EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

Vol 1/5

Presentation and Analysis

1) Presentation of the four studies

2) Analysis: Data protection and human rights in the European Union and the role of the European Parliament.

Document de travail pour le Panel STOA

Luxembourg, December 1999 PE 168.184/Vol 1/5/EN

Cataloguing data:

Title:	**Vol 1/5: Présentation et analyse** **1) Présentation des quatre études** **2) Analyse: protection des données et Droit de l'Homme dans l'Union Européenne et rôle du Parlement Européen**
Workplan Ref.:	EP/IV/B/STOA/98/1401
Publisher:	European Parliament Directorate General for Research Directorate A The STOA Programme
Author:	Peggy Becker - visiting researcher Under the supervision of Dick Holdsworth Head of the STOA Team
Editor:	Mr Dick HOLDSWORTH, Head of STOA Unit
Date:	Octobre 1999
PE number:	PE 168.184 Vol 1/5/EN

This document is a working Document for the 'STOA Panel'. It is not an official publication of STOA.
This document does not necessarily represent the views of the European Parliament

C O N T E N T S

INTRODUCTION

The term 'privacy', although in use for only a comparatively short time, actually refers to a situation which is as old as the desire of individuals to be protected from interference by others. Privacy is the individual's intimate sphere of existence which must, therefore, be concealed from the knowledge of other people and shielded from their curiosity.

The right to respect for privacy is an individual right acknowledged fairly recently. Article 8(1) of the European Convention on Human Rights[1] (ECHR) lays down that: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' That Convention is one of a number of international and national legal instruments which acknowledge that principle of protection. But 'privacy' has never been properly defined: it covers the right to a private life, the right to secrecy of a person's correspondence, including communication by telephone and other electronic means, and protection against the misuse of information technology and the processing of personal data. That right was initially protected by specific provisions – inviolability of the home, of correspondence and of professional secrecy. Subsequently, with the arrival of more modern forms of attacks and violations – electronic interception; telephone tapping; recording, etc. - an individual's private life came to be protected by general provisions since, during the 1990s, infringements had increased beyond all measure. Accordingly, the Data Protection Convention was signed in Strasbourg on 28 January 1981, and it entered into force on 1 October 1985. The Convention does not include any rules which are directly applicable in the national legal orders of the Member States, it merely sets out principles designed to govern the protection of privacy which the Member States undertake to implement, with all the states having had to adopt legislation in conformity with the those principles before depositing their instruments of ratification.

The protection of privacy is, therefore, properly enshrined in national and international legal orders as well as in Community law. Set out in those terms, one might imagine that the right was indefeasible, but we must add that it has to be reconciled with requirements relating to security, national defence and anti-terrorism campaigns. It is with a view to meeting those requirements that certain exceptions are authorised. For example, lawful interception of communications is authorised, but it is subject to compliance with stringent strict rules, the broad thrust of which was set out by the European Union and subsequently followed by the Member States. Apart from such 'lawful interceptions', the European Union, which is bound to apply the ECHR and the other relevant conventions, will have to combat not only unlawful interceptions but also lawful interceptions used for purposes other than the primary (authorised) intention. The development of new technologies has made it easy to do that.

Specific risks arise from the use of modern means of communication (fax, cellular phones, the Internet, etc.) with respect to the confidentiality of messages, particularly in the economic sphere where such means are being used more and more frequently for commercial activities.

Furthermore, over the same period, a vast range of surveillance techniques has been developed, such as parabolic and laser microphones. They may be defined as being devices or systems which can monitor, track and assess the movements of individuals, their property and other assets. These new forms of surveillance have led to the intercepted communications being processed by computer. The consequences of such interceptions may be significant, particularly from the economic point of view. This is, therefore, an area of technical progress in which the rules of a bygone age have been rendered obsolete by new forms of interception which are constantly increasing in number and which may not yet be deemed to be violations.

[1] The definitive text of this Convention was signed in Rome on 4 November 1950. However, its ratification by the Member States took some time. It was not until September 1997 that all the Member States had ratified it.

In order to remedy that, the European Union and, more specifically, the European Parliament have set in motion a joint action. That is why the Committee on Civil Liberties and Internal Affairs[2] asked STOA (Scientific and Technological Options Assessment) to draw up a study on this topic. The aim of this Briefing Note is to present that study which consists of four reports setting out a list of the new telecommunications technologies, the risks inherent therein and the methods to be developed with a view to eliminating those risks.

In an effort to provide an overview of the entire issue, this Briefing Note begins by summarising the four studies before undertaking an analysis which covers lawful interceptions and legislation currently in force as well as global interceptions of communications and cryptography, which might provide a solution to the issue of confidentiality.

[2] In July 1999, the name of the committee was changed to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, known by the acronym LIBE.

Part One:

PRESENTATION OF THE FOUR STUDIES

INTRODUCTION:

In response to a request from the Committee on Civil Liberties and Internal Affairs[3], STOA commissioned a study entitled: 'DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION'. That study is the logical continuation of the study[4] published by STOA in September 1998 entitled: 'AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL' drawn up by the Manchester-based OMEGA Foundation. That document deals with the specific issue of electronic surveillance and, hence, refers to recent developments in that area, summarising trends in current legislation in Europe and in third countries. It also outlines a series of options such as the commissioning of a more detailed study into the social, political, commercial and constitutional implications of the global electronic surveillance networks to which it refers with a view to the organisation of a hearing of experts designed to underpin the future European Union policy on civil liberties.

The four studies presented here fully comply with that request. This is a study concerning the impact of electronic surveillance in the European Union which will enable the institutions and, in particular, Members of the European Parliament to understand and comprehend the current state of the equipment used in and the use made of electronic surveillance so that they will have all the information they need to put in place legislation which will provide enhanced respect for the confidentiality of communications and also eliminate as far as possible the economic risks which may arise from such interceptions and from free competition.

1. Study One: The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition[5]

This study, drawn up by Duncan Campbell[6] for the European Parliament's Directorate-General for Research (more specifically for STOA), summarises the current state of electronic surveillance via Communications Intelligence (COMINT), i.e. the automated search for electronic communications which makes the global interception of such communications possible. It is defined by the NSA as an industrial activity which makes it possible for all foreign communications to be intercepted[7].

The author refers to the new technologies used and explains how they operate. In order to enhance our understanding of those systems, he draws the reader's attention to the targets of global interceptions. These new systems facilitate mass surveillance of all telecommunications. Without encoding, modern means of communication have no defence against the high-tech interception equipment which may be used, for example, to tap telephones. This study therefore shows that, since the inception of communications intelligence, the production of interception equipment[8] has mushroomed, and the equipment itself has become increasingly sophisticated (the funds invested, EUR 15-20 billion, are proportional to the ends sought).

---

[3] In July 1999, the name of the committee was changed to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs.
[4] The STOA project entitled: 'AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL' was the subject of an interim study drawn up by OMEGA (PE 166.499).
[5] STOA PE 168.184, Vol. 4/4, April 1999.
[6] Duncan CAMPBELL, IPTV Ltd., Edinburgh. *mailto :iptv@cw.com.net.*
[7] NSA = National Security Agency. That definition was given at the meeting of the US National Security Council of 17 February 1972 in Intelligence Directive No 6.
[8] See study, pp. 3-13.

Communications intelligence is a large-scale industrial activity used by most nations. However, the principal user is *UKUSA*[9], an association of English-speaking nations. The study also provides new information about the *ECHELON* system[10], which forms part of the Anglo-American network and provides world-wide surveillance. Unlike many other systems, it is designed primarily for use against non-military targets. It operates by intercepting very large quantities of information and then syphoning out what is valuable, using artificial intelligence aids.

