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**<br>**1) Présentation des quatre études**<br>**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<br>Directorate General for Research<br>Directorate A<br>The STOA Programme |
| Author: | Peggy Becker - visiting researcher<br>Under the supervision of Dick Holdsworth<br>Head of the STOA Team |
| Editor: | Mr Dick HOLDSWORTH,<br>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

# DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

**Vol 2/5**

**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 targetting and selection, including speech recognition**

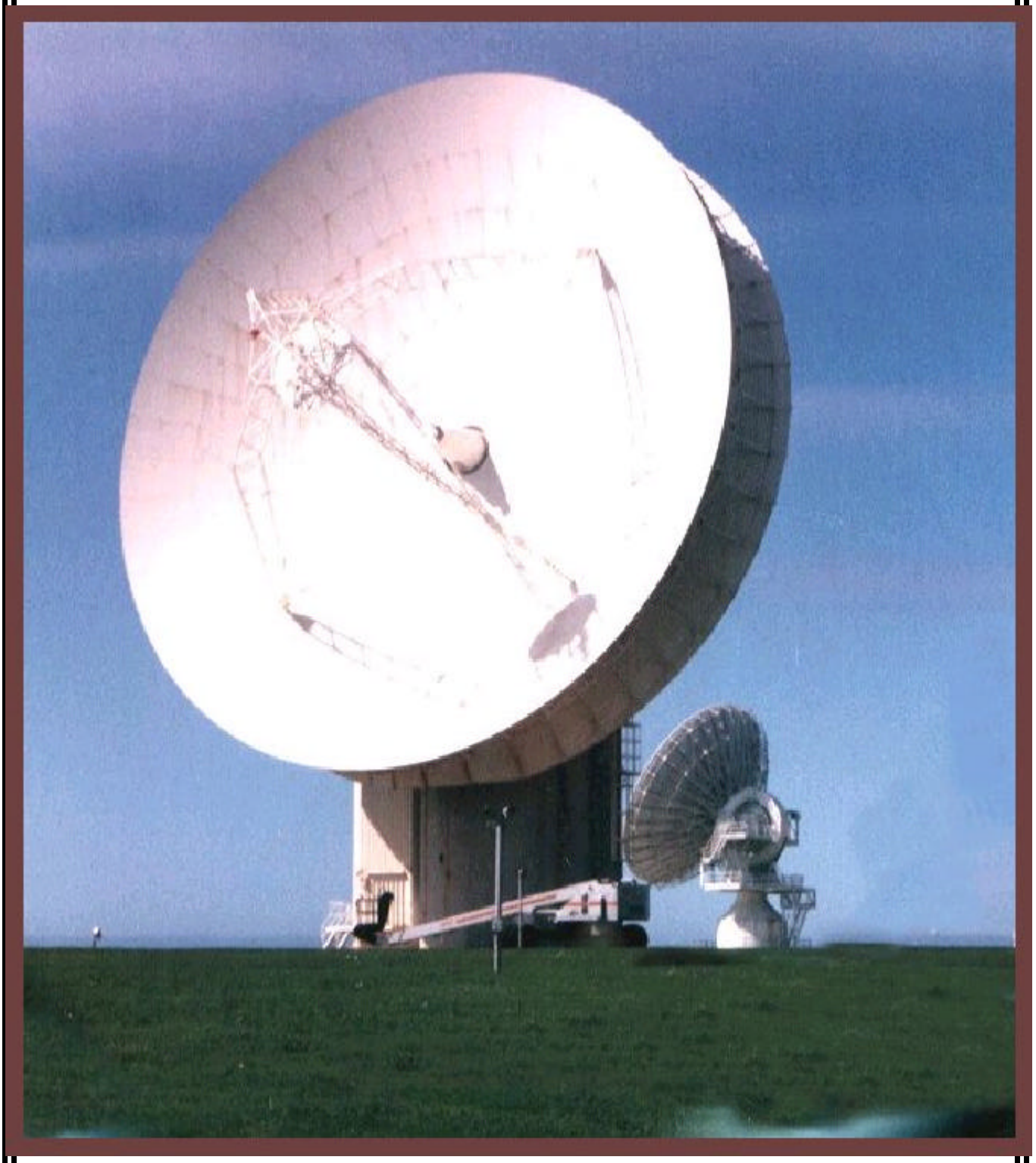
Working document for the STOA Panel

Luxembourg,October 1999 PE 168.184/Vol 2/5

*Cataloguing data*:

| | |
|---|---|
| Title: | **Part 2/5:The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ulti-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition** |
| Workplan Ref.: | EP/IV/B/STOA/98/1401 |
| Publisher: | European Parliament<br>Directorate General for Research<br>Directorate A<br>The STOA Programme |
| Author: | Duncan Campbell - IPTV Ltd.- Edinburgh |
| Editor: | Mr Dick HOLDSWORTH,<br>Head of STOA Unit |
| Date: | October 1999 |
| PE number: | **PE 168. 184 Vol 2/5** |

# Interception Capabilities 2000



**Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of**

**economic information. This study considers 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.**

# Interception Capabilities 2000

## Contents

**Duncan Campbell**
**IPTV Ltd**
**Edinburgh, Scotland**
**April, 1999**

***mailto:iptv@cwcom.net***

Cover : 30 metre antennae at the Composite Signals Organisation Station, Morwenstow, England, intercepting communications from Atlantic Ocean and Indian Ocean regional satellites. (D Campbell)

# Summary


1. **Communications intelligence** (Comint) involving the covert interception of foreign communications has been practised by almost every advanced nation since international telecommunications became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments. The capabilities of and constraints on Comint activity may usefully be considered in the framework of the "intelligence cycle" (section 1).

2. Globally, about 15-20 billion Euro is expended annually on Comint and related activities. The largest component of this expenditure is incurred by the major English-speaking nations of the UKUSA alliance. [1] This report describes how Comint organisations have for more than 80 years made arrangements to obtain access to much of the world's international communications. These include the unauthorised interception of commercial satellites, of long distance communications from space, of undersea cables using submarines, and of the Internet. In excess of 120 currently in simultaneous operation collecting intelligence (section 2).

3. The highly automated UKUSA system for processing Comint, often known as ECHELON, has been widely discussed within Europe following a 1997 STOA report.[2] That report summarised information from the only two primary sources then available on ECHELON. [3] This report provides original new documentary and other evidence about the ECHELON system and its involvement in the interception of communication satellites (section 3). A technical annexe give a supplementary, detailed description of Comint processing methods.

4. Comint information derived from the interception of international communications has long been routinely used to obtain sensitive data concerning individuals, governments, trade and international organisations. This report sets out the organisational and reporting frameworks within which economically sensitive information is collected and disseminated, summarising examples where European commercial organisations have been the subject of surveillance (section 4).

5. This report identifies a previously unknown international organisation - “ILETS” - which has, without parliamentary or public discussion or awareness, put in place contentious plans to require manufacturers and operators of new communications systems to build in monitoring capacity for use by national security or law enforcement organisations (section 5).

6. Comint organisations now perceive that the technical difficulties of collecting communications are increasing, and that future production may be costlier and more limited than at present. The perception of such difficulties may provide a useful basis for policy options aimed at protective measures concerning economic information and effective encryption (section 6).

7. **Key findings** concerning the state of the art in Comint include :

   - Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions (section 2, technical annexe);
   - Contrary to reports in the press, effective "word spotting" search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research. However, speaker recognition systems – in effect, "voiceprints" – have been developed and are deployed to recognise the speech of targeted individuals making international telephone calls;
   - Recent diplomatic initiatives by the United States government seeking European agreement to the "key escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non-US nationals, including European governments, companies and citizens;
   - There is wide-ranging evidence indicating that major governments are routinely utilising communications intelligence to provide commercial advantage to companies and trade.

# 1. Organisations and methods

## What is communications intelligence?

1. Communications intelligence (Comint) is defined by NSA, the largest agency conducting such operations as "technical and intelligence information derived from foreign communications by other than their intended recipient". [4] Comint is a major component of Sigint (signals intelligence), which also includes the collection of non-communications signals, such as radar emissions.[5] Although this report deals with agencies and systems whose overall task may be Sigint, it is concerned only with Comint.

2. Comint has shadowed the development of extensive high capacity new civil telecommunications systems, and has in consequence become a large-scale industrial activity employing many skilled workers and utilising exceptionally high degrees of automation.

3. The targets of Comint operations are varied. The most traditional Comint targets are military messages and diplomatic communications between national capitals and missions abroad. Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of Comint. More recent targets include narcotics trafficking, money laundering, terrorism and organised crime.

4. Whenever access to international communications channels is obtained for one purpose, access to every other type of communications carried on the same channels is automatic, subject only to the tasking requirements of agencies. Thus, for example, NSA and its British counterpart GCHQ, used Comint collected primarily for other purposes to provide data about domestic political opposition figures in the United States between 1967 and 1975.

### UKUSA alliance

5. The United States Sigint System (USSS) consists of the National Security Agency (NSA), military support units collectively called the Central Security Service, and parts of the CIA and other organisations. Following wartime collaboration, in 1947 the UK and the US made a secret agreement to continue to conduct collaborative global Comint activities. Three other English-speaking nations, Canada, Australia and New Zealand joined the UKUSA agreement as "Second Parties". The UKUSA agreement was not acknowledged publicly until March 1999, when the Australian government confirmed that its Sigint organisation, Defence Signals Directorate (DSD) "does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship".[6] The UKUSA agreement shares facilities, tasks and product between participating governments.

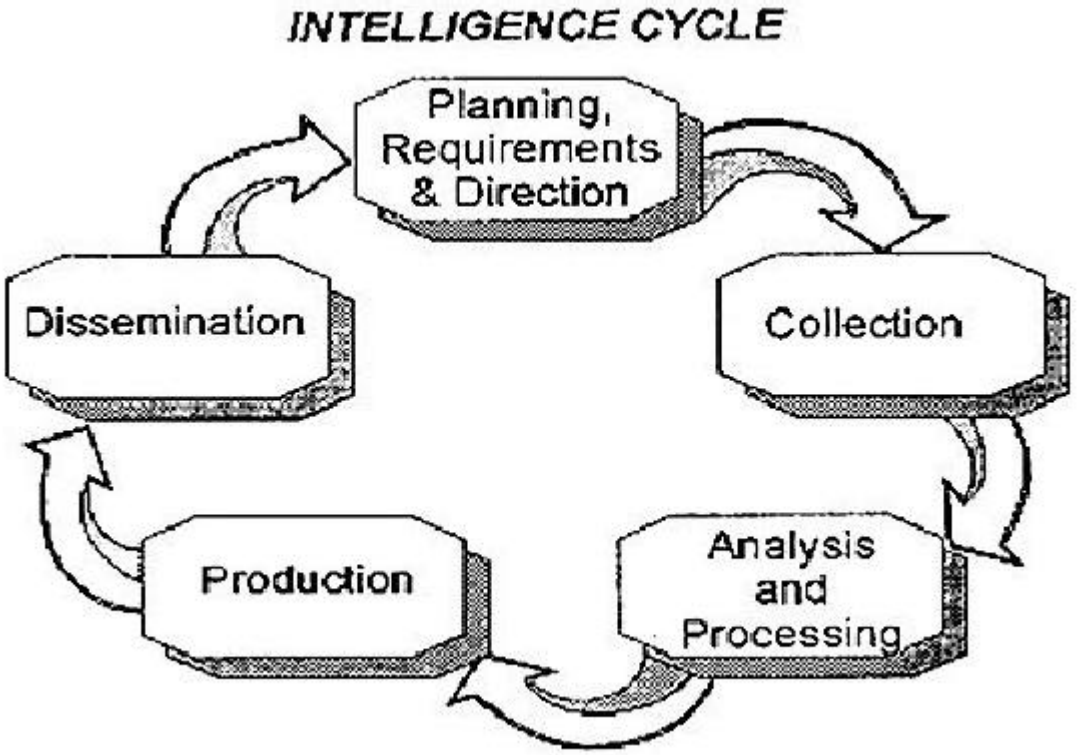
6. Although UKUSA Comint agency staffs and budgets have shrunk following the end of the cold war, they have reaffirmed their requirements for access to all the world's communications. Addressing NSA staff on his departure in 1992, then NSA director Admiral William Studeman described how "the demands for increased global access are growing". The "business area" of "global access" was, he said, one of "two, hopefully strong, legs upon which NSA must stand" in the next century.[7]

### Other Comint organisations

7. Besides UKUSA, there at least 30 other nations operating major Comint organisations. The largest is the Russian FAPSI, with 54,000 employees.[8] China maintains a substantial Sigint system, two stations of which are directed at Russia and operate in collaboration with the United States. Most Middle Eastern and Asian nations have invested substantially in Sigint, in particular Israel, India and Pakistan.

## How intelligence works

8. In the post cold war era, Comint interception has been constrained by recognisable industrial features, including the requirement to match budgets and capabilities to customer requirements. The multi-step process by means of which communications intelligence is sought, collected, processed and passed on is similar for all countries, and is often described as the "intelligence cycle". The steps of the intelligence cycle correspond to distinct organisational and technical features of Comint production. Thus, for example, the administration of NSA's largest field station in the world, at Menwith Hill in England and responsible for operating over 250




classified projects, is divided into three directorates: OP, Operations and Plans; CP, Collection Processing; and EP, Exploitation and Production.

### Planning

9. Planning first involves determining customer requirements. Customers include the major ministries of the sponsoring government – notably those concerned with defence, foreign affairs, security, trade and home affairs. The overall management of Comint involves the identification of requirements for data as well as translating requirements into potentially achievable tasks, prioritising, arranging analysis and reporting, and monitoring the quality of Comint product.

10. Once targets have been selected, specific existing or new collection capabilities may be **tasked**, based on the type of information required, the susceptibility of the targeted activity to collection, and the likely effectiveness of collection.

### Access and collection

11. The first essential of Comint is **access** to the desired communications medium so that communications may be intercepted. Historically, where long-range radio communications were used, this task was simple. Some important modern communications systems are not "Comint friendly" and may require unusual, expensive or intrusive methods to gain access. The physical means of communication is usually independent of the type of information carried. For example, inter-city microwave radio-relay systems, international satellite links and fibre optic submarine cables will all usually carry mixed traffic of television, telephone, fax, data links, private voice, video and data.

