Europe to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities;

7. Urges the EU institutions in the meantime to apply the fundamental rights enshrined in the ECHR and its protocols and in the Charter within the scope of their respective powers and activities;

8. Calls on the UN Secretary-General to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations;

9. Regards it as essential that an agreement should be negotiated and signed between the European Union and the United States stipulating that each of the two parties should observe, vis-à-vis the other, the provisions governing the protection of the privacy of citizens and the confidentiality of business communications applicable to its own citizens and firms;

10. Calls on the US to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the US can be submitted to the Human Rights Committee set up under the Covenant; calls on the relevant American NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), to exert pressure on the US Administration to that end;

National legislative measures to protect citizens and firms

11. Urges the Member States to review and if necessary to adapt their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights as laid down in the ECHR and with the case law of the European Court of Human Rights;

12. Calls on the Member States to endow themselves with binding instruments which afford natural and legal persons effective protection against all forms of illegal interception of their communications;

13. Calls on the Member States to aspire to a common level of protection against intelligence operations and, to that end, to draw up a Code of Conduct (as referred to in paragraph 4) based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services;

14. Calls on the Member States to negotiate with the US a Code of Conduct similar to that of the EU;

15. Calls on those Member States which have not yet done so to guarantee appropriate parliamentary and legal supervision of their secret services;

16. Urges the Council and the Member States to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level; proposes that the European Parliament should play an important role in this monitoring and control system;

17. Calls on the Member States to pool their communications interception resources with a view to enhancing the effectiveness of the ESDP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission;

18. Calls on the Member States to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions;

Specific legal measures to combat industrial espionage

19. Calls on the Member States to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void; calls on the United States, Australia, New Zealand and Canada to join this initiative;

20. Calls on the Member States to undertake to incorporate in the EC Treaty a clause prohibiting industrial espionage and not to engage in industrial espionage against one another, either directly or with the assistance of a foreign power which might carry out operations on their territory, nor to allow a foreign power to conduct espionage operations from the soil of an EU Member State, thereby complying with the letter and spirit of the EC Treaty;

21. Calls on the Member States to undertake by means of a clear and binding instrument not to engage in industrial espionage, thereby signifying their compliance with the letter and spirit of the EC Treaty; calls on the Member States to transpose this binding principle into their national legislation on intelligence services;

22. Calls on the Member States and the US Administration to start an open US-EU dialogue on economic intelligence-gathering;

Wednesday 5 September 2001

Measures concerning the implementation of the law and the monitoring of that implementation

23. Calls on the national parliaments which have no parliamentary monitoring body responsible for scrutinising the activities of the intelligence services to set up such a body;

24. Calls on the monitoring bodies responsible for scrutinising the activities of the secret services, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals;

25. Calls on the Member States to make sure that their intelligence systems are not misused for the purposes of gathering competitive intelligence, an act at odds with the Member States' duty of loyal cooperation and with the concept of a common market based on free competition;

26. Calls on Germany and the United Kingdom to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights;

Measures to encourage self-protection by citizens and firms

27. Calls on the Commission and the Member States to inform their citizens and firms about the possibility that their international communications may, under certain circumstances, be intercepted; insists that this information should be accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology;

28. Calls on the Commission, the Council and the Member States to develop and implement an effective and active policy for security in the information society; insists that as part of this policy specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information; furthermore, insists on the establishment of a Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies;

29. Urges the Commission and Member States to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software;

30. Calls on the Commission and Member States to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes;

31. Calls on the Commission to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category;

32. Calls on the European institutions and the public administrations of the Member States systematically to encrypt e-mails, so that ultimately encryption becomes the norm;

33. Calls on the Community institutions and the public administrations of the Member States to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses;

34. Calls for particular attention to be paid to the position of the applicant countries; urges that they should be given support, if their lack of technological independence prevents them from implementing the requisite protective measures;

Other measures

35. Calls on firms to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency;

36. Calls on the Commission to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up;

37. Calls on the Commission to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authorities (the Council together with Parliament) to provide the necessary funding;

38. Proposes that its competent committee draw up an own-initiative report on security and the protection of secrecy in the European institutions;

39. Calls on the Commission to ensure that data is protected in its own data-processing systems and to step up the protection of secrecy in relation to documents not accessible to the public;

40. Calls on the Commission and the Member States to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme;

41. Urges states which have been placed at a disadvantage by distortions of competition resulting from state aid or the economic misuse of espionage to inform the authorities and monitoring bodies of the state from which the activities were undertaken in order to put a stop to the distorting activities;

42. Calls on the Commission to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres — in particular in those Member States where such centres do not yet exist — to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance;

43. Takes the view that an international congress on the protection of privacy against telecommunications surveillance should be held in order to provide NGOs from Europe, the US and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action;

*

* *

44. Instructs its President to forward this resolution to the Council, the Commission, the Secretary-General and Parliamentary Assembly of the Council of Europe and the governments and parliaments of the Member States and applicant countries, the United States, Australia, New Zealand and Canada.

"Individuals are essentially at the mercy of foreign [surveillance] systems, and here the need for protection is greater still. It must also be borne in mind that, by virtue of the specific nature of intelligence services, EU citizens may be affected by the activities of several such services at the same time. A uniform level of protection consistent with democratic principles would hence be desirable". (Report A5-264/2001 by Gerhard Schmid on the Echelon interception system).

"[...] technically it is possible, and if something is possible it doesn't matter very much if it has been done or not; what is important to me is that we should protect ourselves, and that neither France nor Germany nor the Netherlands protect themselves in isolation because this is a question that concerns the European Union as a whole." (Statement by Arthur Paecht, rapporteur of the Committee for Defence and the Armed Forces, French National Assembly, at the meeting of the Echelon Committee, 28 November 2000).

This study, the first to appear in the new *European Parliament History Series*, retraces the work of Parliament and in particular of its Temporary Committee on the Echelon Interception System, following the revelation of the existence of a spy system managed by the United States and designed for non-military targets: governments, organisations and businesses virtually all over the world.

The studies of the European Parliament History Series are primarily based on documents preserved in and made available to the public by the Historical Archives of the European Parliament.

This is a publication of the
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services, European Parliament

PE 538.877
ISBN: 978-92-823-6260-0
DOI: 10.2861/76176
CAT: QA-02-14-934-EN-N