Once these organisations had been set up, the various countries involved in them needed to take certain steps to regulate and monitor them. This study summarises the background to the various laws adopted and demonstrates clearly the predominance of the United States which, early on, under pressure from the FBI, convened a meeting of states[11] to discuss together the various ways in which activities might be regulated. The study sets out the position taken by the United States. The author feels that that position does not promote confidentiality and, hence, privacy. Indeed, the policy pursued by the *NSA* (National Security Agency) seems rather inclined to require anything which might facilitate interceptions. The Agency justifies its stance by quoting aims such as combating crime and terrorism, and it puts its views across to the other countries involved in an attempt to persuade them to pursue the same policy. The study also outlines the reaction of the European Union and of the *OECD* countries. As far as the Union is concerned, that reaction may best be summed up in a Council resolution adopted in January 1995 which broadly follows the American view (although some Member States have actually succeeded in resisting).

The question remains as to why the American interest is so great. The author's reply is connected quite simply with the *ECHELON* system which enables the countries using it to obtain significant economic information and, hence, to secure a leading position on the commercial markets. That has an impact which is more than negligible. The study quotes examples where American companies have secured contracts as a result of communications having been intercepted. Should we assume that the end justifies the means when it comes down to beating the competition?

The new technologies developed at the end of this century have therefore enabled *COMINT* to build up enormous interception capabilities. However, when the year 2000 arrives, all that will change radically, since technological progress and changes in attitude will enable encryption and cryptography to be properly integrated into telecommunications.

Nevertheless, measures must be taken by the European Union and, more specifically, by Parliament which has been excluded from the discussions about this issue for too long. The study puts forward a number of policy options which Parliament might pursue and which would enable the European Union to free itself from the influence of the United States.

Respect for confidentiality of communications is, therefore, far from being total. That gives rise to serious inequalities in the economic sphere between the countries which are more committed and those which are less committed to that principle in their national legislation. If they comply with that legislation, they may well find themselves sidelined, when contracts are being concluded, by countries which use communications intelligence. The problem might be resolved by the general introduction of encryption and cryptography. The second study deals with that subject and provides us with a useful insight into those systems.

2. Study Two: Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues[12]

[9] UKUSA dates back to the 1947 agreement between the United Kingdom and the United States on electronic interceptions. The nations in the UKUSA alliance are the United States, the United Kingdom, Canada, Australia and New Zealand.

[10] The ECHELON system was set up in the 1970s. It expanded considerably between 1975 and 1995.

[11] These meetings are called ILETS: International Law Enforcement Telecommunications Seminars. They were initiated and founded by the FBI in 1993.

[12] STOA PE 168.184, Vol. 3/4, April 1999.

The aim of this study is to illustrate the main techniques that may be used for protection against all forms of technological interception of communications. It was drawn up by Dr Franck Leprevost[13].

This study lists the various types of telecommunications equipment that have been produced and the risks inherent therein[14]. It then outlines cryptographic and encryption techniques, since electronic surveillance, which is frequently used for the protection of national security, may also be misused, for industrial espionage, for example. The author therefore highlights the various means (encryption, cryptography) by which the security of communications may be guaranteed and also outlines the consequences of cryptanalysis, which is the perfection of techniques or attacks to reduce the theoretical security of cryptographic algorithms, and quantum cryptanalysis, which is the set of the techniques whereby the secret keys of cryptographic protocols can be found by means of quantum computers. It is, therefore, true to say that respect for the confidentiality of communications and secrecy in correspondence may be protected. However, there is no such thing as blanket protection.

The problem of the interception of communications is always present, even if the sender uses the most sophisticated encoding methods. What is more, the European institutions, hot on the heels of the United States, are working to perfect a quantum coprocessor which would make public-key cryptography (a term which is defined and explained in the study) obsolete.

According to the author, therefore, the European Union is, on the one hand, promoting fundamental rights and, on the other, working to some extent to deny them.

The political, diplomatic and financial consequences of cryptanalysis and quantum cryptography may be very significant. That is why the various countries have signed several agreements to regulate these procedures. The most recent agreement of this kind is the WASSENAAR Arrangement[15]. Dr Leprevost's study discusses the part thereof entitled '*INFORMATION SECURITY'* and highlights its consequences.

The WASSENAAR Arrangement[16] establishes an international system for controlling the export of conventional weapons and dual-use equipment and technologies and lists the articles involved. Cryptography is included in that list. This Arrangement replaces COCOM. It controls the export of encryption products on the grounds that they constitute dual-use goods, i.e. goods which have both civil and military applications.
However, the Arrangement also stipulates that products clearly identified and sold for civil or commercial purposes may not be subject to restrictions or control. In actual fact, only technologies providing a very limited degree of security are authorised for uncontrolled export. That has specific implications, especially at Community level. This study describes those technologies and subsequently suggests possible measures which the European institutions might implement in order to put in place legislation which provides enhanced respect for privacy, since commercial undertakings, authorities and individuals using a cryptosystem complying with the lawful criteria may well find their communications intercepted and decoded by the ECHELON network. 'Lawful' cryptography offers no real protection against global interceptions of communications.

It is, therefore, clear that, far from limiting crime and terrorism, further restrictions on cryptography will simply create an environment where the individual will not be protected against 'information terrorism and cyber-criminal activities', i.e. one where crime may prosper with impunity, since no information will enjoy genuine protection and, hence, genuine confidentiality.

[13] Dr Leprevost teaches at the Technical University of Berlin (TUB).
[14] See pages 2 and 3 of the study.
[15] The WASSENAAR Arrangement was signed on 19 December 1995 by 33 countries, including most European countries, together with AUSTRALIA, CANADA, the UNITED STATES, JAPAN and NEW ZEALAND.
[16] See: http://www.wassenaar.org/

Although major progress remains to be made in the use of cryptography and encryption, all the countries of the European Union have adopted legislation governing lawful interceptions. Such interceptions are closely monitored and tightly controlled, as we shall see from Study Three, which will also enable us to decide whether or not such legislation is or is not compatible with the relevant international conventions.

Study Three: The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law[17]

This study was drawn up by Professor Chris Elliott, a barrister and an engineer specialising in telecommunications, and reviews the various existing policies concerning the lawful interception of communications.

He lists the various international agreements concerning human rights and the protection of privacy and highlights the possible loopholes for legislation which might adversely affect those rights. For example, the Universal Declaration of Human Rights[18] does not lay down that all lawful interceptions are prohibited, only those deemed to be arbitrary. Accordingly, the European Union has put in place legislation[19] enabling the Member States to legalise the interception of some communications. The Union is not violating the rights set out in the international conventions it has ratified by not prohibiting lawful and non-arbitrary interceptions, since those conventions do not themselves prohibit them.

The various Member States have each adopted legislation governing lawful interceptions which must comply with secondary Community law. Such laws are broadly similar. This study sets out briefly the current national legislation governing this issue, thereby providing the reader with an overview of the principal provisions thereof. However, in order to ascertain whether or not the Member States are genuinely singing from the same hymn sheet as the Union, we need to review the case-law of the Community authorities (see Part Two below).

Conventions relating to human rights (especially the ECHR) provide effective protection against the unlawful interception of communications. However, that protection is less apparent in the case of lawful interceptions, especially if they are made by foreign powers (i.e. if the interceptor is a country other than the country of the sender). Some countries are even able to intercept communications inside another country. Measures must be taken to restrict such interception, and the European Union is in a position to ensure greater protection of privacy without breaching national laws currently in force, for example by requiring network operators to protect the privacy of communications by using encryption. Professor Elliott makes a number of observations and gives a few examples which the Union should follow with a view to enhancing respect for privacy and for correspondence.

This study therefore gives us a useful summary of current legislation governing the lawful interception of communications.

4. Study Four: The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception[20]

[17] STOA PE 168.184, Vol. 2/4, April 1999.

[18] The Universal Declaration of Human Rights was adopted by the UN General Assembly in the form of a resolution on 10 December 1948.

[19] European Union legislation: Council Resolution of 17 January 1995 (OJ C 329, 4.11.1996).
Directive 95/46/EC
Directive 97/66/EC.

[20] This document highlights the analytical findings of the study: PE 168.184/Int.St./Vol. 1/4.

This study of the development of electronic surveillance, which was completed in June 1999, was carried out, in response to a request from STOA, by the Patras-based ZEUS Agency (an EEIG), under the supervision of Mr Nikos BOGONIKOLOS. Its aim was to review the use of lawful interceptions of communications and to highlight the possible risks inherent therein, with particular regard to electronic commerce.