**12.** **Collection** follows **interception**, but is a distinct activity in that many types of signals may be intercepted but will receive no further processing save perhaps technical searches to verify that communications patterns remain unchanged. For example, a satellite interception station tasked to study a newly launched communications satellite will set up an antenna to intercept all that the satellite sends to the ground. Once a survey has established which parts of the satellite's signals carry, say, television or communications of no interest, these signals will not progress further within the system.

13. Collection includes both acquiring information by interception and passing information of interest downstream for **processing** and **production**. Because of the high information rates used in many modern networks, and the complexity of the signals within them, it is now common for high speed recorders or "snapshot" memories temporarily to hold large quantities of data while processing takes place. Modern collection activities use secure, rapid communications to pass data via global networks to human analysts who may be a continent

away. Selecting messages for collection and processing is in most cases automated, involving large on-line databanks holding information about targets of interest.

### Processing

**14.** **Processing** is the conversion of collected information into a form suitable for analysis or the production of intelligence, either automatically or under human supervision. Incoming communications are normally converted into standard formats identifying their technical characteristics, together with message (or signal) related information (such as the telephone numbers of the parties to a telephone conversation).

15. At an early stage, if it is not inherent in the selection of the message or conversation, each intercepted signal or channel will be described in standard "case notation". Case notation first identifies the countries whose communications have been intercepted, usually by two letters. A third letter designates the general class of communications: C for commercial carrier intercepts, D for diplomatic messages, P for police channels, etc. A fourth letter designates the type of communications system (such as S for multi-channel). Numbers then designate particular links or networks. Thus for example, during the 1980s NSA intercepted and processed traffic designated as "FRD" (French diplomatic) from Chicksands, England, while the British Comint agency GCHQ deciphered "ITD" (Italian diplomatic) messages at its Cheltenham headquarters. [9]

16. Processing may also involve translation or "gisting" (replacing a verbatim text with the sense or main points of a communication). Translation and gisting can to some degree be automated.

### Production and dissemination

17. Comint **production** involves analysis, evaluation, translation and interpretation of raw data into finished intelligence. The final step of the intelligence cycle is **dissemination**, meaning the passing of reports to the intelligence consumers. Such reports can consist of raw (but decrypted and/or translated) messages, gists, commentary, or extensive analyses. The quality and relevance of the disseminated reports lead in turn to the re-specification of intelligence collection priorities, thereby completing the intelligence cycle.

18. The nature of dissemination is highly significant to questions of how Comint is exploited to obtain economic advantage. Comint activities everywhere are highly classified because, it is argued, knowledge of the success of interception would be likely to lead targets to change their communications methods to defeat future interception. Within the UKUSA system, the dissemination of Comint reports is limited to individuals holding high-level security "SCI" clearances.[10] Further, because only cleared officials can see Comint reports, only they can set requirements and thus control tasking. Officials of commercial companies normally neither have clearance nor routine access to Comint, and may therefore only benefit from commercially relevant Comint information to the extent that senior, cleared government officials permit. The ways in which this takes place is described in Section 5, below.

19. Dissemination is further restricted within the UKUSA organisation by national and international rules generally stipulating that the Sigint agencies of each nation may not normally collect or (if inadvertently collected) record or disseminate information about citizens of, or companies registered in, any other UKUSA nation. Citizens and companies are collectively known as "legal persons". The opposite procedure is followed if the person concerned has been targeted by their national Comint organisation.

20. For example, Hager has described [11] how New Zealand officials were instructed to remove the names of identifiable UKUSA citizens or companies from their reports, inserting instead words such as "a Canadian citizen" or "a US company". British Comint staff have described following similar procedures in respect of US citizens following the introduction of legislation to limit NSA's domestic intelligence activities in 1978. [12]The Australian government says that "DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others … the Rules [on Sigint and Australian persons] prohibit the dissemination of information relating to Australian persons gained accidentally during the course of routine collection of foreign communications; or the reporting or recording of the names of Australian persons mentioned in foreign communications".[13] The corollary is also true; <u>UKUSA nations place no restrictions on intelligence gathering affecting either citizens or companies of any non-UKUSA nation, including member states of the European Union (except the UK)</u>.

# 2. Intercepting international communications

## International Leased Carrier (ILC) communications

21. It is a matter of record that foreign communications to and from, or passing through the United Kingdom and the United States have been intercepted for more than 80 years.[14] Then and since, most international communications links have been operated by international carriers, who are usually individual national PTTs or private companies. In either case, capacity on the communication system is leased to individual national or international telecommunications undertakings. For this reason, Comint organisations use the term ILC (International Leased Carrier) to describe such collection.

### High frequency radio

22. Save for direct landline connections between geographically contiguous nations, high frequency (HF) radio system were the most common means of international telecommunications prior to 1960, and were in use for ILC, diplomatic and military purposes. An important characteristic of HF radio signals is that they are reflected from the ionosphere and from the earth's surface, providing ranges of thousands of miles. This enables both reception and interception.

### Microwave radio relay

23. Microwave radio was introduced in the 1950s to provide high capacity inter-city communications for telephony, telegraphy and, later, television. Microwave radio relay communications utilise low power transmitters and parabolic dish antennae placed on towers in high positions such as on hilltops or tall buildings. The antennae are usually 1-3m in diameter. Because of the curvature of the earth, relay stations are generally required every 30-50km.

### Subsea cables

24. Submarine telephone cables provided the first major reliable high capacity international communications systems. Early systems were limited to a few hundred simultaneous telephone channels. The most modern optical fibre systems carry up to 5 Gbps (Gigabits per second) of digital information. This is broadly equivalent to about 60,000 simultaneous telephone channels.

### Communications satellites

25. Microwave radio signals are not reflected from the ionosphere and pass directly into space. This property has been exploited both to provide global communications and, conversely, to intercept such communications in space and on land. The largest constellation of communications satellites (COMSATs) is operated by the International Telecommunications Satellite organisation (Intelsat), an international treaty organisation. To provide permanent communications from point to point or for broadcasting purposes, communications satellites are placed into so-called "geostationary" orbits such that, to the earth-based observer, they appear to maintain the same position in the sky.

26. The first geostationary Intelsat satellites were orbited in 1967. Satellite technology developed rapidly. The fourth generation of Intelsat satellites, introduced in 1971, provided capacity for 4,000 simulataneous telephone channels and were capable of handling all forms of communications simultaneously –telephone, telex, telegraph, television, data and facsimile. In 1999, Intelsat operated 19 satellites of its 5th to 8th generations. The latest generation can handle the equivalent to 90,000 simultaneous calls.

### Communications techniques

27. Prior to 1970, most communications systems (however carried) utilised analogue or continuous wave techniques. Since 1990, almost all communications have been digital, and are providing ever higher capacity. The highest capacity systems in general use for the Internet, called STM-1 or OC-3, operates at a data rate of 155Mbs. (Million bits per second; a rate of 155 Mbps is equivalent to sending 3 million words every second, roughly the text of one thousand books a minute.) For example, links at this capacity are used to provide backbone Internet connections between Europe and the United States. Further details of communications techniques are given in the technical annexe.

## ILC communications collection

### Access

28. Comint collection cannot take place unless the collecting agency obtains access to the communications channels they wish to examine. Information about the means used to gain access are, like data about code-breaking methods, the most highly protected information within any Comint organisation. Access is gained both with and without the complicity or co-operation of network operators.

### Operation SHAMROCK

29. From 1945 onwards in the United States the NSA and predecessor agencies systematically obtained cable traffic from the offices of the major cable companies. This activity was codenamed SHAMROCK. These activities remained unknown for 30 years, until enquiries were prompted by the Watergate affair. On 8 August 1975, NSA Director Lt General Lew Allen admitted to the Pike Committee of the US House of Representatives that :

*"NSA systematically intercepts international communications, both voice and cable".*

*High frequency radio interception antenna (AN/FLR9)*


*DOJOCC sign at NSA Station, Chicksands.*

30. He also admitted that "messages to and from American citizens have been picked up in the course of gathering foreign intelligence". US legislators considered that such operations might have been unconstitutional. During 1976, a Department of Justice team investigated possible criminal offences by NSA. Part of their report was released in 1980. It described how intelligence on US citizens:

> *"was obtained <u>incidentally</u> in the course of NSA's interception of aural and non-aural (e.g., telex) international communications and the receipt of GCHQ-acquired telex and ILC (International Leased Carrier) cable traffic (SHAMROCK)" (emphasis in original).* [15]

### High frequency radio interception

31. High frequency radio signals are relatively easy to intercept, requiring only a suitable area of land in, ideally, a "quiet" radio environment. From 1945 until the early 1980s, both NSA and GCHQ operated HF radio interception systems tasked to collect European ILC communications in Scotland. [16]

32. The most advanced type of HF monitoring system deployed during this period for Comint purposes was a large circular antenna array known as AN/FLR-9. AN/FLR-9 antennae are more than 400 metres in diameter. They can simultaneously intercept and determine the bearing of signals from as many directions and on as many frequencies as may be desired. In 1964, AN/FLR-9 receiving systems were installed at San Vito dei Normanni, Italy; Chicksands, England, and Karamursel, Turkey.

33. In August 1966, NSA transferred ILC collection activities from its Scottish site at Kirknewton, to Menwith Hill in England. Ten years later, this activity was again transferred, to Chicksands. Although the primary function of the Chicksands site was to intercept Soviet and Warsaw Pact air force communications, it was also tasked to collect ILC and "NDC" (Non-US Diplomatic Communications). Prominent among such tasks was the collection of FRD traffic (i.e., French diplomatic communications). Although most personnel at Chicksands were members of the US Air Force, diplomatic and ILC interception was handled by civilian NSA employees in a unit called DODJOCC. [17]

34. During the 1970s, British Comint units on Cyprus were tasked to collect HF communications of allied NATO nations, including Greece and Turkey. The interception took place at a British army unit at Ayios Nikolaos, eastern Cyprus.[18] In the United States in 1975, investigations by a US Congressional Committee revealed that NSA was collecting diplomatic messages sent to and from Washington from an army Comint site at Vint Hill Farms, Virginia. The targets of this station included the United Kingdom.[19]

*Inter-city microwave radio relay tower "spills" its signals into space (below)*

### Space interception of inter-city networks

35. Long distance microwave radio relay links may require dozens of intermediate stations to receive and re-transmit communications. Each subsequent receiving station picks up only a tiny fraction of the original transmitted signal; the remainder passes over the horizon and on into space, where satellites can collect it. These principles were exploited during the 1960s to provide Comint collection from space. The nature of microwave "spillage" means that the best position for such satellites is not above the chosen target, but up to 80 degrees of longitude away.

36. The first US Comint satellite, CANYON, was launched In August 1968, followed soon by a second. The satellites were controlled from a ground station at Bad Aibling, Germany. In order to provide permanent coverage of selected targets, CANYON satellites were placed close to geostationary orbits. However, the orbits were not exact, causing the satellites to change position and obtain more data on ground targets.[20] Seven CANYON satellites were launched between 1968 and 1977.

links extended for thousands of miles, much of it over Siberia, where permafrost restricted the reliable use of underground cables. Geographical circumstances thus favoured NSA by making Soviet internal communications links highly accessible. The satellites performed better than expected, so the project was extended.

38. The success of CANYON led to the design and deployment of a new class of Comint satellites, CHALET. The ground station chosen for the CHALET series was Menwith Hill, England. Under NSA project P-285, US companies were contracted to install and assist in operating the satellite control system and downlinks (RUNWAY) and ground processing system (SILKWORTH). The first two CHALET satellites were launched in June 1978 and October 1979. After the name of the first satellite appeared in the US press, they were renamed VORTEX. In 1982, NSA obtained approval for expanded "new mission requirements" and were given funds and facilities to operate four VORTEX satellites simultaneously. A new 5,000m$^2$ operations centre (STEEPLEBUSH) was constructed to house processing equipment. When the name VORTEX was published in 1987, the satellites were renamed MERCURY.[21]

39. The expanded mission given to Menwith Hill after 1985 included MERCURY collection from the Middle East. The station received an award for support to US naval operations in the Persian Gulf from 1987 to 1988. In 1991, a further award was given for support of the Iraqi war operations, Desert Storm and Desert Shield.[22] Menwith Hill is now the major US site for Comint collection against its major ally, Israel. Its staff includes linguists trained in Hebrew, Arabic and Farsi as well as European languages. Menwith Hill has recently been expanded to include ground links for a new network of Sigint satellites launched in 1994 and 1995 (RUTLEY). The name of the new class of satellites remains unknown.

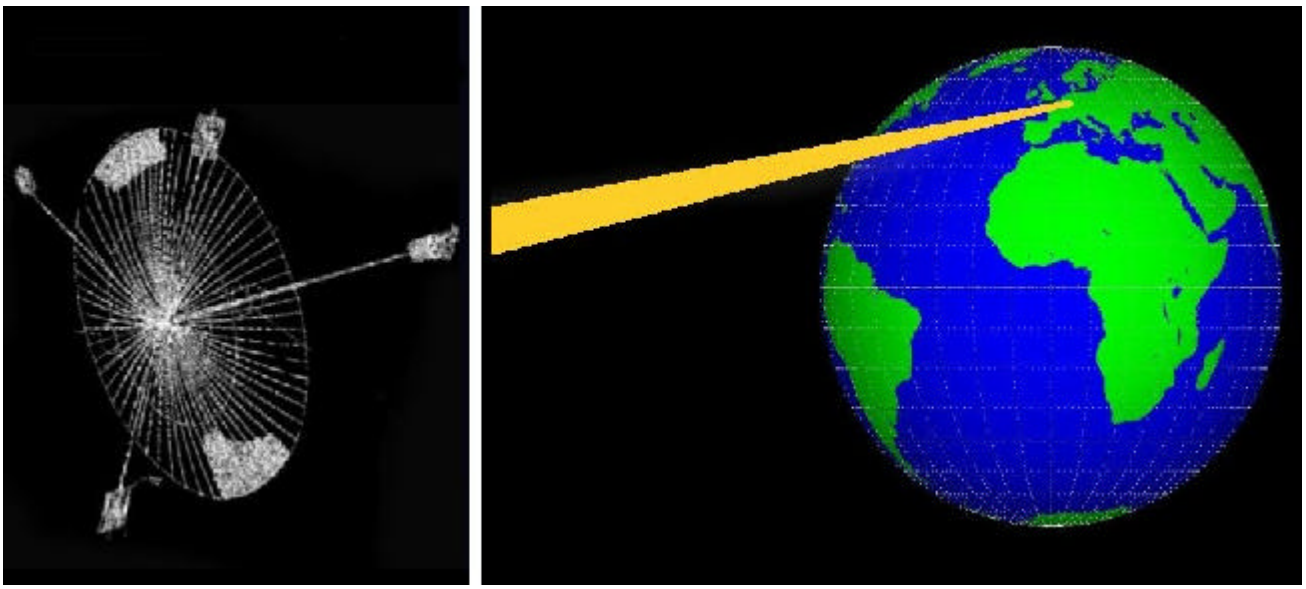
### Sigint satellites

40. The CIA developed a second class of Sigint satellite with complementary capabilities over the period from 1967 to 1985. Initially known as RHYOLITE and later AQUACADE, these satellites were operated from a remote ground station in central Australia, Pine Gap. Using a large parabolic antenna which unfolded in space, RHYOLITE intercepted lower frequency signals in the VHF and UHF bands. Larger, most recent satellites of this type have been named MAGNUM and then ORION. Their targets include telemetry, VHF radio, cellular mobile phones, paging signals, and mobile data links.

41. A third class of satellite, known first as JUMPSEAT and latterly as TRUMPET, operates in highly elliptical near-polar orbits enabling them to "hover" for long period over high northern latitudes. They enable the United States to collect signals from transmitters in high northern latitudes poorly covered by MERCURY or ORION, and also to intercept signals sent to Russian communications satellites in the same orbits.

42. Although precise details of US space-based Sigint satellites launched after 1990 remain obscure, it is apparent from observation of the relevant ground centres that collection systems have expanded rather than contracted. The main stations are at Buckley Field, Denver, Colorado; Pine Gap, Australia; Menwith Hill, England; and Bad Aibling, Germany. The satellites and their processing facilities are exceptionally costly (of the order of $1 billion US each). In 1998, the US National Reconnaissance Office (NRO) announced plans to combine the three separate classes of Sigint satellites into an Integrated Overhead Sigint Architecture (IOSA) in order to " improve Sigint performance and avoid costs by consolidating systems, utilising … new satellite and data processing technologies". [23]

43. It follows that, within constraints imposed by budgetary limitation and tasking priorities, the United States can if it chooses direct space collection systems to intercept mobile communications signals and microwave city-to-city traffic anywhere on the planet. The geographical and processing difficulties of collecting messages simultaneously from all parts of the globe suggest strongly that the tasking of these satellites will be directed towards the highest priority national and military targets. Thus, although European communications passing on inter-city microwave routes can be collected, it is likely that they are normally ignored. But it is very highly probable that communications to or from Europe and which pass through the microwave communications networks of Middle Eastern states are collected and processed.



*Comint satellites in geostarionary orbits, such as VORTEX, intercept terrestial microwave "spillage".*

44. No other nation (including the former Soviet Union) has deployed satellites comparable to CANYON, RHYOLITE, or their successors. Both Britain (project ZIRCON) and France (project ZENON) have attempted to do so, but neither persevered. After 1988 the British government purchased capacity on the US VORTEX (now MERCURY) constellation to use for unilateral national purposes. [24] A senior UK Liaison Officer and staff from GCHQ work at Menwith Hill NSA station and assist in tasking and operating the satellites.

### COMSAT ILC collection

45. Systematic collection of COMSAT ILC communications began in 1971. Two ground stations were built for this purpose. The first at Morwenstow, Cornwall, England had two 30-metre antennae. One intercepted communications from the Atlantic Ocean Intelsat; the other the Indian Ocean Intelsat. The second Intelsat interception site was at Yakima, Washington in the northwestern United States. NSA's "Yakima Research Station" intercepted communications passing through the Pacific Ocean Intelsat satellite.

46. ILC interception capability against western-run communications satellites remained at this level until the late 1970s, when a second US site at Sugar Grove, West Virginia was added to the network. By 1980, its three satellite antenna had been reassigned to the US Naval Security Group and were used for COMSAT interception. Large-scale expansion of the ILC satellite interception system took place between 1985 and 1995, in conjunction with the enlargement of the ECHELON processing system (section 3). New stations were constructed in the United States (Sabana Seca, Puerto Rico), Canada (Leitrim, Ontario), Australia (Kojarena, Western Australia) and New Zealand (Waihopai, South Island). Capacity at Yakima, Morwenstow and Sugar Grove was expanded, and continues to expand.

    Based on a simple count of the number of antennae currently installed at each COMSAT interception or satellite SIGINT station, it appears that indicates that **the UKUSA nations are between them currently operating at least 120 satellite based collection systems.** The approximate number of antennae in each category are :

    - **Tasked on western commercial communications satellites (ILC) 40**
    - **Controlling space based signals intelligence satellites 30**
    - **Currently or formerly tasked on Soviet communications satellites 50**

    Systems in the third category may have been reallocated to ILC tasks since the end of the cold war. [25]

47. Other nations increasingly collect Comint from satellites. Russia's FAPSI operates large ground collection sites at Lourdes, Cuba and at Cam Ranh Bay, Vietnam.[26] Germany's BND and France's DGSE are alleged to collaborate in the operation of a COMSAT collection site at Kourou, Guyana, targeted on "American and South American satellite communications". DGSE is also said to have COMSAT collection sites at Domme (Dordogne, France), in New Caledonia, and in the United Arab Emirates.[27] The Swiss intelligence service has recently announced a plan for two COMSAT interception stations.[28]

*Satellite ground terminal at Etam, West Virginia, connecting Europe and the US via Intelsat IV*

*GCHQ constructed an identical "shadow" station in 1972 to intercept Intelsat messages for UKUSA*

### Submarine cable interception

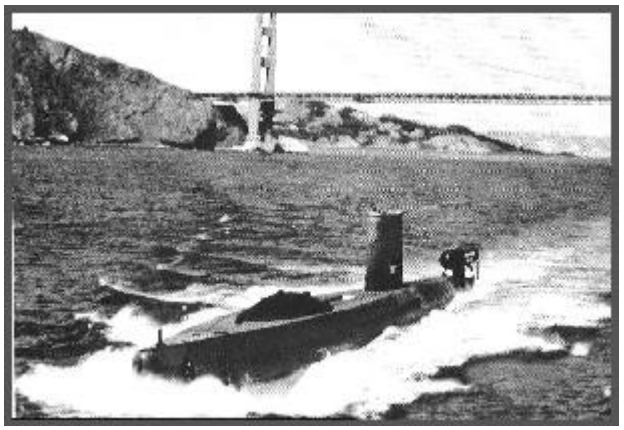
48. Submarine cables now play a dominant role in international telecommunications, since – in contrast to the limited bandwidth available for space systems – optical media offer seemingly unlimited capacity. Save where cables terminate in countries where telecommunications operators provide Comint access (such as the UK and the US), submarine cables appear intrinsically secure because of the nature of the ocean environment.

49. In October 1971, this security was shown not to exist. A US submarine, Halibut, visited the Sea of Okhotsk off the eastern USSR and recorded communications passing on a military cable to the Khamchatka Peninsula. Halibut was equipped with a deep diving chamber, fully in view on the submarine's stern. The chamber was described by the US Navy as a "deep submergence rescue vehicle". The truth was that the "rescue vehicle" was welded immovably to the submarine. Once submerged, deep-sea divers exited the submarine and wrapped tapping coils around the cable. Having proven the principle, USS Halibut returned in 1972 and laid a high capacity recording pod next to the cable. The technique involved no physical damage and was unlikely to have been readily detectable. [29]

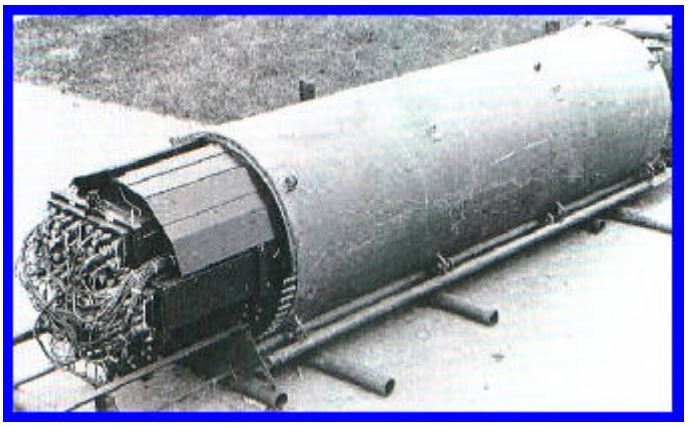
50. The Okhotsk cable tapping operation continued for ten years, involving routine trips by three different specially equipped submarines to collect old pods and lay new ones; sometimes, more than one pod at a time. New targets were added in 1979. That summer, a newly converted submarine called USS Parche travelled from San Francisco under the North Pole to the Barents Sea, and laid a new cable tap near Murmansk. Its crew received a presidential citation for their achievement. The Okhotsk cable tap ended in 1982, after its location was compromised by a former NSA employee who sold information about the tap, codenamed IVY BELLS, to the Soviet Union. One of the IVY BELLS pods is now on display in the Moscow museum of the former KGB. The cable tap in the Barents Sea continued in operation, undetected, until tapping stopped in 1992.

51. During 1985, cable-tapping operations were extended into the Mediterranean, to intercept cables linking Europe to West Africa. [30] After the cold war ended, the USS Parche was refitted with an extended section to accommodate larger cable tapping equipment and pods. Cable taps could be laid by remote control, using drones. USS Parche continues in operation to the present day, but the precise targets of its missions remain unknown. The Clinton administration evidently places high value on its achievements, Every year from 1994 to 1997, the submarine crew has been highly commended. [31] Likely targets may include the Middle East, Mediterranean, eastern Asia, and South America. The United States is the only naval power known to have deployed deep-sea technology for this purpose.

52. Miniaturised inductive taps recorders have also been used to intercept underground cables.[32] Optical fibre cables, however, do not leak radio frequency signals and cannot be tapped using inductive loops. NSA and other Comint agencies have spent a great deal of money on research into tapping optical fibres, reportedly with little success. But long distance optical fibre cables are not invulnerable. The key means of access is by tampering with optoelectronic "repeaters" which boost signal levels over long distances. It follows that any submarine cable system using submerged optoelectronic repeaters cannot be considered secure from



*USS Halibut with disguised chamber for diving*



*Cable tapping pod laid by US submarine off Khamchatka*

interception and communications intelligence activity.

### Intercepting the Internet

53. The dramatic growth in the size and significance of the Internet and of related forms of digital communications has been argued by some to pose a challenge for Comint agencies. This does not appear correct. During the 1980s, NSA and its UKUSA partners operated a larger international communications network than the then Internet but based on the same technology.[33] According to its British partner "all GCHQ systems are linked together on the largest LAN [Local Area Network] in Europe, which is connected to other sites around the world via one of the largest WANs [Wide Area Networks] in the world … its main networking protocol is Internet Protocol (IP).[34] This global network, developed as project EMBROIDERY, includes PATHWAY, the NSA's main computer communications network. It provides fast, secure global communications for ECHELON and other systems.

54. Since the early 1990s, fast and sophisticated Comint systems have been developed to collect, filter and analyse the forms of fast digital communications used by the Internet. Because most of the world's Internet capacity lies within the United States or connects to the United States, many communications in "cyberspace" will pass through intermediate sites within the United States. Communications from Europe to and from Asia, Oceania, Africa or South America normally travel via the United States.

55. Routes taken by Internet "packets" depend on the origin and destination of the data, the systems through which they enter and leaves the Internet, and a myriad of other factors including time of day. Thus, routers within the western United States are at their most idle at the time when central European traffic is reaching peak usage. It is thus possible (and reasonable) for messages travelling a short distance in a busy European network to travel instead, for example, via Internet exchanges in California. It follows that a large proportion of international communications on the Internet will by the nature of the system pass through the United States and thus be readily accessible to NSA.

56. Standard Internet messages are composed of packets called "datagrams" . Datagrams include numbers representing both their origin and their destination, called "IP addresses". The addresses are unique to each computer connected to the Internet. They are inherently easy to identify as to country and site of origin and destination. Handling, sorting and routing millions of such packets each second is fundamental to the operation of major Internet centres. The same process facilitates extraction of traffic for Comint purposes.

57. Internet traffic can be accessed either from international communications links entering the United States, or when it reaches major Internet exchanges. Both methods have advantages. Access to communications systems is likely to be remain clandestine - whereas access to Internet exchanges might be more detectable

but provides easier access to more data and simpler sorting methods. Although the quantities of data involved are immense, NSA is normally legally restricted to looking only at communications that start or finish in a foreign country. Unless special warrants are issued, all other data should normally be thrown away by machine before it can be examined or recorded.

58. Much other Internet traffic (whether foreign to the US or not) is of trivial intelligence interest or can be handled in other ways. For example, messages sent to "Usenet" discussion groups amounts to about 15 Gigabytes (GB) of data per day; the rough equivalent of 10,000 books. All this data is broadcast to anyone wanting (or willing) to have it. Like other Internet users, intelligence agencies have open source access to this data and store and analyse it. In the UK, the Defence Evaluation and Research Agency maintains a 1 Terabyte database containing the previous 90 days of Usenet messages.[35] A similar service, called "Deja News", is available to users of the World Wide Web (WWW). Messages for Usenet are readily distinguishable. It is pointless to collect them clandestinely.