The study is divided into three parts: Part A. Options; Part B. Arguments and Evidence (expert opinions); Part C. Technical File. The study is interesting because it is based on expert opinions: forty-nine specialists in the telecommunications and new technologies sector have contributed thereto.

Some policy options are proposed therein, such as the establishment of a global communications network and the possibility of defining the technical capabilities of providing anonymity which should be recommended. It was possible to adopt the latter following a review of the opinions of the experts among whom there is now general agreement that virtually all economic information is exchanged electronically. Efficiency requires consideration of electronic protection in the context of an international network, and it is essential to establish genuine confidence in communications carried by the new technologies. 90% of the experts take the view that, notwithstanding the various laws in force, unlawful activities continue to exist and that, since the development of the Internet, the increase in the number of transactions implies a need to define a stable framework for business. They also think that political and social policy decisions to ensure privacy should be drawn up.

The Technical File in this study gives an overview of electronic surveillance; in that section, the author defines some technical terms and explains how electronic surveillance works, such as global (i.e. international) interceptions authorised by *COMINT*, communications intelligence, which is a kind of industrial activity enabling communications to be intercepted. A non-exhaustive list of the organisations using such intelligence is highlighted in that section, the most important one being the association of English-speaking nations, *UKUSA*.

It is clear that the Internet and the other modern communications systems impinge more and more on our daily lives. But those systems are vulnerable since they fail to ensure genuine respect for confidentiality. What is more, over the same period, surveillance systems such as *CALEA* and *ECHELON* have been developed. They are defined in this study[21], which also explains how and why these systems are used.

It therefore appears that the nature of the information collected by interceptions does indeed have repercussions on the impact and on the purpose of such activities. Fewer problems arise if communications are intercepted with a view to protecting people, i.e. for national defence or to combat crime and terrorism. However, if the information collected is used solely for economic purposes, dangers may arise, such as the risk of such information being misused so as to ensure that specific companies secure commercial contracts (industrial espionage). The study gives examples of abuse which properly illustrate these dangers[22]. But technical progress does not go in one direction only (making interceptions increasingly easy); accordingly, new protection systems have been developed such as encryption and cryptography[23].

[21] See pages 11 and 12 of the study.
[22] See pages 13-15 of the study.
[23] Cf. STOA PE 168.184/Int.St./Vol. 3/4: Encryption and cryptosystems in electronic surveillance, 1999.

If we are to understand fully the entire issue of electronic surveillance, we must not forget to look at current legislation[24]. This study gives the background thereto. Europe is the first area where legislation to protect privacy has been enacted. In Europe, confidentiality is deemed to be a fundamental right. The same cannot be said for every country. In the United States, for example, such protection is restricted by conflicts of interests, especially economic interests. That country is trying to use its predominance (being the major world power) to impose its views on other countries: restrict encryption and cryptography, increase interception capacity, etc. That is what this study shows. However, the European Union has been able to push through a number of measures to provide better protection for confidentiality and, hence, of personal data.

This study therefore gives an overall view of the issue of electronic surveillance and helps us to understand the interest which certain countries might have in using these methods. Accordingly, lawful interceptions of communications exist. They are lawful since they are governed by national legislation.

That completes the presentation of the four studies. The original texts constitute Volumes 2-5 of this Briefing Note. However, it should be added that the information set out in the various studies, such as the issue of lawful interceptions and the way in which they are regulated in the Member States or the issue of cryptography, requires a more in-depth analysis relating to data protection and to human rights in the European Union. That is why we shall endeavour to supply new information, which will provide a better response to those issues, in Part Two of this study.

[24] See pages 16-21 of the study.

Part Two:

ANALYSES: DATA PROTECTION AND HUMAN RIGHTS IN THE EUROPEAN UNION AND THE ROLE OF THE EUROPEAN PARLIAMENT

INTRODUCTION:

The history of mankind is characterised by the various endeavours undertaken to ensure respect for human dignity. The concept of Human Rights was initiated and developed by thinkers from different religious and cultural backgrounds. Statesmen and lawyers have contributed greatly to the advancement of those rights and to the establishment of appropriate standards. Accordingly, individual rights have gradually become enshrined in the legislations of the various countries.

The matter which concerns us here – electronic surveillance – lies at the very heart of the human rights issue, since it involves respect for privacy, a fundamental right fully acknowledged today. The studies presented in Part One prompt a number of observations, with particular regard to human rights in Europe, interception of communications and current legislation, and encryption and cryptography.

1. Human rights and Europe:

We shall begin by outlining the general situation of human rights in the European Union and then go on to consider the issue more specifically in relation to one of the institutions, the European Parliament. We shall also highlight the importance attached to respect for privacy in the European Convention on Human Rights.

A. Human rights and the European Union:

Soon after the Council of Europe had been established in 1949, six of its founder members[25] decided to integrate their economies in two sectors: coal and steel[26]. That marked the birth of new common institutions. Relations between those countries underwent a radical change, and de facto solidarity between them was soon institutionalised. The 'law' was enshrined in the first treaty with the establishment of the European Court of Justice, but human rights in the broad sense of the term were not referred to in that treaty. Nor were they explicitly referred to in the Treaty of Rome[27] establishing the European Economic Community.

However, we must not forget that, in 1950, the old continent drew up the European Convention for the Protection of Human Rights and Fundamental Freedoms, which is the benchmark for such matters in Europe. At the same, a supervisory body was established: the European Court of Human Rights, which has its seat in Strasbourg and is responsible for ensuring compliance with the Convention. It must, however, be noted that the Community institutions are not under the direct jurisdiction of the Strasbourg Court.

[25] Belgium, France, the Federal Republic of Germany, Italy, Luxembourg and the Netherlands.
[26] The Treaty of Paris, signed on 18 April 1951, provided for such integration.
[27] The Treaty of Rome was signed on 25 March 1957.

Article 6 of the Treaty on European Union lays down for the first time ever the fundamental principles governing respect for human rights: *'The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.'* However, it was not until the Treaty of Amsterdam was signed[28] that, pursuant to Article 46 thereof, the jurisdiction of the Court of Justice of the European Communities was extended to cover the action of the institutions, the objective being to verify respect for fundamental human rights via the reference in Article 6 to the ECHR. A common system for the protection of fundamental rights has developed from that basis. The Community Court has codified the principles enshrined in the treaties and incorporated general principles of law, such as fundamental rights, in the Community's legal order.

Among the other aspects to be taken into account as regards human rights and the European Union, we should note that respect for fundamental rights is a precondition for the accession of new Member States: *'Any European State which respects the principles set out in Article 6(1) may apply to become a member of the Union'*[29]. Furthermore, provision is made for penalties to be imposed should a Member State not respect these principles. Should the Council determine the existence of a serious and persistent breach of fundamental rights by a Member State, it may, acting by unanimity on a proposal by one third of the Member States or by the Commission, and after obtaining the assent of Parliament, decide to suspend certain of the rights deriving from the Community treaties, including the voting rights of that Member State in the Council.

The promotion of human rights has, therefore, developed steadily ever since the European Communities were first established. The Community institutions have played a significant role in that process.

B. Human rights and the European Parliament:

The European Parliament has concerned itself with this issue ever since the 1960s. The issue has been the subject of several debates and of a large number of reports which have been followed by the adoption of resolutions. Since 1975, the Commission had been planning to draw up a catalogue of fundamental rights, one which would correspond more closely to the requirements of the Communities by including economic and social rights not set out in the European Convention (ECHR). The Joint Declaration of the European Parliament, the Council and Commission of 5 April 1977[30], based on the case-law of the Court of Justice, symbolised the commitment of those institutions to comply with the ECHR.

The Single European Act remained vague on the issue of fundamental rights, notwithstanding specific proposals submitted to the Luxembourg Conference by some Member States and by Parliament with a view to the adoption of a text proclaiming fundamental rights. The signatory states declared that they were *'determined to work together to promote democracy on the basis of the fundamental rights recognised in the constitutions and laws of the Member States and in the ECHR ... .'* Article 4 of Parliament's 1984 draft Treaty on European Union included a much more specific provision: *'The Union shall protect the dignity of the individual and grant every person coming within its jurisdiction the fundamental rights and freedoms ...'*. However, for lack of time, Parliament did not pursue the issue of a catalogue of human rights when adopting the draft Treaty.