59. Similar considerations affect the World Wide Web, most of which is openly accessible. Web sites are examined continuously by "search engines" which generate catalogues of their contents. "Alta Vista" and "Hotbot" are prominent public sites of this kind. NSA similarly employs computer "bots" (robots) to collect data of interest. For example, a New York web site known as JYA.COM (http://www.jya.com/cryptome) offers extensive public information on Sigint, Comint and cryptography. The site is frequently updated. Records of access to the site show that every morning it is visited by a "bot" from NSA's National Computer Security Centre, which looks for new files and makes copies of any that it finds.[36]

60. It follows that foreign Internet traffic of communications intelligence interest – consisting of e-mail, file transfers, "virtual private networks" operated over the internet, and some other messages - will form at best a few per cent of the traffic on most US Internet exchanges or backbone links. According to a former employee, NSA had by 1995 installed “sniffer” software to collect such traffic at nine major Internet exchange points (IXPs).[37] The first two such sites identified, FIX East and FIX West, are operated by US government agencies. They are closely linked to nearby commercial locations, MAE East and MAE West (see table). Three other sites listed were Network Access Points originally developed by the US National Science Foundation to provide the US Internet with its initial "backbone".

| Internet site | Location | Operator | Designation |
|---|---|---|---|
| FIX East | College Park, Maryland | US government | Federal Information Exchange |
| FIX West | Mountain View, California | US government | Federal Information Exchange |
| MAE East | Washington, DC | MCI | Metropolitan Area Ethernet |
| New York NAP | Pennsauken, New Jersey | Sprintlink | Network Access Point |
| SWAB | Washington, DC | PSInet / Bell Atlantic | SMDS Washington Area Bypass |
| Chicago NAP | Chicago, Illinois | Ameritech / Bellcorp | Network Access Point |
| San Francisco NAP | San Francisco, California | Pacific Bell | Network Access Point |
| MAE West | San Jose, California | MCI | Metropolitan Area Ethernet |
| CIX | Santa Clara California | CIX | Commercial Internet Exchange |

*Table 1 NSA Internet Comint access at IXP sites (1995)* [38]

61. The same article alleged that a leading US Internet and telecommunications company had contracted with NSA to develop software to capture Internet data of interest, and that deals had been struck with the leading manufacturers Microsoft, Lotus, and Netscape to alter their products for foreign use. The latter allegation has proven correct (see technical annexe). Providing such features would make little sense unless NSA had also arranged general access to Internet traffic. Although NSA will not confirm or deny such allegations, a 1997 court case in Britain involving alleged "computer hacking" produced evidence of NSA surveillance of the Internet. Witnesses from the US Air Force component of NSA acknowledged using packet sniffers and specialised programmes to track attempts to enter US military computers. The case collapsed after the witnesses refused to provide evidence about the systems they had used.[39]

### Covert collection of high capacity signals

62. Where access to signals of interest is not possible by other means, Comint agencies have constructed special purpose interception equipment to install in embassies or other diplomatic premises, or even to carry by hand to locations of special interest. Extensive descriptions of operations of this kind have been published by Mike

Frost, a former official of CSE, the Canadian Sigint agency.[40] Although city centre embassy premises are often ideally situated to intercept a wide range of communications, ranging from official carphone services to high capacity microwave links, processing and passing on such information may be difficult. Such collection operations are also highly sensitive for diplomatic reasons. Equipment for covert collection is therefore specialised, selective and miniaturised.

63. A joint NSA/CIA "Special Collection Service" manufactures equipment and trains personnel for covert collection activities One major device is a suitcase-sized computer processing system. ORATORY. ORATORY is in effect a miniaturised version of the Dictionary computers described in the next section, capable of selecting non-verbal communications of interest from a wide range of inputs, according to pre-programmed selection criteria. One major NSA supplier ("The IDEAS Operation") now offers micro-miniature digital receivers which can simultaneously process Sigint data from 8 independent channels. This radio receiver is the size of a credit card. It fits in a standard laptop computer. IDEAS claim, reasonably, that their tiny card "performs functions that would have taken a rack full of equipment not long ago".

### New satellite networks

64. New network operators have constructed mobile phone systems providing unbroken global coverage using satellites in low or medium level earth orbits. These systems are sometimes called satellite personal communications systems (SPCS). Because each satellite covers only a small area and moves fast, large numbers of satellites are needed to provide continuous global coverage. The satellites can relay signals directly between themselves or to ground stations. The first such system to be completed, Iridium, uses 66 satellites and started operations in 1998. Iridium appears to have created particular difficulties for communications intelligence agencies, since the signals down from the Iridium and similar networks can only be received in a small area, which may be anywhere on the earth's surface.

# 3. ECHELON and Comint production

65. The ECHELON system became well known following publication of the previous STOA report. Since then, new evidence shows that ECHELON has existed since the 1970s, and was greatly enlarged between 1975 and 1995. Like ILC interception, ECHELON has developed from earlier methods. This section includes new information and documentary evidence about ECHELON and satellite interception.

## The "Watch List"

66. After the public revelation of the SHAMROCK interception programme, NSA Director Lt General Lew Allen described how NSA used '"watch lists" as an aid to watch for foreign activity of reportable intelligence interest".[41] "We have been providing details … of any messages contained in the foreign communications we intercept that bear on named individuals or organisations. These compilations of names are commonly referred to as 'Watch Lists'", he said.[42] Until the 1970s, Watch List processing was manual. Analysts examined intercepted ILC communications, reporting, "gisting" or analysing those which appeared to cover names or topics on the Watch List.

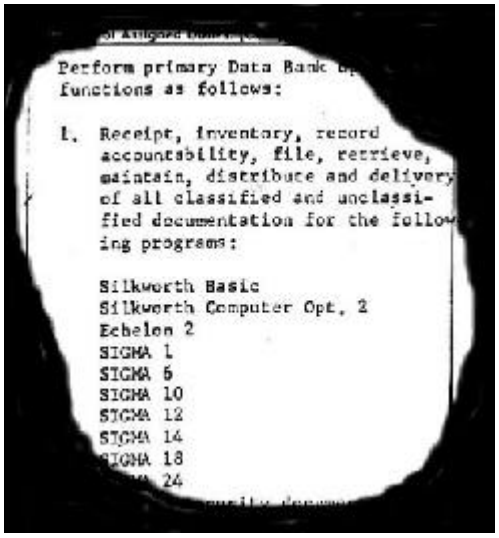
## New information about ECHELON sites and systems

67. It now appears that the system identified as ECHELON has been in existence for more than 20 years. The need for such a system was foreseen in the late 1960s, when NSA and GCHQ planned ILC satellite interception stations at Mowenstow and Yakima. It was expected that the quantity of messages intercepted from the new satellites would be too great for individual examination. According to former NSA staff, the first ECHELON computers automated Comint processing at these sites.[43]

68. NSA and CIA then discovered that Sigint collection from space was more effective than had been anticipated, resulting in accumulations of recordings that outstripped the available supply of linguists and analysts. Documents show that when the SILKWORTH processing systems was installed at Menwith Hill for the new satellites, it was supported by ECHELON 2 and other databanks (see illustration).

69. By the mid 1980s, communications intercepted at these major stations were heavily sifted, with a wide variety of specifications available for non-verbal traffic. Extensive further automation was planned in the mid 1980s as NSA Project P-415. Implementation of this project completed the automation of the previous Watch List activity. From 1987 onwards, staff from international Comint agencies travelled to the US to attended training courses for the new computer systems.

70. Project P-415/ECHELON made heavy use of NSA and GCHQ's global Internet-like communication network to enable remote intelligence customers to task computers at each collection site, and receive the results automatically. The key component of the system are local "Dictionary" computers, which store an extensive database on specified targets, including names, topics of interest, addresses, telephone numbers and other selection criteria. Incoming messages are compared to these criteria; if a match is found, the raw intelligence is forwarded automatically. Dictionary computers are tasked with many thousands of different collection requirements, described as "numbers" (four digit codes).


Perform primary Data Bank
functions as follows:

1. Receipt, inventory, record accountability, file, retrieve, maintain, distribute and delivery of all classified and unclassified documentation for the following programs:

Silkworth Basic
Silkworth Computer Opt. 2
Echelon 2
SIGMA 1
SIGMA 6
SIGMA 10
SIGMA 12
SIGMA 14
SIGMA 18
24

*List of intelligence databanks operating at Menwith Hill in 1979 included the second generation of ECHELON*

*ECHELON satellite interception site at Sugar Grove, West Virgina, showing 6 antenna targeted on European and Atlantic regional communications satellites (November 1998)*

71. Tasking and receiving intelligence from the Dictionaries involves processes familiar to anyone who has used the Internet. Dictionary sorting and selection can be compared to using search engines, which select web pages containing key words or terms and specifying relationships. The forwarding function of the Dictionary computers may be compared to e-mail. When requested, the system will provide lists of communications matching each criterion for review, analysis, "gisting" or forwarding. An important point about the new system is that before ECHELON, different countries and different stations knew what was being intercepted and to whom it was sent. Now, all but a fraction of the messages selected by Dictionary computers at remote sites are forwarded to NSA or other customers without being read locally.

### Westminster, London – Dictionary computer

72. In 1991, a British television programme reported on the operations of the Dictionary computer at GCHQ's Westminster, London office. The system "secretly intercepts every single telex which passes into, out of or through London; thousands of diplomatic, business and personal messages every day. These are fed into a programme known as `Dictionary'. It picks out keywords from the mass of Sigint, and hunts out hundreds of individuals and corporations".[44] The programme pointed out that the Dictionary computers, although controlled and tasked by GCHQ, were operated by security vetted staff employed by British Telecom (BT), Britain's dominant telecommunications operator.[45] The presence of Dictionary computers has also been confirmed at Kojarena, Australia; and at GCHQ Cheltenham, England.[46]

### Sugar Grove, Virginia – COMSAT interception at ECHELON site

73. US government documents confirm that the satellite receiving station at Sugar Grove, West Virginia is an ECHELON site, and that collects intelligence from COMSATs. The station is about 250 miles south-west of Washington, in a remote area of the Shenandoah Mountains. It is operated by the US Naval Security Group and the US Air Force Intelligence Agency.

74. An upgraded system called TIMBERLINE II, was installed at Sugar Grove in the summer of 1990. At the same time, according to official US documents, an "ECHELON training department" was established. [47] With training complete, the task of the station in 1991 became "to **maintain and operate an ECHELON site**". [48]

75. The US Air Force has publicly identified the intelligence activity at Sugar Grove: its "mission is to **direct satellite communications equipment [in support of] consumers of COMSAT information** ... This is achieved by providing a trained cadre of collection system operators, analysts and managers". [49] In 1990, satellite photographs showed that there were 4 satellite antennae at Sugar Grove. By November 1998, ground inspection revealed that this had expanded to a group of 9.

### Sabana Seca, Puerto Rico and Leitrim, Canada – COMSAT interception sites

76. Further information published by the US Air Force identifies the US Naval Security Group Station at Sabana Seca, Puerto Rico as a COMSAT interception site. Its mission is "to become the premier **satellite communications processing and analysis** field station". [50]

77. Canadian Defence Forces have published details about staff functions at the Leitrim field station of the Canadian Sigint agency CSE. The station, near Ottawa, Ontario has four satellite terminals, erected since 1984. The staff roster includes seven Communications Satellite Analysts, Supervisors and Instructors. [51]

78. In a publicly available resume, a former Communication Satellite Analyst employed at Leitrim describes his job as having required expertise in the "**operation and analysis of numerous Comsat computer systems and associated subsystems ... [utilising] computer assisted analysis systems ... [and] a broad range of sophisticated electronic equipment to intercept and study foreign communications and electronic transmissions**." [52] Financial reports from CSE also indicate that in 1995/96, the agency planned payments of $7 million to ECHELON and $6 million to Cray (computers). There were no further details about ECHELON. [53]

### Waihopai, New Zealand – Intelsat interception at ECHELON site

79. New Zealand's Sigint agency GCSB operates two satellite interception terminals at Waihopai, tasked on Intelsat satellites covering the Pacific Ocean. Extensive details have already been published about the station's Dictionary computers and its role in the ECHELON network. [54] After the book was published, a New Zealand TV station obtained images of the inside of the station operations centre. The pictures were obtained clandestinely by filming through partially curtained windows at night. The TV reporter was able to film close-ups of technical manuals held in the control centre. These were **Intelsat technical manuals**, providing confirmation that the station targeted these satellites Strikingly, the station was seen to be virtually empty, operating fully automatically. One guard was inside, but was unaware he was being filmed. [55]

## ILC processing techniques

80. The technical annexe describes the main systems used to extract and process communications intelligence. The detailed explanations given about processing methods are not essential to understanding the core of this report, but are provided so that readers knowledgeable about telecommunications may fully evaluate the state of the art.

81. Fax messages and computer data (from modems) are given priority in processing because of the ease with which they are understood and analysed. The main method of filtering and analysing non-verbal traffic, the Dictionary computers, utilise traditional information retrieval techniques, including keywords. Fast special purpose chips enable vast quantities of data to be processed in this way. The newest technique is "topic spotting". The processing of telephone calls is mainly limited to identifying call-related information, and traffic analysis. Effective voice "wordspotting" systems do not exist are not in use, despite reports to the contrary. But "voiceprint" type speaker identification systems have been in use since at least 1995. The use of strong cryptography is slowly impinging on Comint agencies' capabilities. This difficulty for Comint agencies has been offset by covert and overt activities which have subverted the effectiveness of cryptographic systems supplied from and/or used in Europe.

82. The conclusions drawn in the annexe are that Comint equipment currently available has the capability, as tasked, to intercept, process and analyse every modern type of high capacity communications system to which access is obtained, including the highest levels of the Internet. There are few gaps in coverage. The scale, capacity and speed of some systems is difficult fully to comprehend. Special purpose systems have been built to process pager messages, cellular mobile radio and new satellites.

# 4. Comint and Law Enforcement

83. In 1990 and 1991, the US government became concerned that the marketing of a secure telephone system by AT&T could curtail Comint activity. AT&T was persuaded to withdraw its product. In its place the US government offered NSA "Clipper" chips for incorporation in secure phones. The chips would be manufactured by NSA, which would also record built-in keys and pass this information to other government agencies for storage and, if required, retrieval. This proposal proved extremely unpopular, and was abandoned. In its place, the US government proposed that <u>non</u> government agencies should be required to keep copies of every user's keys, a system called "key escrow" and, later, "key recovery". Viewed in retrospect, the actual purpose of these proposals was to provide NSA with a single (or very few) point(s) of access to keys, enabling them to continue to access private and commercial communications.