[28] It was signed on 2 October 1997.
[29] Article 49 of the Treaty of Amsterdam.
[30] OJ C 103, 24.4.1977.

Parliament subsequently resumed its work on the basis of a motion for a resolution, tabled by Mr LUSTER and Mr PFENNIG, to supplement the draft Treaty establishing the European Union[31]. In 1988, the Committee on Institutional Affairs adopted a report on the Declaration of fundamental rights and freedoms of European citizens[32], and Parliament held a public hearing on human rights in the Union[33] in Florence. On 12 April 1989, it adopted a Declaration of fundamental rights and freedoms annexed to a resolution[34]. It called on the other institutions to associate themselves with the Declaration, which is in no way binding but which guarantees a series of civil and political rights.

Parliament is, therefore, very sensitive to the issue of human rights. It also acts as a driving force and has on several occasions secured positive results following condemnation of human rights violations. At each part-session, part of the parliamentary proceedings is devoted to the condemnation of instances of human rights violations throughout the world. Parliament has sought, and has obtained, a guarantee that, in the Union's relations with third countries, emphasis is placed on respect for human rights as a precondition for the granting of economic concessions.

However, Parliament does not simply highlight and condemn violations of fundamental rights, it also adopts an annual report on respect for human rights in the European Union[35]. In addition, it has set itself the target of funding human rights initiatives such as the *European Initiative for Democracy and the Protection of Human Rights.*

The European Parliament does not, therefore, hesitate to express its concern at the various breaches of the very values of the Union: human dignity, respect privacy and peaceful coexistence. Respect for privacy is therefore included in the protection that Europe offers for fundamental rights.

C. Respect for privacy in the European Convention on Human Rights:

Notwithstanding the best endeavours of those who drafted the ECHR, the Convention frequently seems to say very little about the protection of human rights, and it has needed to be interpreted and supplemented in a very positive fashion by the Commission and the Court of Justice. The simple phrase 'private and family life' in Article 8 of the ECHR, which entails a whole raft of implications, constitutes just one example thereof.

Right to respect for private and family life, home and correspondence is therefore subject to protection on a fairly wide scale. Interpreting the Convention as a 'living' instrument, one to be adapted to meet the requirements of modern society, the Court of Justice and Commission have analysed those concepts in the light of changes in manners and attitudes and the development of science and technology. Nevertheless, this broad power of interpretation is not unlimited.

The scope of the protection provided for in Article 8 has also been extended on the basis of the very frequent appeals made in this field to the positive obligations of the signatory states. Since the Convention is designed to protect specific, actual rights, it sometimes requires the signatory states to take positive and proactive measures.

This development demonstrates the increasing significance of human rights in every aspect of Community action. Although the initial Community acts contained no references to this issue, respect for fundamental rights rapidly became the main theme for both European integration and the affirmation of the European identity. Respect for privacy and, consequently, the secrecy of correspondence constitute an integral part of human rights. They are therefore protected in Europe, particularly against electronic surveillance, which is subject to legislation.

---

[31] B2-0363/84.
[32] PE 115.274/fin.
[33] PE 124.155.
[34] Resolution of 12 April 1989, OJ C 120, 16.5.1989, p. 51.
[35] The most recent report was drawn up by Mr BARROS MOURA and published on 6 November 1998.

2. Electronic surveillance and legislation:

Surveillance technology may be defined as devices or systems which can monitor, track and assess the movement of individuals, their property and other assets. In the 1980s, new forms of electronic surveillance were developed which have resulted in electronic interceptions being processed by computer. If we are to gain a complete insight into this matter, we must begin by looking at lawful interceptions before going on to consider more specifically global interceptions of communications and the risks inherent therein.

A. Lawful interceptions:

Respect for the secrecy of correspondence must be reconciled with other equally important principles such as law and order and national security. Accordingly, some violations of those rights are authorised, but only for specific purposes and provided that they are themselves lawful.

1. Community legislation and the position of the European Parliament:

Lawful interceptions of communications violate respect for privacy and may result in the storage of the data intercepted.

It would, therefore, be appropriate to review the legislation governing the protection of personal data in the telecommunications sector, since such legislation covers part of the activity under consideration, namely electronic surveillance, before looking in greater detail at the current legislation governing the lawful interception of telecommunications.

- Protection of personal data in the field of telecommunications:

The Data Protection Convention referred to in the Introduction, which was signed on 21 January 1981, concerns the protection of individuals with regard to data processing. It lays down principles for the protection of privacy, but those are merely general principles which are not binding. For that reason, secondary law has been used.

On 25 October 1995, the European Parliament and the Council adopted Directive 95/46/EC[36] on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The basis for the Directive was a Commission proposal[37] which sought the harmonisation of the provisions required to ensure an equal level of protection of privacy in the Member States and to provide for the free movement of telecommunications equipment and services in the Community. That proposal was drawn up in the light of the opinion of the Economic and Social Committee of 3 April 1991[38].

The Directive points out that 'data-processing systems are designed to serve man and must respect the fundamental freedoms and rights of [natural] persons …'. Accordingly, Article 1 of the Directive requires the Member States to 'protect the fundamental freedoms and rights of natural persons, and in particular their right to privacy with respect to the processing of personal data.' Article 29 of the Directive provides for the setting up of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The working party is required to draw up and submit to the Commission, the European Parliament and the Council an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries.

---

[36] OJ L 281, 23.11.1995, p. 31.
[37] Submitted on 14 June 1994, OJ C 200, 22.7.1994, p. 4.
[38] OJ C 159, 17.6.1991, p. 38.

On 25 June 1997, the Working Party on the Protection of Individuals adopted an initial report which covered the major developments noted in 1996 in this field. A second report, dated 30 November 1998, largely followed the structure of the earlier report and outlined the progress recorded in the European Union in this field.

A start was made in 1996 on implementing this Directive in the Member States and at European Union level. The European institutions, and the Commission in particular, habitually process personal data in the course of their activities. On the date when the Directive was adopted, the Commission and Council made a public declaration[39] in which they undertook to respect the provisions of the Directive and called on the other Community institutions and bodies to do likewise.

Although the Directive is the key element in European data-protection policy, it is supplemented by a number of other initiatives designed to ensure that individuals enjoy a consistent framework of protection.

On 15 December 1997, on the basis of the common position adopted by the Council of Ministers on 12 September 1996, which subsequently became subject to the conciliation procedure, the European Parliament and the Council adopted a Directive[40] concerning the processing of personal data and the protection of privacy in the telecommunications sector.

The aim of that Directive is to guarantee the free movement of such data and of telecommunications equipment and services in the Community by harmonising the level of data protection for subscribers to and users of public telecommunications services with regard to the processing of personal data in the telecommunications sector. The Directive spells out in detail for the telecommunications sector the general rules set out in Directive 95/46/EC and enhances protection of the privacy and the legitimate interests of subscribers.

Accordingly, that Directive is closely connected with the general Directive on data protection (adopted on 24 October 1995) since it spells out in detail the general rules already laid down in the first Directive. However, its scope is much wider: it covers the rights and legitimate interests of individuals and embraces aspects of privacy which are not directly connected with data protection. The Directive includes provisions relating to: security of information transmitted along public telecommunications networks; confidentiality of the information transmitted; limits and duration of data processing as regards billing; identification of malicious calls; protection of privacy as regards unsolicited calls.

Note: The Council of Europe has continued with its regular work on data protection issues. The Committee of Ministers has adopted two Recommendations, R(97)5 on 13 February 1997 and R(97)18 on 30 September 1997.

Following discussions, the Working Party on the Protection of Individuals adopted a number of documents, including Recommendation 1/97 on data protection and the media[41], Opinion 1/97 on the Canadian initiative regarding standardisation with regard to the protection of privacy[42] and Recommendation 3/97 concerning anonymity on the Internet[43].

Protection of personal data is therefore strictly governed by the two Directives referred to above. What is more, the Treaty of Amsterdam covers this issue by incorporating a specific provision on the protection of personal data.

[39] This declaration was published on 24 July 1995, 9012/95 (Press 226).
[40] Directive 97/66/EC, OJ L 24, 30.1.1998.
[41] Document WP1 – 5012/97.
[42] WP2 – 5023/97.
[43] WP2 – 5057/97.

It is clear that the Directive which is of most interest to us is Directive 97/66/EC, adopted on 15 December 1997, since it concerns 'the processing of personal data and the protection of privacy in the telecommunications sector.' Article 5 thereof specifically deals with the issue of the confidentiality of the communications: *'Member States shall ensure via national regulations the confidentiality of communications .... In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, without the consent of the users concerned, except when legally authorised ....'*

Pursuant to that Directive, then, the right to respect for privacy may therefore be attained by the lawful interception of communications. We must therefore study the relevant legislation.

- Lawful interception of telecommunications:

European legislation concerning lawful interceptions is less binding and extensive than that governing the storage of personal data. To date, the European institutions have contented themselves with resolutions in this area, i.e. acts which do not provide for any procedure that is binding in law and which simply set out the political will of the Member States and merely indicate the way in which their actions should be targeted. What is more, not many resolutions on this matter have been adopted. The Council has adopted just one, on 17 January 1995, and it was not until 1998 that a new draft was adopted. It should be noted that the legislation must keep pace with the progress made in the field of electronic surveillance, since today, for example, the use of miniature microphones to intercept telecommunications is outmoded. *Modern-day spies* can purchase laptop computers which may be tuned in to all the mobile phones active in the area simply by cursoring down to their number.

The issue seems to be one of ascertaining whether or not the position taken by the Council when adopting these resolutions will facilitate genuine respect for privacy. The resolution adopted on 17 January 1995[44] must be placed in context if it is to be properly understood.

In the European Union, because of international conventions and the ECHR, private individuals may not and must not be subject to unlawful interception of communications which concern their private life. However, most countries have their own laws concerning lawful interceptions. The United States, for example, has adopted legislation which provides limited protection of confidentiality, since the interests at stake are enormous, especially in the economic sphere. That is why the USA is behind an international campaign seeking an increase in interception capacities. In 1994, a law – CALEA - was adopted which requires the manufacturers of telecommunications equipment to incorporate therein devices designed to facilitate the interception of communications. But that was not enough for the USA, they wanted the Member States of the EU to incorporate CALEA in European legislation.

That is why the Council of Ministers, under pressure from the United States, adopted the resolution of 17 January 1995 which incorporates everything which the number one world power wanted to have incorporated. The resolution was not published until nearly two years after it had been adopted, and the Council did not seek Parliament's opinion. It provides for the drawing up of a list of requirements to be taken into account by the Member States when lawfully intercepting telecommunications. Those requirements are laid down in order to ensure a common technical level when telecommunications are intercepted. That will increase interception capacities. Comparable standards are imperative, partly because of the scale of the interceptions carried out in the fight against international organised crime, and partly because such standards would simplify interceptions carried out in response to letters rogatory issued by a magistrate. It is, of course, just as imperative for interceptions to be carried out for those purposes alone. In that way, it would be possible to reconcile fully respect for privacy with public security requirements.

Technical progress has resulted in new telecommunications technologies being put on the market. Accordingly, the 1995 resolution must be updated to take account of the state of the art.

---

[44] Council Resolution of 17 January 1995, OJ C 329, 4.11.1996, pp. 1-6.

That is why, working on the assumption of on-going progress in telecommunications technology, the Council adopted a draft resolution on 3 December 1998 which proposed that a series of measures be taken with a view to extending the provisions of its January 1995 resolution. That draft resolution therefore included an annex explaining the changes applicable to communications using the new technologies. It therefore seeks to amend the first resolution by adapting it to technological progress. By letter of 27 January 1999, the Council consulted Parliament on the draft pursuant to Article 39 of the Treaty on European Union. At the sitting of 12 April 1999, the President of Parliament announced that he had referred the draft to the Committee on Civil Liberties and Internal Affairs as the committee responsible and to the Committee on Legal Affairs and Citizens' Rights and the Committee on Economic and Monetary Affairs and Industrial Policy for their opinions.

The Committee on Civil Liberties and Internal Affairs delivered its report[45] on 23 April1999. The report includes the opinion[46] of the Committee on Legal Affairs and Citizens' Rights, adopted on 25 March 1999, which rejects the Council proposal on the grounds that it is imperfect and imprecise and that it might, consequently, adversely affect individuals' rights. However, the report actually approves the proposal subject to amendment and asks to be consulted again, should the Council intend to make substantial modifications thereto. Accordingly, when it adopted the report on 7 May 1999 by adopting the legislative resolution, Parliament approved the draft Council resolution but recalled the imperative need to ensure that personal data was protected. It therefore called on the Council to ascertain, by 1 July 2000, the extent to which the Member States had transposed that resolution and the 1995 resolution.

Neither the 1995 resolution, as we have seen, nor the one of which the draft was adopted in 1998, is legally binding on the Member States. There is, therefore, no European legislation regulating telephone tapping and, more generally, the lawful interception of communications. At national level, procedures have been laid down providing for telephones to be tapped by the police on the basis of authorisation from the relevant Minister or letters rogatory issued by a magistrate.

After that brief presentation of the legislation currently in force in the Community on the protection of personal data and lawful interceptions, let is look now at the way it is applied in the Member States.

[45] Rapporteur: G. SCHMID. PE 229.986/fin.
[46] Draftsman: Luigi A. FLORIO, PE 229.986/fin.

2. Application in the Member States:

- Application of the legislation governing data protection:

During 1997, progress was made in the transposition of the relevant Directives into the national laws of the Member States. The situation is as follows in the various Member States:

BELGIUM: The Law of 11 December 1998 transposing Directive 95/46/EC of the European Parliament and of the Council has been adopted.

DENMARK: A law adopted in June 1998 is similar to the Belgian law referred to above.

GREECE: The Greek Data Protection Act was ratified by the Hellenic Parliament on 26 March 1997 and published on 10 April 1997.

SPAIN: A Bill was debated by Parliament during the summer of 1998. Most of its provisions have already been transposed by the 'Organic Law' (Ley Organica) of 29 October 1992.

ITALY: The Personal Data Protection Act was adopted on 31 December 1996. The Italian Parliament authorised the government to legislate by way of regulation in order to amend and supplement it with a view to the transposition of the Directive. That was done on 6 October 1998.

AUSTRIA: The revised draft transposition of the Directive was adopted by the Austrian Parliament on 18 October 1998.

PORTUGAL: The Constitution was revised by means of a constitutional law of 20 September 1997 so that the Directive could be transposed. A Bill was submitted to the Portuguese Parliament on 2 April 1998 and adopted on 26 October 1998.

SWEDEN: The Data Protection Act was adopted by the Swedish Parliament on 16 April 1998. Additional regulatory measures were adopted in September 1998.

UNITED KINGDOM: A Data Protection Act transposing the Directive was adopted in July 1998.

The other Member States of the Union do not, as yet, have any information available about this legislation because they have not yet adopted personal data protection laws. For example, France has simply implemented a report submitted to the Prime Minister in March 1998, and the French authority responsible for data protection, *La commission nationale de l'informatique et des libertés* (National Data Processing and Freedoms Commission), will be consulted about the preliminary draft laws. Nor has Finland any relevant legislation as yet, since the measures required to apply the Directive, which will include amendments to the 1988 Data Protection Act, are still being drawn up.

As regards the Directive of 15 December 1997, the Member States had until 24 October 1998 to transpose it, save with regard to certain aspects concerning the confidentiality of communications for which the deadline was extended until 24 October 2000.

- The position of the Member States on the lawful interception of communications:

As we have already seen, there is no binding European legislation governing lawful interceptions, each Member State having its own relevant legislation, but it is true to say that the rules applicable in the Member States are broadly similar.