## <u>Misrepresentation of law enforcement interception requirements</u>

84. Between 1993 to 1998, the United States conducted sustained diplomatic activity seeking to persuade EU nations and the OECD to adopt their "key recovery" system. Throughout this period, the US government insisted that the purpose of the initiative was to assist law enforcement agencies. Documents obtained for this study suggest that these claims wilfully misrepresented the true intention of US policy. Documents obtained under the US Freedom of Information Act indicate that policymaking was led exclusively by NSA officials, sometimes to the complete exclusion of police or judicial officials. For example, when the specially appointed US "Ambassador for Cryptography", David Aaron, visited Britain on 25 November 1996, he was accompanied and briefed by NSA's most senior representative in Britain, Dr James J Hearn, formerly Deputy Director of NSA. Mr Aaron had did not meet or consult FBI officials attached to his Embassy. His meeting with British Cabinet officials included NSA's representative and staff from Britain's GCHQ, but police officers or justice officials from both nations were excluded.

85. Since 1993, unknown to European parliamentary bodies and their electors, law enforcement officials from many EU countries and most of the UKUSA nations have been meeting annually in a separate forum to discuss their requirements for intercepting communications. These officials met under the auspices of a hitherto unknown organisation, ILETS (International Law Enforcement Telecommunications Seminar). ILETS was initiated and founded by the FBI. Table 2 lists ILETS meetings held between 1993 and 1997.

86. At their 1993 and 1994 meetings, ILETS participants specified law enforcement user requirements for communications interception. These appear in a 1974 ILETS document called "IUR 1.0". This document was based on an earlier FBI report on "Law Enforcement Requirements for the Surveillance of Electronic Communications", first issued in July 1992 and revised in June 1994. The IUR requirement differed little in substance from the FBI's requirements but was enlarged, containing ten requirements rather than nine. **IUR did not specify <u>any</u> law enforcement need for "key escrow" or "key recovery".** Cryptography was mentioned solely in the context of network security arrangements.

87. Between 1993 and 1997 police representatives from ILETS were not involved in the NSA-led policy making process for "key recovery", nor did ILETS advance any such proposal, even as late as 1997. Despite this, during the same period the US government repeatedly presented its policy as being motivated by the stated needs of law enforcement agencies. At their 1997 meeting in Dublin, ILETS did not alter the IUR. It was not until 1998 that a revised IUR was prepared containing requirements in respect of cryptography. It follows from this that the US government misled EU and OECD states about the true intention of its policy.

88. This US deception was, however, clear to the senior Commission official responsible for information security. In September 1996, David Herson, head of the EU Senior Officers' Group on Information Security, stated his assessment of the US "key recovery" project :

*"'Law Enforcement' is a protective shield for all the other governmental activities … We're talking about foreign intelligence, that's what all this is about. There is no question [that] 'law enforcement' is a smoke screen".*[56]

89. It should be noted that technically, legally and organisationally, law enforcement requirements for communications interception differ fundamentally from communications intelligence. Law enforcement agencies (LEAs) will normally witsh to intercept a specific line or group of lines, and must normally justify their requests to a judicial or administrative authority before proceeding. In contract, Comint agencies conduct broad international communications "trawling" activities, and operate under general warrants. Such operations do not require or even suppose that the parties they intercept are criminals. Such distinctions are vital to civil liberty, but risk being eroded it the boundaries between law enforcement and communications intelligence interception becomes blurred in future.

| *Year* | *Venue* | *Non-EU participants* | *EU participants* |
|---|---|---|---|
| 1993 | Quantico, Virginia, USA | Australia, Canada, Hong Kong, Norway United States | Denmark, France, Germany, Netherlands, Spain, Sweden, United Kingdom |
| 1994 | Bonn, Germany | Australia, Canada, Hong Kong, Norway, United States | Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom |
| 1995 | Canberra, Australia | Australia, Canada, Hong Kong, New Zealand, Norway, United States | Belgium, France, Germany, Greece, Ireland, Italy, Netherlands, Spain, Sweden, United Kingdom |
| 1997 | Dublin, Ireland | Australia, Canada, Hong Kong, New Zealand, Norway, United States | Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom |

*Table 2 ILETS meetings, 1993-1997*

### Law enforcement communications interception – policy development in Europe

90. Following the second ILETS meeting in Bonn in 1994, IUR 1.0 was presented to the Council of Ministers and was passed without a single word being altered on 17January 1995.[57] During 1995, several non EU members of the ILETS group wrote to the Council to endorse the (unpublished) Council resolution. The resolution was not published in the Official Journal for nearly two years, on 4 November 1996.

91. Following the third ILETS meeting in Canberra in 1995, the Australian government was asked to present the IUR to International Telecommunications Union (ITU). Noting that "law enforcement and national security agencies of a significant number of ITU member states have agreed on a generic set of requirements for legal interception", the Australian government asked the ITU to advise its standards bodies to incorporate the IUR requirements into future telecommunications systems on the basis that the "costs of [providing] legal interception capability and associated disruptions can be lessened by providing for that capability at the design stage".[58]

92. It appears that ILETS met again in 1998 and revised and extended its terms to cover the Internet and Satellite Personal Communications Systems such as Iridium. The new IUR also specified "additional security requirements for network operators and service providers", extensive new requirements for personal information about subscribers, and provisions to deal with cryptography.

93. On 3 September 1998, the revised IUR was presented to the Police Co-operation Working Group as ENFOPOL 98. The Austrian Presidency proposed that, as in 1994, the new IUR be adopted verbatim as a Council Resolution on interception "in respect of new technology".[59] The group did not agree. After repeated redrafting, a fresh paper has been prepared by the German Presidency, for the eventual consideration of Council Home and Justice ministers.[60]

# 5. Comint and economic intelligence

94. During the 1998 EP debate on "Transatlantic relations/ECHELON system" Commissioner Bangeman observed on behalf of the Commission that "If this system were to exist, it would be an intolerable attack against individual liberties, competition and the security of the states".[61] The existence of ECHELON was described in section 3, above. This section describes the organisational and reporting frameworks within which economically sensitive information collected by ECHELON and related systems is disseminated, summarising examples where European organisations have been the subject of surveillance.

## Tasking economic intelligence

95. US officials acknowledge that NSA collects economic information, whether intentionally or otherwise. Former military intelligence attaché Colonel Dan Smith worked at the US Embassy, London until 1993. He regularly received Comint product from Menwith Hill. In 1998, he told the BBC that at Menwith Hill:

> *"In terms of scooping up communications, inevitably since their take is broadband, there will be conversations or communications which are intercepted which have nothing to do with the military, and probably within those there will be some information about commercial dealings"*
>
> *"Anything would be possible technically. Technically they can scoop all this information up, sort through it and find out what it is that might be asked for . . . But there is not policy to do this specifically in response to a particular company's interest*[62]

96. In general, this statement is not incorrect. But it overlooks fundamental distinctionS between tasking and dissemination, and between commercial and economic intelligence. There is no evidence that companies in any of the UKUSA countries are able to task Comint collection to suit their private purposes. They do not have to. Each UKUSA country authorises national level intelligence assessment organisations and relevant individual ministries to task and receive economic intelligence from Comint. Such information may be collected for myriad purposes, such as: estimation of future essential commodity prices; determining other nation's private positions in trade negotiations; monitoring international trading in arms; tracking sensitive technology; or evaluating the political stability and/or economic strength of a target country. Any of these targets and many others may produce intelligence of direct commercial relevance. The decision as to whether it should be disseminated or exploited is taken not by Comint agencies but by national government organisation(s).

## Disseminating economic intelligence

97. In 1970, according to its former Executive Director, the US Foreign Intelligence Advisory Board recommended that "henceforth economic intelligence be considered a function of the national security, enjoying a priority equivalent to diplomatic, military, technological intelligence".[63] On 5 May 1977, a meeting between NSA, CIA and the Department of Commerce authorised the creation of secret new department, the "Office of Intelligence Liaison". Its task was to handle "foreign intelligence" of interest to the Department of Commerce. Its standing orders show that it was authorised to receive and handle SCI intelligence – Comint and Sigint from NSA. The creation of this office THUS provided a formal mechanism whereby NSA data could be used to support commercial and economic interests. After this system was highlighted in a British TV programme in 1993, its name was changed to the "Office of Executive Support".[64] Also in 1993, President Clinton extended US intelligence support to commercial organisations by creating a new National Economic Council, paralleling the National Security Council.

98. The nature of this intelligence support has been widely reported. "Former intelligence officials and other experts say tips based on spying … regularly flow from the Commerce Department to U.S. companies to help them win contracts overseas.[65] The Office of Executive Support provides classified weekly briefings to security officials. One US newspaper obtained reports from the Commerce Department demonstrating intelligence support to US companies:

> *One such document consists of minutes from an August 1994 Commerce Department meeting [intended] to identify major contracts open for bid in Indonesia in order to help U.S. companies win the work. A CIA employee … spoke at the meeting; five of the 16 people on the routine distribution list for the minutes were from the CIA.*

99. In the United Kingdom, GCHQ is specifically required by law (and as and when tasked by the British government) to intercept foreign communications "in the interests of the economic well-being of the United Kingdom ...in relation to the actions or intentions of persons outside the British Islands". Commercial interception is tasked and analysed by GCHQ's K Division. Commercial and economic targets can be specified by the government's Overseas Economic Intelligence Committee, the Economic Staff of the Joint Intelligence Committee, the Treasury, or the Bank of England.[66] According to a former senior JIC official, the Comint take routinely includes "company plans, telexes, faxes, and transcribed phone calls. Many were calls between Europe and the South[ern Hemisphere]".[67]

100. In Australia, commercially relevant Comint is passed by DSD to the Office of National Assesments, who consider whether, and if so where, to disseminate it. Staff there may pass information to Australian companies if they believe that an overseas nation has or seeks an unfair trade advantage. Targets of such activity have included Thomson-CSF, and trade negotiations with Japanese purchasers of coal and iron ore. Similar systems operate in the other UKUSA nations, Canada and New Zealand.

## The use of Comint economic intelligence product

### Panavia European Fighter Aircraft consortium and Saudi Arabia

101. In 1993, former National Security Council official Howard Teicher described in a programme about Menwith Hill how the European Panavia company was specifically targeted over sales to the Middle East. "I recall that the words 'Tornado' or 'Panavia' - information related to the specific aircraft - would have been priority targets that we would have wanted information about".[68]

### Thomson CSF and Brazil

102. In 1994, NSA intercepted phone calls between Thomson-CSF and Brazil concerning SIVAM, a $1.3 billion surveillance system for the Amazon rain forest. The company was alleged to have bribed members of the Brazilian government selection panel. The contract was awarded to the US Raytheon Corporation - who announced afterwards that "the Department of Commerce worked very hard in support of U.S. industry on this project".[69] Raytheon also provide maintenance and engineering services to NSA's ECHELON satellite interception station at Sugar Grove.

### Airbus Industrie and Saudi Arabia

103. According to a well-informed 1995 press report :"from a commercial communications satellite, NSA lifted all the faxes and phone calls between the European consortium Airbus, the Saudi national airline and the Saudi government. The agency found that Airbus agents were offering bribes to a Saudi official. It passed the information to U.S. officials pressing the bid of Boeing Co and McDonnell Douglas Corp., which triumphed last year in the $6 billion competition." [70]

### International trade negotiations

104. Many other accounts have been published by reputable journalists and some firsthand witnesses citing frequent occasions on which the US government has utlitised Comint for national commercial purposes. These include targeting data about the emission standards of Japanese vehicles;[71] 1995 trade negotiations the import of Japanese luxury cars;[72] French participation in the GATT trade negotiations in 1993; the Asian-Pacific Economic Conference (APEC), 1997.

### Targeting host nations

105. The issue of whether the United States utilises communications intelligence facilities such as Menwith Hilll or Bad Aibling to attack host nations' communications also arises. The available evidence suggests that such conduct may normally be avoided. According to former National Security Council official Howard Teicher, the US government would not direct NSA to spy on a host governments such as Britain:

> *"[But] I would never say never in this business because, at the end of the day, national interests are national interests … sometimes our interests diverge. So never say never - especially in this business".*

# 6. Comint capabilities after 2000

## Developments in technology

106. Since the mid-1990s, communications intelligence agencies have faced substantial difficulties in maintaining global **access** to communications systems. These difficulties will increase during and after 2000. The major reason is the shift in telecommunications to high capacity optical fibre networks. Physical access to cables is required for interception. Unless a fibre network lies within or passes through a collaborating state, effective interception is practical only by tampering with optoelectronic repeaters (when installed). This limitation is likely to place many foreign land-based high capacity optical fibre networks beyond reach. The physical size of equipment needed to process traffic, together with power, communications and recording systems, makes clandestine activity impractical and risky.

107. Even where access is readily available (such as to COMSATs), the proliferation of new systems will limit **collection** activities, partly because budgetary constraint will restrict new deployments, and partly because some systems (for example, Iridium) cannot be accessed by presently available systems.

108. In the past 15 years the substantial technological lead in computers and information technology once enjoyed by Comint organisations has all but disappeared. Their principal computer systems are bought "off the shelf" and are the equal of or even inferior to those used by first rank industrial and academic organisations. They differ only in being "TEMPEST shielded", preventing them emitting radio signals which could be used to analyse Sigint activity.

109. Communications intelligence organisations recognise that the long war against civil and commercial cryptography has been lost. A thriving academic and industrial community is skilled in cryptography and cryptology. The Internet and the global marketplace have created a free flow in information, systems and software. NSA has failed in its mission to perpetuate access by pretending that that "key escrow" and like systems were intended to support law enforcement (as opposed to Comint) requirements.

110. Future trends in Comint are likely to include limits on investment in Comint collection from space; greater use of human agents to plant collection devices or obtain codes than in the past; and an intensified effort to attack foreign computer systems, using the Internet and other means (in particular, to gain access to protected files or communications before they are encrypted).