The European Court of Justice has no power of scrutiny since no issue concerning transposition arises. However, such legislation is not totally exempt from verification. Each Member State must have ratified the ECHR, so legislation on lawful interceptions is subject to monitoring under that Convention by the legal body created for that purpose, the European Court of Human Rights.

National legislation must, therefore, be in conformity with the Convention and, consequently, not contradict the principles set out therein, such as respect for privacy, family life and correspondence (Article 8). Should it do so, the Court will rule against the Member State involved.

The Court's case-law shows that fundamental rights have not always been respected when telecommunications have been lawfully intercepted. For example, on 2 August 1984, the Court found against the United Kingdom in the MALONE case on the grounds that Article 8 of the ECHR had been breached by the (lawful) interception of communications. The Court found that, while legislation authorising the interception of communications in order to assist the Criminal Investigation Department in the performance of its duties might be necessary for the prevention of disorder and crime, the surveillance system adopted must include adequate guarantees against abuse. The British legislation did not meet that criterion.

Monitoring is, therefore, necessary and effective since, as we shall see, once the Court has ruled against them, the various countries which have found themselves in the dock have amended their legislation with a view to respecting human rights and, more particularly, to respecting the confidentiality of correspondence. The European Court of Human Rights found, for example, against France. As a result, France subsequently brought its legislation into line with the ECHR.

As regards telephone tapping, the Court's case-law had a significant and direct impact on French national law. In two rulings handed down on 24 April 1990 in the KRUSLIN and HUVIG cases, the European Court of Human Rights largely confirmed the findings of the MALONE case. The Court held that the guarantees given to the person whose telephone was being tapped on the instructions of the examining magistrate were imprecise or inadequate. Given the seriousness of the violation of privacy resulting from telephones being tapped without the knowledge of the users of the telephone, the legislator must lay down detailed and precise rules to govern such eavesdropping. The Court therefore found that Article 8 of the ECHR had been breached. The law must be sound. Accordingly, the French legislative body drew up a new law, dated 10 July 1991, which governs interceptions of communications while attempting to maintain a balance between the requirements of national security and respect for the secrecy of telephone conversations.

Those are the rulings of principle handed down by the Strasbourg Court. Relevant case-law is so extensive that it would be impossible to give an exhaustive list within the confines of this Briefing Note. There have been some recent rulings in this field, and new cases will no doubt crop up, especially when we take account of the new equipment for intercepting communications that has become available. The law will have to be adapted to incorporate provisions relating to the new methods of telephone tapping. A whole series of tapping devices has been developed with a view to recording communications and intercepting telecommunications. However, the scale of the tapping of communications carried out by judicial and administrative authorities, i.e. that subject to the legislation reviewed above, is minimal when compared with government interceptions at national and international level.

B. Global interceptions:

In order to provide a true understanding of what is meant by the term 'global interception', we shall describe it briefly and then consider the risks that may arise and the existing legislation in this field. All the information set out here has been taken from the various studies presented in Part One and from the STOA study entitled: 'An Appraisal of Technologies of Political Control'[47].

1. Description:

Global surveillance systems facilitate mass surveillance of all telecommunications, including telephone, fax and e-mail, of private individuals, politicians, trade unionists and private companies.

Global interceptions are possible thanks to *COMINT,* communications intelligence, an industrial activity enabling all foreign communications to be intercepted. Used principally for military purposes, it was developed during the Cold War when espionage was the order of the day. Most developed countries use *COMINT* either on their own account or in partnership with other countries. The most significant organisation using *COMINT* is undoubtedly *UKUSA*, an association of English-speaking nations which uses a system called *ECHELON*. Today, that system is directed largely towards non-military targets. It operates by intercepting very large quantities of information and then syphoning out what is valuable, using artificial intelligence aids. Five nations share the results of the intelligence-gathering operation among themselves, the United States being the First Party under the *UKUSA* agreement, with the United Kingdom, Canada, New Zealand and Australia, the Second Parties, supplying information.

The National Security Agency (NSA) is the body which uses *ECHELON* in the United States. It is responsible for counter-espionage and for protecting government and military communications and is also active in research and development. It covers the entire spectrum of military and civil information technologies.

The *UKUSA* agreement dates from 1947. Its powers expanded during the 1970s and 1980s when the *ECHELON* network was set up. We might wonder about the role of the European Union in these systems. The Member States, which seem to find a cause for concern in the predominance of the English-speaking nations, i.e. those belonging to *UKUSA*, are not to be outdone. They seem to follow the position of the Union which is implementing an electronic surveillance project similar to *ECHELON.*

Politicians, police forces and customs services advocate the extension of their surveillance capacity on the grounds that it will help them in their fight against crime. The work is being carried out under the aegis of the Council of Ministers of the European Union and is notable for its lack of transparency.

Mr Glyn FORD, a British member of the European Parliament's Committee on Civil Liberties and Internal Affairs, has said that some elementary requirements must be respected. There must be some measure of control over what was subject to surveillance as well as parliamentary scrutiny at European and national level. There could be no objection of principle to the fact of telephone tapping, but combating terrorism and money-laundering networks must not serve as a pretext for eavesdropping on Amnesty International, for example, or for economic espionage[48].

We must add that, as a result of the technical modifications made to telecommunications networks, there is a worrying grey area as regards the monitoring of telephone tapping and protection under the law which should ensure that respect for privacy, a fundamental right, could be safeguarded.

[47] PE 166.499/Int.St./Exec.Summ./en. 14 September 1998.
[48] Le Monde diplomatique, March 1999.

Global interceptions which result in the securing of information about terrorist or criminal organisations do not really pose a problem. It is where information gathered is used for different ends, to gain an economic advantage for example, that questions arise.

2. Possible risks:

No one can deny the role played by these networks in combating terrorism, drug trafficking, money-laundering and illicit arms dealing, but the scale of the foreign communications interception network is such as to arouse concerns with regard to the legislation governing systems for protecting data and privacy currently in force in the Member States. Such legislation is supposed to protect confidentiality among the individuals and commercial undertakings in the Union and in third countries. Furthermore, economic risks, i.e. misuse of information for commercial ends, may arise if this type of interception is used.

Some journalists have not hesitated in affirming that *ECHELON* has been used to benefit American companies involved in arms contracts and to strengthen Washington's hand in major negotiations with Europe in the World Trade Organisation in relation to disputes with Japan concerning the export of motor vehicle spare parts. If those examples should prove to be true, the risks arising might be very significant and result in European Union undertakings losing a large number of contracts.

One of the studies presented in Part One[49] gives some examples of the misuse of economic information intercepted by global networks such as *ECHELON.* We can actually quote the contract which was 'spirited away' from France in January 1994. It involved an arms supply contract worth 30 million francs with Saudi Arabia. The contract ended up with McDonnell-Douglas, the rival of the Airbus consortium, because the former was privy to the financial terms offered by Airbus thanks to the electronic interception system.

Then the 'Sunday Times'[50] reported that the French electronics giant, Thomson, had lost a contract worth 1.4 million dollars for the supply of a surveillance system to Brazil because the Americans had intercepted details of the negotiations and passed them on to the US Raytheon Corporation, which subsequently won the contract.

Europeans may be paralysed when confronted by a system of this nature. But, in the absence of any proof that *ECHELON* has been used for economic espionage, nobody wants to jeopardise 'good trade relations with America'[51].

3. The attitude of the European Union and of Parliament to global interception networks (and, hence, to transatlantic relations):

Although Europe is pretending to become concerned about electronic espionage carried out world wide by the Americans, its police forces are themselves drawing up, in conditions of the utmost secrecy, a project for telephone and Internet surveillance[52].

In January 1997, Statewatch, an organisation devoted to the monitoring of and research into public freedoms based in the United Kingdom, reported that the European Union had secretly agreed to set up an international telephone tapping network via a secret network of committees established under the third pillar of the Treaty of Maastricht which covers cooperation on law and order. The key points of that plan are outlined in a Memorandum of Understanding signed by the Member States of the Union in 1995[53] without any prior Council meeting.