111. Attempts to restrict cryptography have nevertheless delayed the large-scale introduction of effective cryptographic security systems. The reduced cost of computational power has also enabled Comint agencies to deploy fast and sophisticated processing and sorting tools.

112. Recent remarks to CIA veterans by the head of staff of the US House of Representatives Permanent Select Committee on Intelligence, ex CIA officer John Millis illustrate how NSA views the same issues:

> *"Signals intelligence is in a crisis. … Over the last fifty years ... In the past, technology has been the friend of NSA, but in the last four or five years technology has moved from being the friend to being the enemy of Sigint.*
>
> *The media of telecommunications is no longer Sigint-friendly. It used to be. When you were doing RF signals, anybody within range of that RF signal could receive it just as clearly as the intended recipient. We moved from that to microwaves, and people figured out a great way to harness that as well. Well, we're moving to media that are very difficult to get to.*
>
> *Encryption is here and it's going to grow very rapidly. That is bad news for Sigint … It is going to take a huge amount of money invested in new technologies to get access and to be able to break out the information that we still need to get from Sigint".*

# Policy issues for the European Parliament

1. The 1998 Parliamentary resolution on "Transatlantic relations/ECHELON system" [73] called for "protective measures concerning economic information and effective encryption". Providing such measures may be facilitated by developing an in-depth understanding of present and future Comint capabilities.

2. At the technical level, protective measures may best be focused on defeating hostile Comint activity by denying access or, where this is impractical or impossible, preventing processing of message content and associated traffic information by general use of cryptography.

3. As the SOGIS group within the Commission has recognised, [74] the contrasting interests of states is a complex issue. Larger states have made substantial investments in Comint capabilities. One member state is active in the UKUSA alliance, whilst others are either "third parties" to UKUSA or have made bilateral arrangements with NSA. Some of these arrangements were a legacy of the cold war; others are enduring. These issues create internal and international conflicts of interest. Technical solutions are not obvious. It should be possible to define a shared interest in implementing measures to defeat future external Comint activities directed against European states, their citizens and commercial activities.

4. A second area of apparent conflict concerns states' desires to provide communications interception for legitimate law enforcement purposes. The technical and legal processes involved in providing interception for law enforcement purpose differ fundamentally from those used in communications intelligence. Partly because of the lack of parliamentary and public awareness of Comint activities, this distinction is often glossed over, particularly by states that invest heavily in Comint. Any failure to distinguish between legitimate law enforcement interception requirements and interception for clandestine intelligence purposes raises grave issues for civil liberties. A clear boundary between law enforcement and "national security" interception activity is essential to the protection of human rights and fundamental freedoms.

5. At the present time, Internet browsers and other software used in almost every personal computer in Europe is deliberately disabled such that "secure" communications they send can, if collected, be read without difficulty by NSA. US manufacturers are compelled to make these arrangements under US export rules. A level playing field is important. Consideration could be given to a countermeasure whereby, if systems with disabled cryptographic systems are sold outside the United States, they should be required to conform to an "open standard" such that third parties and other nations may provide additional applications which restore the level of security to at least enjoyed by domestic US customers.

6. The work of ILETS has proceeded for 6 years without the involvement of parliaments, and in the absence of consultation with the industrial organisations whose vital interests their work affects. It is regrettable that, prior to the publication of this report, public information has not been available in states about the scope of the policy-making processes, inside and outside the EU, which have led to the formulation of existing and new law enforcement "user requirements". As a matter of urgency, the current policy-making process should be made open to public and parliamentary discussion in member states and in the EP, so that a proper balance may be struck between the security and privacy rights of citizens and commercial enterprises, the financial and technical interests of communications network operators and service providers, and the need to support law enforcement activities intended to suppress serious crime and terrorism.

# Technical annexe

## Broadband (high capacity multi-channel) communications

1. From 1950 until the early 1980s, high capacity multi-channel analogue communications systems were usually engineered using separate communications channels carried at different frequencies The combined signal, which could include 2,000 or more speech channels, was a "multiplex". The resulting "frequency division multiplex" (FDM) signal was then carried on a much higher frequency, such as by a microwave radio signal.

2. Digital communications have almost universally taken over from analogue methods. The basic system of digital multi-channel communications is time division multiplexing (TDM). In a TDM telephony system, the individual conversational channels are first digitised. Information concerning each channel is then transmitted sequentially rather than simultaneously, with each link occupying successive time "slots".

3. Standards for digital communications evolved separately within Europe and North America. In the United States, the then dominant public network carrier (the Bell system, run by AT&T) established digital data standards. The basic building block, a T-1 link, carries the equivalent of 24 telephone channels at a rate of 1.544 Mbps. Higher capacity systems operate at greater data transmission rates Thus, the highest transmission rate, T-5, carries the equivalent of 8,000 speech channels at a data rate of 560 Mbps.

4. Europe adopted a different framework for digital communications, based on standards originally agreed by the CEPT. The basic European standard digital link, E-1, carries 30 telephone channels at a data rate of 2 Mbps. Most European telecommunications systems are based on E-1 links or (as in North America), multiples thereof. The distinction is significant because most Comint processing equipment manufactured in the United States is designed to handle intercepted communications working to the European forms of digital communications.

5. Recent digital systems utilise synchronised signals carried by very high capacity optical fibres. Synchronising signals enables single channels to be easily extracted from high capacity links. The new system is known in the US as the synchronous optical network (SONET), although three equivalent definitions and labels are in use.[75]

## Communications intelligence equipment

6. Dozens of US defence contractors, many located in Silicon Valley (California) or in the Maryland "Beltway" area near Washington, manufacture sophisticated Sigint equipment for NSA. Major US corporations, such as Lockheed Martin, Space Systems/Loral, TRW, Raytheon and Bendix are also contracted by NSA to operate major Sigint collection sites. A full report on their products and services is beyond the scope of this study. The state of the art in contemporary communications intelligence may usefully be demonstrated, however, by examining some of the Comint processing products of two specialist NSA niche suppliers: Applied Signal Technology Inc (AST), of Sunnyvale, California, and The IDEAS Operation of Columbia, Maryland (part of Science Applications International Corporation (SAIC)).[76]

7. Both companies include senior ex-NSA staff as directors. When not explicitly stated, their products can be identified as intended for Sigint by virtue of being "TEMPEST screened". AST states generally that its "equipment is used for signal reconnaissance of foreign telecommunications by the United States government". One leading cryptographer has aptly and and engagingly described AST as a "one-stop ECHELON shop".

### Wideband extraction and signal analysis

8. Wideband (or broadband) signals are normally intercepted from satellites or tapped cables in the form of multiplex microwave or high frequency signals. The first step in processing such signals for Comint purposes is "**wideband extraction**". An extensive range of Sigint equipment is manufactured for this purpose, enabling newly intercepted systems to be surveyed and analysed. These include transponder survey equipment which identify and classify satellite downlinks, demodulators, decoders, demultiplexers, microwave radio link analysers, link survey units, carrier analysis systems, and many other forms of hardware and software.

9. A newly intercepted communications satellite or data link can be analysed using the AST Model 196 "Transponder characterisation system". Once its basic communications structure has been analysed, the Model 195 "Wideband snapshot analyser", also known as SNAPPER, can record sample data from even the highest capacity systems, sufficient to analyse communications in minute detail. By the start of 1999, operating in conjunction with the Model 990 "Flexible Data Acquisition Unit", this systems was able to record,

playback and analyse at data rates up to 2.488 Gbps (SONET OC-48). This is 16 times faster than the largest backbone links in general use on the Internet; larger than the telephony capacity of any current communications satellite; and equivalent to 40,000 simultaneous telephone calls. It can be fitted with 48 Gbyte of memory (500-1000 times larger than found in an average personal computer), enabling relatively lengthy recordings of high-speed data links. The 2.5 Gbps capacity of a single SNAPPER unit exceeds the current daily maximum data rate found on a typical large Internet exchange.[77]

10. Both AST and IDEAS offer a wide range of recorders, demultiplexers, scanners and processors, mostly designed to process European type (CEPT) E-1, E-3 (etc) signals at data rates of up to 160 Mbps. Signals may be recorded to banks of high-speed tape recorders, or into high capacity "RAID"[78] hard disk networks. Intercepted optical signals can be examined with the AST Model 257E "SONET analyser".

11. Once communications links have been analysed and broken down to their constituent parts, the next stage of Comint collection involves multi-channel processors which extract and filter messages and signals from the desired channels. There are three broad categories of interest: "voice grade channels", normally carrying telephony; fax communications; and analogue data modems. A wide selection of multi-channel Comint processors are available. Almost all of them separate voice, fax and data messages into distinct "streams" for downstream processing and analysis.

12. The AST Model 120 multi-channel processor – used by NSA in different configurations known as STARQUAKE, COBRA and COPPERHEAD - can handle 1,000 simultaneous voice channels and automatically extract fax, data and voice traffic. Model 128, larger still, can process 16 European E-3 channels (a data rate of 500 Mbps) and extract 480 channels of interest. The 1999 giant of AST's range, the Model 132 "Voice Channel Demultiplexer", can scan up to 56,700 communications channels, extracting more than 3,000 voice channels of interest. AST also provides Sigint equipment to intercept low capacity VSAT[79] satellite services used by smaller businesses and domestic users. These systems can be intercepted by the AST Model 285 SCPS processor, which identifies and extracts up to 48 channels of interest, distinguished between voice, fax and data.

13. According to US government publications, an early Wideband Extraction system was installed at NSA's Vint Hill Farms field station in 1970, about the time that systematic COMSAT interceptio collection began. That station is now closed. US publications identify the NSA/CSS Regional Sigint Operations Centre at San Antonio, Texas, as a site currently providing a multi-channel Wideband Extraction service.

### Filtering, data processing, and facsimile analysis

14. Once communications channels have been identified and signals of interest extracted, they are analysed further by sophisticated workstations using special purpose software. AST's ELVIRA Signals Analysis Workstation is typical of this type of Sigint equipment. This system, which can be used on a laptop computer in covert locations, surveys incoming channels and extracts standard Comint data, including technical specifications (STRUM) and information about call destinations (SRI, or signal related information). Selected communications are relayed to distant locations using NSA standard "Collected Signals Data Format" (CSDF).[80]

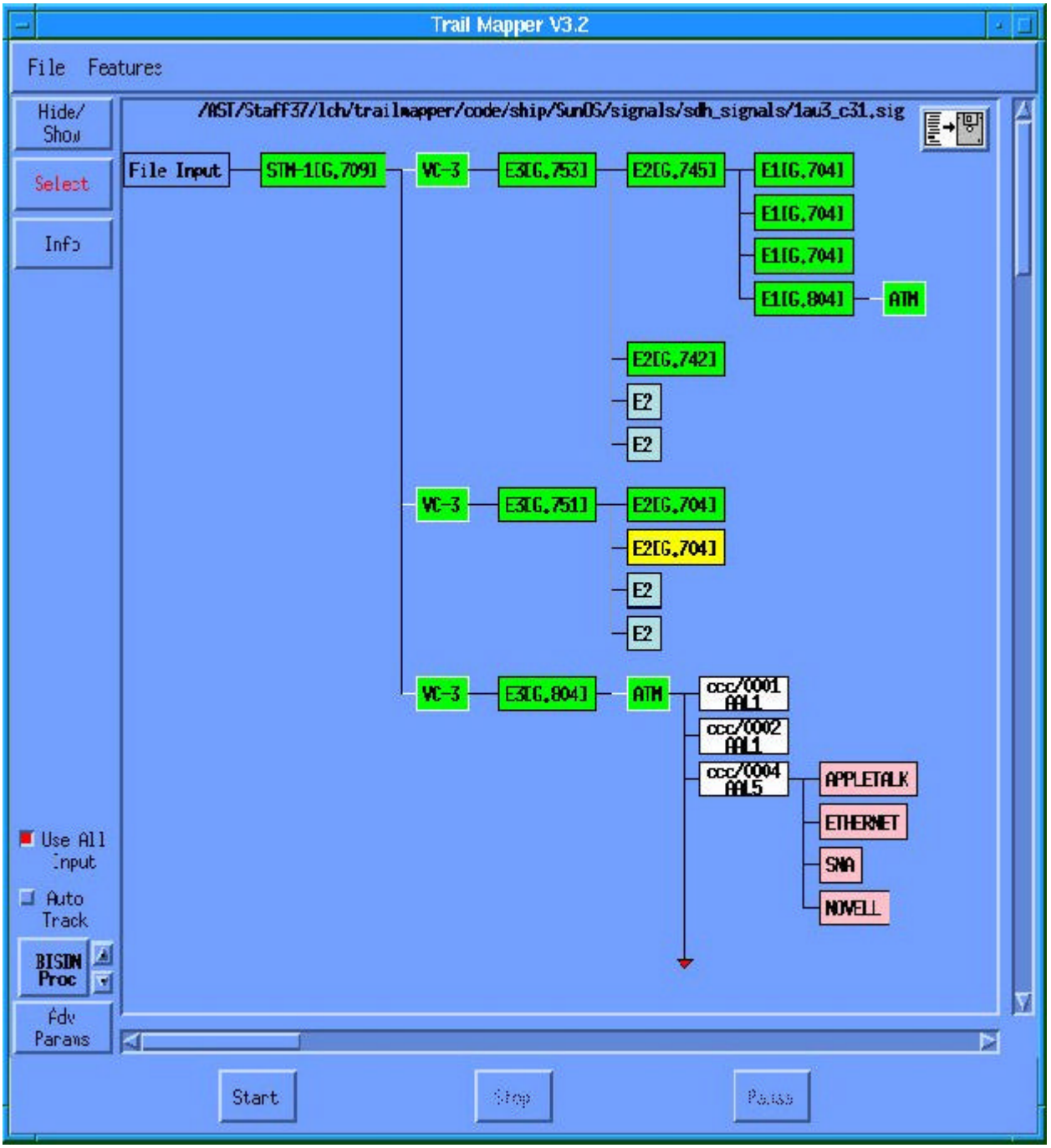
15. High-speed data systems can also be passed to AST's TRAILMAPPER software system, which works at a data rate of up to 2.5 Gbps. It can interpret and analyse every type of telecommunications system, including European, American and optical standards. TRAILMAPPER appears to have been designed with a view to analysing ATM (asynchronous transfer mode) communications. ATM is a modern, high-capacity digital communications system. It is better suited than standard Internet connections to carrying multimedia traffic and to providing business with private networks (VPN, LAN or WAN). TRAILMAPPER will identify and characterise such business networks.

16. In the next stage downstream, intercepted signals are processed according to whether they are voice, fax or data. AST's "Data Workstation" is designed to categorise all aspects of data communications, including systems for handling e-mail or sending files on the Internet.[81] Although the very latest modem systems (other than ISDN) are not included in its advertised specification, it is clear from published research that AST has developed the technology to intercept and process the latest data communications systems used by individuals and business to access the Internet.[82] The Data Workstation can stored and automatically process 10,000 different recorded signals.

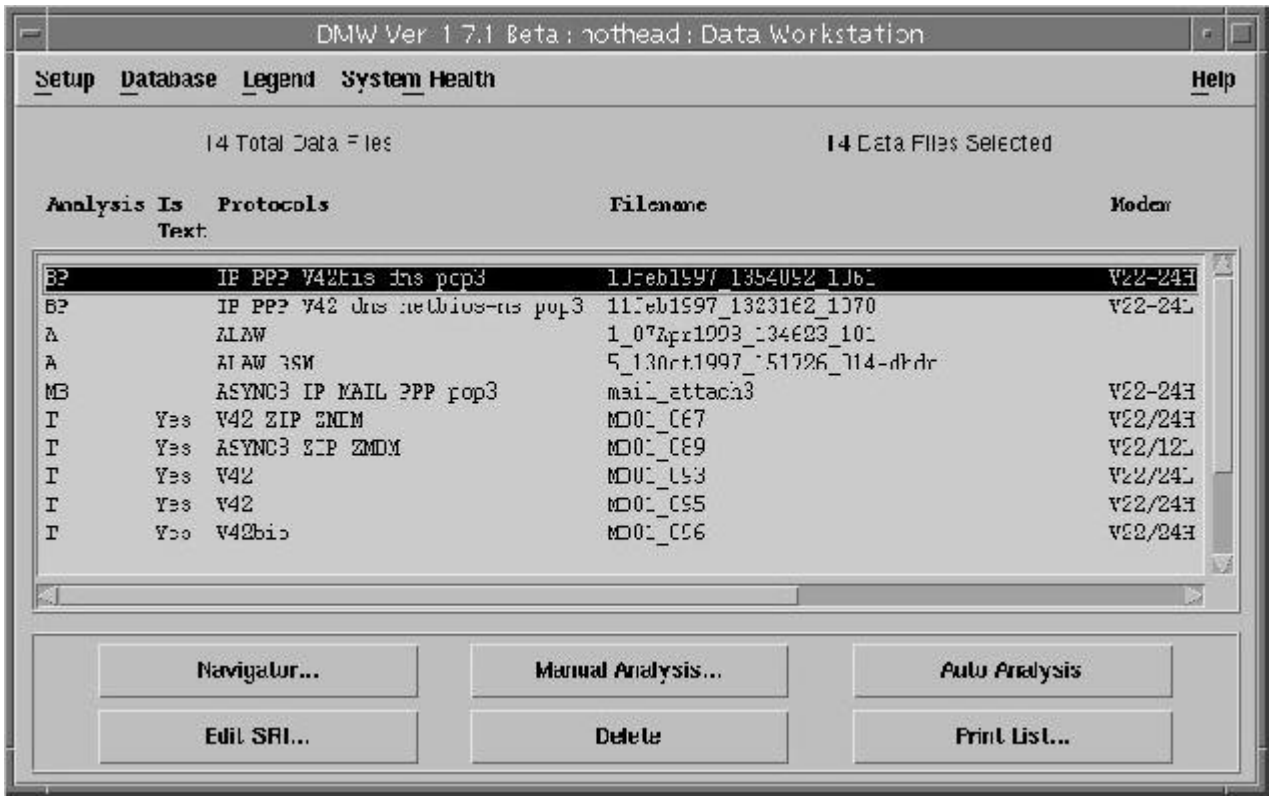
17. Fax messages are processed by AST's Fax Image Workstation. This is described as a "user friendly, interactive analysis tool for rapid examination images stored on disk. Although not mentioned in AST's literature, standard fax pre-processing for Dictionary computers involves automatic "optical character

recognition" (OCR) software. This turns the typescript into computer readable (and processable) text. The effectiveness of these systems makes fax-derived Comint an important collection subsystem. It has one drawback. OCR computer systems that can reliably recognise handwriting do not exist. No one knows how to design such a system. It follows that, perversely, hand-written fax messages may be a secure form of communication that can evade Dictionary surveillance criteria, provided always that the associated "signal related information" (calling and receiving fax numbers) have not been recognised as being of interest and directed to a Fax Image Workstation.

18. AST also make a "Pager Identification and Message Extraction" system which automatically collects and processes data from commercial paging systems. IDEAS offer a Video Teleconferencing Processor that can simultaneously view or record two simultaneous teleconferencing sessions. Sigint systems to intercept cellular mobile phone networks such as GSM are not advertised by AST or IDEAS, but are available from other US contractors. The specifications and ready availability of such systems indicate how industrialised and pervasive Comint has became. It has moved far from the era when (albeit erroneously), it was publicly associated only with monitoring diplomatic or military messages.




*NSA "Trailmapper" software showing automatic detection of private networks inside intercepted high capacity STM-1 carrier*




*The "Data Workstation" software system analyses up to 10,000 recorded messages, identifying Internet traffic, e-mail messages and attachments*

### Traffic analysis, keyword recognition, text retrieval, and topic analysis

19. Traffic analysis is a method of obtaining intelligence from signal related information, such as the number dialled on a telephone call, or the Calling Line Identification Data (CLID) which identifies the person making the call. Traffic analysis can be used where message content is not available, for example when encryption is used. By analysing calling patterns, networks of personal associations may be analysed and studied. This is a principal method of examining voice communications.

20. Whenever machine readable communications are available, keyword recognition is fundamental to Dictionary computers, and to the ECHELON system. The Dictionary function is straightforward. Its basic mode of operation is akin to web search engines. The differences are of substance and of scale. Dictionaries implement the tasking of their host station against the entire mass of collected communications, and automate the distribution of selected raw product.

21. Advanced systems have been developed to perform very high speed sorting of large volumes of intercepted information. In the late 1980s, the manufacturers of the RHYOLITE Sigint satellites, TRW, designed and manufactured a Fast Data Finder (FDF) microchip for NSA. The FDF chip was declassified in 1972 and made available for commercial use by a spin-off company, Paracel. Since then Paracel has sold over 150 information filtering systems, many of them to the US government. Paracel describes its current FDF technology as the "fastest, most accurate adaptive filtering system in the world":

> *A single TextFinder application may involve trillions of bytes of textual archive and thousands of online users, or gigabytes of live data stream per day that are filtered against tens of thousands of complex interest profiles … the TextFinder chip implements the most comprehensive character-string comparison functions of any text retrieval system in the world.*

Devices like this are ideal for use in ECHELON and the Dictionary system.

22. A lower capacity system, the PRP-9800 Pattern Recognition Processor, is manufactured by IDEAS. This is a computer card which can be fitted to a standard PC. It can analyse data streams at up to 34 Mbps (the European E-3 standard), matching every single bit to more than 1000 pre-selected patterns.

23. Powerful though Dictionary methods and keyword search engines may be, however, they and their giant associated intelligence databases may soon seem archaic. **Topic analysis** is a more powerful and intuitive technique, and one that NSA is developing and promoting with confidence. Topic analysis enables Comint customers to ask their computers to "find me documents about subject X". X might be "Shakespeare in love" or "Arms to Iran".

24. In a standard US test used to evaluate topic analysis systems,[83] one task the analysis program is given is to find information about "Airbus subsidies". The traditional approach involves supplying the computer with the key terms, other relevant data, and synonyms. In this example, the designations A-300 or A-320 might be synonymous with "Airbus". The disadvantage of this approach is that it may find irrelevant intelligence (for example, reports about export subsidies to goods flown on an Airbus) and miss relevant material (for example a financial analysis of a company in the consortium which does not mention the Airbus product by name). Topic analysis overcomes this and is better matched to human intelligence.

25. The main detectable thrust of NSA research on topic analysis centres on a method called N-gram analysis. Developed inside NSA's Research group - responsible for Sigint automation - N-gram analysis is a fast, general method of sorting and retrieving machine-readable text according to language and/or topic. The N-gram system is claimed to work independently of the language used or the topic studied. NSA patented the method in 1995.[84]

26. To use N-gram analysis, the operator ignores keywords and defines the enquiry by providing the system with selected written documents concerning the topic of interest. The system determines what the topic is from the seed group of documents, and then calculates the probability that other documents cover the same topic. In 1994, NSA made its N-gram system available for commercial exploitation. NSA's research group claimed that it could be used on "very large data sets (millions of documents)", could be quickly implemented on any computer system and that it could operate effectively "in text containing a great many errors (typically 10-15% of all characters)".

27. According to former NSA Director William Studeman, "information management will be the single most important problem for the (US) Intelligence Community" in the future.[85] Explaining this point in 1992, he described the type of filtering involved in systems like ECHELON:

> *One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report Is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.*

### Speech recognition systems

28. For more than 40 years, NSA, ARPA, GCHQ and the British government Joint Speech Research Unit have conducted and sponsored research into speech recognition. Many press reports (and the previous STOA report) have suggested that such research has provided systems which can automatically select telephone communications of intelligence interest based on the use of particular "key words" by a speaker. If available, such systems would enable vastly more extensive Comint information to be gathered from telephone conversations than is available from other methods of analysis. The contention that telephone word-spotting systems are readily available appears to by supported by the recent availability of a string of low-cost software products resulting from this research. These products permit PC users to dictate to their computers instead of entering data through the keyboard. [86]

29. The problem is that for Comint applications, unlike personal computer dictation products, speech recognition systems have to operate in a multi-speaker, multi-language environment where numerous previously never heard speakers may each feature physiological differences, dialect variations, and speech traits. Commercial PC systems usually require one or more hours of training in order reliably to recognise a single speaker. Even then, such systems may mistranscribe 10% or more of the words spoken.

30. In PC dictation applications, the speaker can correct mistranscriptions and continually retrain the recognition system, making a moderate error rate acceptable. For use in Comint, where the interception system has no prior knowledge of what has been said (or even the language in use), and has to operate in the poorer signal environment of a telephone speech channel, such error rates are unachievable. Worse still, even moderate error rates can make a keyword recognition system worthless by generating both false positive outputs (words wrongly identified as keywords) and false negative outputs (missing genuine keywords).

31. This study has found no evidence that voice keyword recognition systems are currently operationally deployed, nor that they are yet sufficiently accurate to be worth using for intelligence purposes.

### Continuous speech recognition

32. The fundamental technique in many speech recognition applications is a statistical method called Hidden Markov Modelling (HMM). HMM systems have been developed at many centres and are claimed academically to offer "good word spotting performance … using very little or no acoustic speech training".[87] The team which reported this result tested its system using data from the US Department of Defense "Switchboard Data", containing recordings of thousand of different US telephone conversations. On a limited test the probabilities of correctly detecting the occurrences of 22 keywords ranged from 45-68% on settings which allowed for 10 false positive results per keyword per hour. Thus if 1000 genuine keywords appeared during an hour's conversation, there would be at least 300 missed key words, plus 220 false alarms.

33. At about the same time, (February 1990), the Canadian Sigint organisation CSE awarded a Montreal-based computer research consultancy the first of a series of contracts to develop a Comint wordspotting system.[88] The goal of the project was to build a word-spotter that worked well even for noisy calls. Three years later, CRIM reported that "our experience has taught us that, regardless of the environmental conditions, wordspotting remains a difficult problem". The key problem, which is familiar to human listeners, is that a single word heard on its own can easily be misinterpreted, whereas in continuous speech the meaning may be deduced from surrounding words. CRIM concluded in 1993 that "it is probable that the most effective way of building a reliable wordspotter is to build a large vocabulary continuous speech recognition (CSR) system".

34. Continuous speech recognition software working in real time needs a powerful fast, processor. Because of the lack of training and the complex signal environment found in intercepted telephone calls, it is likely that even faster processors and better software than used in modern PCs would yield poorer results than are now provided by well-trained commercial systems. Significantly, an underlying problem is that voice keyword recognition is, as with machine-readable messages, an imperfect means to the more useful intelligence goal - **topic spotting**.

35. In 1993, having failed to build a workable wordspotter, CRIM suggesting "bypassing" the problem and attempting instead to develop a voice topic spotter. CRIM reported that "preliminary experiments reported at a recent meeting of American defense contractors … indicate that this may in fact be an excellent approach to the problem". They offered to produce an "operational topic spotting" system by 1995. They did not succeed. Four years later, they were still experimenting on how to built a voice topic spotter.[89] They received a further research contract. One method CRIM proposed was NSA's N-gram technique.

### Speaker identification and other voice message selection techniques

36. In 1993, CRIM also undertook to supply CSE with an operational speaker identification module by March 1995. Nothing more was said about this project, suggesting that the target may have been met. In the same year, according to NSA documents, the IDEAS company supplied a "Voice Activity Detector and Analyser", Model TE464375-1, to NSA's offices inside GCHQ Cheltenham. The unit formed the centre of a 14-position computer driven voice monitoring system. This too may have been an early speaker identification system.