---

[49] The draft final study, June 1999.
[50] Edition of 11 May 1998.
[51] Le Monde diplomatique, March 1999: American 'Big Ears', by Philippe Rivière.
[52] Le Monde diplomatique, March 1999. All Europe is listening, by Philippe Rivière.
[53] ENFOPOL 112 10037/95, 25.10.95.

On the basis of that information, which was also highlighted by the STOA study entitled: 'An Appraisal of Technologies of Political Control'[54], a debate began in Parliament. Accordingly, several Members tabled questions to the Commission and Council about *ECHELON* and global surveillance systems.

Those questions led to the adoption of a resolution. They are based on the various documents already referred to, such as the various STOA studies. The Commission seems to have taken rather a bizarre stance on this issue: on the one hand, it roundly condemns any infringement of privacy though the interception of communications, while on the other, it says that it has no powers to initiate a programme which would prevent Member States from spying on each other[55]. Nor does the Commission have anything to say about whether any measures will be taken against the countries belong to the *UKUSA* alliance. It simply notes that it 'condemns any and all threats to the integrity of classified information held by the institutions'[56].

We must, however, add that the Commission advocates the liberalisation of encryption in order to protect the confidentiality of communications (see above). As for the Council, a question about the *ECHELON* system was tabled to it on 8 June 1998[57]. It has not yet answered the question, so its position remains vague. However, we do know that it has decided to set up a similar surveillance system under the third pillar.

On 16 September 1998, after several Members had tabled motions for resolutions, Parliament adopted a resolution[58] on transatlantic relations/*ECHELON* system. In that resolution, it recognised the need for electronic surveillance systems but emphasised that democratic accountability was essential and called for greater protection to be provided, with a code of conduct being adopted and the issue being discussed in national parliaments and in the European Parliament. It also emphasised the importance of relations between the United States and the European Union but called for greater transparency and for greater European Parliament involvement in those relations, given that all the decisions relating thereto are taken by the Commission and Council. (The full text of that resolution is annexed to this document).

As we have seen, interception of communications and electronic surveillance therefore give rise to threats to fundamental rights, especially the right to privacy. Nowadays, however, techniques exist which enable confidentiality to be maintained, such as cryptography and encryption, but their implementation is to some extent impeded.

[54] PE 166.499, September 1998.
[55] Written Question E-1040/98 to the Commission, 6 April 1998.
[56] Written Question E-1039/98 to the Commission, 29 April 1998.
[57] Written Question E-1775/98.
[58] Resolution B4-0803/98 of 16 September 1998, OJ C 313, 12.10.1998, p. 98.

3. Cryptography and encryption: the key to the problem?

A. Presentation and problem areas:

'Although it is very difficult to quantify the losses caused by industrial espionage, … the losses incurred by European firms can reasonably be put at several billion euros per year.'[59].

Encryption is a method of combating this type of espionage: it involves a process of converting information that is immediately understandable into information that is unintelligible by the use of secret conventions, the effect of which are reversible. There are two types of cryptography, symmetrical and asymmetrical cryptography. Cryptography is, therefore, the study of techniques designed to ensure confidentiality. In a society where the exchange of information by digital means is developing, we need to have secure systems to protect personal or confidential data, to protect financial or commercial transactions and to conclude contracts without using hard copy. Nowadays, cryptographic technologies are acknowledged as essential tools for security and confidence in electronic communications.

However, if messages and files are encrypted with powerful systems, the content of the communications becomes indecipherable for everybody, including governments. But governments and judicial authorities want to be able to intercept communications and access the content of files in instances authorised by the law in their campaign against crime and to guarantee national security What is more, the security of electronic communications may be guaranteed only by means of strong encryption, and the development of electronic commerce, which is international by its very nature, presupposes the possibility of being able to import and export encrypted data without any restriction whatsoever. However, those requirements run up against various restrictions on the export of encryption products. Encryption products are actually deemed to be 'sensitive' products or 'dual-use' goods (i.e. ones which may be used for either civil or military purposes).

That is why, for various reasons, encryption is subject to very stringent legislation which varies from Member State to Member State. The European Union's position on the issue is very interesting but is not accepted by all the Member States.

B. The position of the European Union:

A Council Regulation of 19 December 1994[60] sets up a regime for the control of exports of dual-use goods in order to establish Community standards in connection with the completion of the internal market. Pursuant to Article 19 of that Regulation, the Member States are required to implement, for a transitional period, a procedure for authorising intra-Community trade in certain sensitive products, by way of derogation from the principle of the free movement of goods. At present, this provision also applies to encryption products. Accordingly, the Member States are required by this Regulation to impose not only controls on the export of dual-use goods but also intra-Community controls on encryption products transferred from one Member State to another.

However, the principal objective of the Regulation is to establish a harmonised procedure for controlling exports to countries outside the Union. The products covered by the Regulation are listed in an annex. With regard to cryptography, telecommunications equipment, high-tech computer software and hardware and products providing security of information are covered. Nevertheless, the software habitually available to the general public is not subject to such controls. The Regulation is currently being revised by the Community institutions. The transitional period was due to end on 1 July 1998. As from that date, exports of encryption products within the European Union should no longer have been subject to any controls.

---

[59] 'ENCRYPTION AND CRYPTOSYSTEMS IN ELECTRONIC SURVEILLANCE' – STOA, PE 168.184, Vol. 3/4.
[60] Council Regulation (EC) No 3381/94.

An international agreement with the same objectives, the WASSENAAR Arrangement, was signed two years later. It was adopted on 11 and 12 July 1996 by 33 countries, including most European countries, to replace COCOM. It controls the export of encryption products, deeming them to be dual-use goods, although it advocates exemption from those controls for software available to the general public.

However, Community legislation did not stop there. Some further measures have been taken by the institutions. On 15 May 1998, the Commission presented a report summarising the application of the Regulation referred to above together with a proposal for a regulation[61] which seeks to remedy the apparent deficiencies of that Regulation.

The regime established in 1994 led to a reduction in export formalities and facilitated the free movement of virtually all dual-use goods in the Community. However, the regime is not watertight as regards the common export control regime. There is no consistency between the various national policies and practices (see the example of France set out below). The Member States have not been able to reach agreement on export policies based on authorisations.

The proposal for a regulation tries to resolve these problems with a view to facilitating and simplifying the export of dual-use goods. It proposes that uniform national forms should be introduced for export authorisations. The Member States would still retain the right to grant an export licence in respect of a specific product, even if another Member State had refused authorisation, but the Member State which decided to grant the export licence would have to justify its decision and consult the other Member State before it did so. The Commission aims to make the regime more flexible and reconcile the wishes of the Member States by informing them and giving them the opportunity of monitoring and controlling exports. As regards encryption products, the proposal would abolish existing restrictions on intra-Community transfers and replace them by a notification procedure.

This proposal for a regulation is part of an overall framework for a Community policy. The Union has set itself the objective of developing, by 2000, a policy for the free movement of encryption products and services. That policy also includes the proposal for a directive on a common framework for electronic signatures[62] which provides for a clear-cut distinction between cryptography used for authentication and cryptography used to ensure the confidentiality of data. The proposal was approved by the European Parliament, subject to the amendments it had made thereto, when it adopted, on 13 January 1999, a legislative resolution[63] contained in a report by the Committee on Legal Affairs and Citizens' Rights[64] dated 16 December 1998. Since Parliament had called for amendments to be made to the Commission proposal, an amended proposal for a European Parliament and Council directive[65] on a common framework for electronic signatures, submitted by the Commission in accordance with the EC Treaty, was adopted on 29April 1999.

In this instance, Parliament is involved in the implementation of Community legislation. However, it should become more involved and support liberalisation of the use of cryptography throughout the Community. That is the finding of the studies drawn up by STOA presented above.

Because of its implications for privacy and data protection, cryptography raises issues which challenge the choices which societies make. Since European legislation has not yet been harmonised, it sometimes differs from national legislation, as may be seen in the case of France.

C. Divergent opinion of one Member State: the case of France:

[61] COM(1998) 258 final.
[62] Submitted on 13 May 1998, see COM(1998) 297.
[63] COM(1998) 297, OJ C 104, 14.4.1999, p. 49.
[64] PE 228.030/fin.
[65] COM(1999) 195.

In a world where exchange of information by electronic means is rapidly developing, we need to have in place secure systems to protect data and ensure the security of financial and commercial transactions. Encryption is frequently the only effective way of meeting those requirements. Accordingly, cryptographic technologies are acknowledged as essential tools for security and confidence in electronic communications. The requirements of user confidentiality were emphasised by the Law of 26 July 1996[66] which refers to the protection of information and the development of secure communications and transactions. However, France, invoking the need to maintain the interests of national defence, has maintained restrictive legislation as regards cryptography. More than eighteen months after the adoption of the 1996 Law, decrees have been published which do not implement the liberalisation announced but demonstrate a hidebound attitude to security.

French legislation draws a distinction between the data authentication and integrity functions, which are subject to a more liberal regime, and confidentiality functions, on which the State intends to maintain a tight grip. However, in order to enable users to enjoy the benefits of cryptographic technology for the purpose of ensuring confidentiality, the law introduces a system known as 'trusted third parties'. Under that system, use of the confidentiality functions is free, provided that the secret codes are managed in accordance with specific procedures and by an approved body. The system exists solely in France, and it has given rise to a huge number of both legal and technical questions.

France is, therefore, the only country in the European Union which has adopted legislation restricting the free use of cryptography. Since the adoption of the Law of 29 December 1990, the most that France will tolerate is the encryption of the signature and of the certification of the integrity of the messages, subject to prior declaration made to a department of the Prime Minister, but does not authorise encryption of the message itself, which must be sent in plaintext (en clair)[67]. French legislation on encryption violates the principles of the free movement of goods, services and persons. It makes it impossible for Community citizens travelling in France to use encryption products authorised in their own countries. It also constitutes a barrier to the free movement of goods, since a product freely marketed in another country in the Union requires authorisation before it may be supplied in France.

French law therefore contradicts Community policy on several counts. The Community Directive on the processing of personal data[68] requires the Member States to protect the rights and freedoms of individuals. The regimes established in France for the use and supply of cryptographic services might adversely affect the application of the Directive because, according to the Commission, the appropriate means required to guarantee the security of personal data are apparently not available in France.

French legislation is clearly justified on grounds of national security and defence. Governments feel that excessive protection of information jeopardises their security and benefits organised crime. The legislation is, therefore, based on security considerations and takes insufficient account of requirements in the field of cryptography. It does not seem to fulfil the criterion of proportionality in European law.

---

[66] *Journal Officiel* dated 27 July 1996.
[67] 'Le Monde', edition of 15 May 1996, p. 14.
[68] Directive 95/46/EC of 24 October 1995, OJ L 281, 23.11.1995, p. 31.

There is also the prospect of further legislation being adopted, as Paul Vidonne wrote in an article which appeared in 'Le Monde' on 15 May 1996. An ex post control system would be much simpler and much less expensive. Freedom to encrypt, leaving it solely to the user's discretion to decide which method to use, would be offset by the obligation to notify systems and encryption keys at the request of any judicial authority. Explicit refusal to notify such information would be severely punished, as would the loss of or failure to remember keys, which would be construed as bad faith. Those countries which have put in place a control system of this nature are not plagued by individual crime involving communications. France may once again show that it is capable of introducing reforms which are liberal, economic and useful.

CONCLUSION

Electronic surveillance prompts a large number of questions and gives grounds for objections, since respect for fundamental rights has become the buzzword of modern society. The European Parliament will, therefore, have its work cut out if it takes up the cudgels to defend respect for confidentiality.

Guaranteeing the secrecy of correspondence amounts to respecting the privacy of users, and it will also create a more equable economic climate.

The role of the European Parliament is becoming more significant. Improved cooperation with the Commission is the order of the day because the new Members and the new President of the Commission, Romano Prodi, (approved by Parliament on 15 September 1999) have committed themselves thereto. Accordingly, Parliament might be able to impose its views, with particular regard to the subject of this Briefing Note, since, as we have seen, it has frequently been excluded in the past when decisions have been taken (such as the Council Resolution of 17 January 1995 on lawful interceptions).

This Briefing Note, which the Committee on Civil Liberties and Internal Affairs[69] asked STOA to draw up and which is presented here, sets out the various options open to Parliament in its endeavours to improve the legislation currently in force and establish genuine security of telecommunications.

[69] In July 1999, the name of that committee was changed to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs.

ANNEX:

DEFINITIONS:

* Confidentiality is the requirement of rendering information unintelligible for unauthorised third parties during conversations and, above, all, during information transfer. Encryption is the technique most widely used for this purpose.

* Respect for privacy; individual freedom is the protection of the individual's personal space as regards information, i.e. the right of the individual to control or significantly influence information which may be collected or stored.

* Cryptology is a series of techniques which enable information to be protected by means of a secret code. In particular, it involves the tools used to make such information secure against institutional threats. Such tools are generally the result of mathematical procedures which are very difficult to resolve for anyone not in possession of the code. It enables security to be provided with a view to protecting data or transactions in electronic form.

* Trusted third-parties are bodies which enjoy the trust of the user and carry out certain operations connected with the management of confidentiality keys on the user's behalf. A distinction must be drawn between third party custodian duties (keys held for confidentiality) and certification authority duties with regard to public keys used solely in applications connected with digital signatures.

* Digital signature is a technique which provides simultaneously for the integrity of data, authentication and non-repudiation.

RESOLUTION OF 16 SEPTEMBER 1998:

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,

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

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;

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.

BIBLIOGRAPHY:

International conventions and primary Community law

* The Universal Declaration of Human Rights, 10 December 1948
* The European Convention on Human Rights, 4 November 1950
* The Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981
* The WASSENAAR Arrangement of 19 December 1995

* The Treaty of Rome signed on 25 March 1957
* The Treaty of Amsterdam signed on 2 October 1997

Secondary Community law

* Joint Declaration by the European Parliament, the Council and the Commission of 5 April 1997 (OJ C 103, 24.7.1977)
* European Parliament motion for a resolution (B2-0363/84)
* Report by the Committee on Institutional Affairs on the Declaration of fundamental rights and freedoms (PE 115.274/fin.)
* European Parliament resolution of 12 April 1989 (OJ C 120, 12.5.1989, p. 51)
* Directive 95/46/EC
* Directive 97/66/EC
* Council Resolution of 17 January 1995 (OJ C 329, 4.11.1996, pp. 1-6)
* European Parliament report (PE 229.986/fin.)
* Resolution of 16 September 1998 (OJ C 313, 12.10.1998, p. 98)
* Regulation (EC) No 3381/94
* Proposal for a regulation (COM(98) 257 final)
* Amended proposal for a directive (COM(1999) 195 final)
* European Parliament report (PE 228.030/fin.)

Miscellaneous publications

* Le Monde diplomatique, March 1999
* Le Monde, edition of 15 May 1996, p. 14
* Cryptography, why should we fully liberalise the French legislation?, Valérie SEDALLIAN (**http://www.iris.sgdg.org/**)
* An Appraisal of Technologies of Political Control – STOA – PE 166.499, 14 September 1998 (accessible on STOA's web site – http://www.europarl.ep.ec)
* French legislation relating to cryptology (**http://www.internet.gouv.fr**)

Other documents

* Community law and the protection of fundamental rights in the Member States, Louis Dubouis, Economica, 1995
* Affirmation of fundamental rights in the European Union – European Commission, 1999
* The European aspect of fundamental rights, Gérard Cohen-Jonathan – preparation for CRFPA – Montchrétien, 1996
* Data processing and freedom, Henri Delahai, La Découverte, 1987

* Protection of privacy and other individual assets, François Rigaux, LGDJ, 1990
* Human rights: European legal landmarks, Council of Europe, January 1999
* Elaboration of a methodology for the assessment of the appropriateness of the protection of legal persons with regard to the processing of personal data, European Commission, 1998
* On-line services and the protection of data and privacy, European Commission, 1998 (Vol. 1)
* Case-law of the European Court of Human Rights, V. Berger, SIREY, 1994