37. In 1995, widely quoted reports suggested that NSA speaker identification had been used to help capture the drug cartel leader Pablo Escobar. The reports bore strong resemblance to a novel by Tom Clancy, suggesting that the story may have owed more to Hollywood than high tech. In 1997, the Canadian CRE awarded a contract to another researcher to develop "new retrieval algorithms for speech characteristics used for speaker identification", suggesting this method was not by then a fully mature technology. According to Sigint staff familiar with the current use of Dictionary, it can be programmed to search to identify particular speakers on telephone channels. But speaker identification is still not a particularly reliablr or effective Comint technique.[90]

38. In the absence of effective wordspotting or speaker identification techniques, NSA has sought alternative means of automatically analysing telephone communications. According NSA's classification guide, other techniques examined include Speech detection – detecting the presence or absence of speech activity; Speaker discrimination – techniques to distinguish between the speech of two or more speakers; and Readability estimation – techniques to determine the quality of speech signals. System descriptions must be classified "secret" if NSA "determines that they represent major advances over techniques known in the research community".[91]

## "Workfactor reduction"; the subversion of cryptographic systems

39. From the 1940s to date, NSA has undermined the effectiveness of cryptographic systems made or used in Europe. The most important target of NSA activity was a prominent Swiss manufacturing company, Crypto AG. Crypto AG established a strong position as a supplier of code and cypher systems after the second world war. Many governments would not trust products offered for sale by major powers. In contrast, Swiss companies in this sector benefited from Switzerland's neutrality and image of integrity.

40. NSA arranged to rig encryption systems sold by Crypto AG, enabling UKUSA agencies to read the coded diplomatic and military traffic of more than 130 countries. NSA's covert intervention was arranged through the company's owner and founder Boris Hagelin, and involved periodic visits to Switzerland by US "consultants" working for NSA. One was Nora L MacKabee, a career NSA employee. A US newspaper obtained copies of confidential Crypto AG documents recording Ms Mackebee's attendance at discussion meetings in 1975 to design a new Crypto AG machine".[92]

41. The purpose of NSA's interventions were to ensure that while its coding systems should appear secure to other cryptologists, it was not secure. Each time a machine was used, its users would select a long numerical key, changed periodically. Naturally users wished to selected their own keys, unknown to NSA. If Crypto AG's machines were to appear strong to outside testers, then its coding system should work, and actually be strong. NSA's solution to this apparent condundrum was to design the machine so that it broadcast the key it was using to listeners. To prevent other listeners recognising what was happening, the key too had also to be sent in code - a different code, known only to NSA. Thus, every time NSA or GCHQ intercepted a message sent using these machines, they would first read their own coded part of the message, called the "*hilfsinformationen*" (help information field) and extract the key the target was using. They could then read the message itself as fast or even faster than the intended recipient[93]

42. The same technique was re-used in 1995, when NSA became concerned about cryptographic security systems being built into Internet and E-mail software by Microsoft, Netscape and Lotus. The companies agreed to adapt their software to reduce the level of security provided to users outside the United States. In the case of Lotus Notes, which includes a secure e-mail system, the built-in cryptographic system uses a 64 bit encryption key. This provides a medium level of security, which might at present only be broken by NSA in months or years.

43. Lotus built in an NSA "help information" trapdoor to its Notes system, as the Swedish government discovered to its embarrassment in 1997. By then, the system was in daily use for confidential mail by Swedish MPs, 15,000 tax agency staff and 400,000 to 500,000 citizens. Lotus Notes incorporates a "workfactor reduction field" (WRF) into all e-mails sent by non US users of the system. Like its predecessor the Crypto AG "help information field" this device reduces NSA's difficulty in reading European and other e-mail from an almost intractable problem to a few seconds work. The WRF broadcasts 24 of the 64 bits of the key used for each communication. The WRF is encoded, using a "public key" system which can only be read by NSA. Lotus, a subsidiary of IBM, admits this. The company told *Svenska Dagbladet*:

> *"The difference between the American Notes version and the export version lies in degrees of encryption. We deliver 64 bit keys to all customers, but 24 bits of those in the version that we deliver outside of the United States are deposited with the American government".*[94]

44. Similar arrangements are built into all export versions of the web "browsers" manufactured by Microsoft and Netscape. Each uses a standard 128 bit key. In the export version, this key is not reduced in length. Instead, 88 bits of the key are broadcast with each message; 40 bits remain secret. It follows that almost every computer in Europe has, as a built-in standard feature, an NSA workfactor reduction system to enable NSA (alone) to break the user's code and read secure messages.

45. The use of powerful and effective encryption systems will increasingly restrict the ability of Comint agencies to **process** collected intelligence. "Moore's law" asserts that the cost of computational power halves every 18 months. This affects both the agencies and their targets. Cheap PCs can now efficiently perform complex mathematical calculations need for effective cryptography. In the absence of new discoveries in physics or mathematics Moore's law favours codemakers, not codebreakers.

# Glossary and definitions

| | |
|---|---|
| ATM | Asynchronous Transfer Mode; a high speed form of digital communications increasingly used for on the Internet |
| BND | Bundesachrichtendienst; the foreign intelligence agency of the Federal Republic of Germany. Its functions include Sigint |
| CCITT | Consultative Committee for International Telephony and Telegraphy; United Nations agency developing standards and protocols for telecommunications; part of the ITU; also known as ITU-T |
| CEPT | Conference Europeene des Postes et des Telecommunications |
| CLID | Calling Line Identification Data |
| Comint | Communications Intelligence |
| COMSAT | (Civil/commercial) communications satellite; for military communications usage, the phraseology is commonly reversed, i.e., SATCOM. |
| CRIM | Centre de Recherche Informatique de Montreal |
| CSDF | Collected Signals Data Format; a term used only in Sigint |
| CSE | Communications Security Establishment, the Sigint agency of Canada |
| CSS | Central Security Service; the military component of NSA |
| DARPA | Defense Advanced Research Projects Agency (United States Department of Defense) |
| DGSE | Directorate General de Securite Exteriere, the foreign intelligence agency of France. Its functions include Sigint |
| DSD | Defence Signals Directorate, the Sigint agency of the Commonwealth of Australia |
| DODJOCC | Department of Defense Joint Operations Centre Chicksands |
| E1, E3 (etc) | Standard for digital or TDM communications systems defined by the CEPT, and primarily used within Europe and outside North America |
| ENFOPOL | EU designation for documents concerned with law enforcement matters/police |
| FAPSI | Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii, the Federal Agency for Government Communications and Information of Russia. Its functions include Sigint |
| FBI | Federal Bureau of Investigation; the national law enforcement and counter-intelligence agency of the United States |
| FDF | Fast Data Finder |
| FDM | Frequency Division Multiplex; a form of multi-channel communications based on analogue signals |
| FISA | Foreign Intelligence Surveillance Act (United States) |
| FISINT | Foreign Instrumentation Signals Intelligence, the third branch of Sigint |
| Gbps | Gigabits per second |
| GCHQ | Government Communications Headquarters; the Sigint agency of the United Kingdom |
| GHz | GigaHertz |
| Gisting | Within Sigint, the analytical task of replacing a verbatim text with the sense or main points of a communication |
| HDLC | High-level Data Link Control |
| HF | High Frequency; frequencies from 3MHz to 30MHz |
| HMM | Hidden Markov Modelling, a technique widely used in speech recognition systems. |
| ILETS | International Law Enforcement Telecommunications Seminar |
| Intelsat | International Telecommunications Satellite |
| IOSA | Interim Overhead Sigint Architecture |
| Iridium | Satellite Personal Communications System involving 66 satellites in low earth orbit, providing global communications from mobile telephones |
| ISDN | Integrated Services Data Network |
| ISP | Internet Service Provider |
| ITU | International Telecommunications Union |
| IUR | International User Requirements (for communications interception); IUR 1.0 was prepared by ILETS (*qv*) in 1994 |
| IXP | Internet Exchange Point |
| LAN | Local Area Network |
| LEA | Law Enforcement Agency (American usage) |

| | |
|---|---|
| Mbps | Megabits per second |
| MHz | MegaHertz |
| Microwave | Radio signals with wavelengths of 10cm or shorter; frequencies above 1GHz |
| Modem | Device for sending data to and from (e.g.) a computer; a “modulator-demodulator) |
| MIME | Multipurpose Internet Message Extension; a systems used for sending computer files, images, documents and programs as "attachments" to an e-mail message |
| N-gram analysis | A system for analysing textual documents; in this context, a system for matching a large group of documents to a smaller group embodying a topic of interest. The method depends on counting the frequency with which character groups of length N appear in each document; hence N-gram |
| NSA | National Security Agency, the Sigint agency of the United States |
| OCR | Optical Character Recognition |
| PC | Personal Computer |
| PCS | Personal Communications Systems; the term includes mobile telephone systems, paging systems and future wide area radio data links for personal computers, etc |
| POP (or POP3) | Post Office Program; a system used for receiving and holding e-mail |
| PTT | Posts Telegraph and Telephone (Administration or Authority) |
| RAID | Redundant Array of Inexpensive Disks |
| SCI | Sensitive Compartmented Intelligence; used to limit access to Comint information according to "compartments" |
| SCPC | Single Channel Per Carrier; low capacity satellite communications system |
| SMTP | Standard Mail Transport Protocol |
| Sigint | Signals Intelligence |
| SONET | Synchronous Optical Network |
| SMDS | Switched Multi-Megabit Data Service |
| SMO | Support for Military Operations |
| SPCS | Satellite Personal Communications Systems |
| SRI | Signal Related Information; a term used only in Sigint |
| STOA | Science and Technology Assessments Office of the European Parliament; the body commissioning this report |
| T1, T3 (etc) | Digital or TDM communications systems originally defined by the Bell telephone system in North America, and primarily used there |
| TCP/IP | Terminal Control Protocol/Internet Protocol |
| TDM | Time Division Muliplex; a form of multi-channel communications normally based on digital signals |
| Traffic analysis | Within Sigint, a method of analysing and obtaining intelligence from messages without reference to their content; for example by studying the origin and destination of messages with a view to eliciting the relationship between sender and recipient, or groups thereof |
| UKUSA | UK-USA agreement |
| VPN | Virtual Private Network |
| VSAT | Very Small Aperture Terminal; low capacity satellite communications system serving home and business users |
| WAN | Wide Area Network |
| WRF | Workfactor Reduction Field |
| WWW | World Wide Web |

*X.25, V.21, V.34, V.90, V.100 (etc) are CCITT telecommunications standards*

*Illustrations : page 5; US Air Force; IPTV Ltd; page 6; Stephen King, Charles V Pick; IPTV Ltd; page 8; Jim Bamford, GCHQ; page 9; US Navy, KGB/Russian Security Service; page 12; D Campbell.*

# Notes

[1.] UKUSA refers to the 1947 United Kingdom – United States agreement on Signals intelligence. The nations of the UKUSA alliance are the United States (the "First Party"), United Kingdom, Canada, Australia and New Zealand (the "Second Parties").
[2.] "An appraisal of the Technologies of Political Control", Steve Wright, Omega Foundation, European Parliament (STOA), 6 January 1998.
[3.] "They've got it taped", Duncan Campbell, *New Statesman*, 12 August 1988. "Secret Power : New Zealand's Role in the International Spy Network", Nicky Hager, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, 1996.
**4.** National Security Council Intelligence Directive No 6, National Security Council of the United States, 17 February 1972 (first issued in 1952).
[5.] SIGINT is currently defined as consisting of COMINT, ELINT (electronic or non-communications intelligence and FISINT (Foreign Instrumentation Signals Intelligence).
[6.] Statement by Martin Brady, Director of DSD, 16 March 1999. Broadcast on the *Sunday Programme*, Channel 9 TV (Australia), 11 April 1999.
[7.] "Farewell", despatch to all NSA staff, William Studeman, 8 April 1992. The two business areas to which Studeman referred were "increased global access" and "SMO" (support to military operations).
[8.] *Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii*, the (Russian) Federal Agency for Government Communications and Information. FAPSI's functions extend beyond Comint and include providing government and commercial communications systems.
**9.** Private communications from former NSA and GCHQ employees.
[10.] Sensitive Compartmented Intelligence.
**11.** See note 1.
[12.] Private communications from former GCHQ employees; the US Act is the Foreign Intelligence Surveillance Act (FISA).
**13.** See note 6.
[14.] In 1919, US commercial cable companies attempted to resist British government demands for access to all cables sent overseas. Three cable companies testified to the US Senate about these practices in December 1920. In the same year, the British Government introduced legislation (the Official Secrets Act, 1920, section 4) providing access to all or any specified class of communications. The same power was recodified in 1985, providing lawful access for Comint purposes to all "external communications", defines as any communications which are sent from or received outside the UK (Interception of Communication Act 1984, Section 3(2)). Similar requirements on telecommunications operators are made in the laws of the other UKUSA countries. See also "Operation SHAMROCK", (section 3).
[15.] "The Puzzle Palace", James Bamford, Houghton Mifflin, Boston, 1982, p331.
[16.] Personal communications from former NSA and GCHQ employees.
[17.] "Dispatches : The Hill", transmitted by Channel 4 Television (UK), 6 October 1993. DODJOCC stood for Department of Defense Joint Operations Centre Chicksands.
[18.] "The Justice Game", Geoffrey Robertson, Chapter 5, Chatto and Windus, London, 1998
[19.] Fink report to the House Committee on Government Operations, 1975, quoted in "NSA spies on the British government", *New Statesman,* 25 July 1980
**20.** "Amerikanskiye sputniki radioelektronnoy razvedki na Geosynchronnykh orbitakh" ("American Geosynchronous SIGINT Satellites"), Major A Andronov, *Zarubezhnoye Voyennoye Obozreniye,* No.12, 1993, pps 37-43.
[21.] "Space collection", in The US Intelligence Community (fourth edition), Jeffrey Richelson, Westview, Boulder, Colorado, 1999, pages 185-191.
[22.] See note 18.
**23.** Richelson, *op cit.*
[24.] "UK Eyes Alpha", Mark Urban, Faber and Faber, London, 1996, pps 56-65.
[25.] Besides the stations mentioned, a major ground station whose targets formerly included Soviet COMSATs is at Misawa, Japan. Smaller ground stations are located at Cheltenham, England; Shoal Bay, Australia.
[26.] "Sword and Shield : The Soviet Intelligence and Security Apparatus", Jeffrey Richelson, Ballinger, Cambridge, Massachusetts, 1986.
[27.] "Les Francais aussi ecountent leurs allies", Jean Guisnel, *Le Point*, 6 June 1998.
[28.] *Intelligence* (Paris), **93**, 15 February 1999, p3.

[29.] "Blind mans Bluff : the untold story of American submarine espionage", Sherry Sontag and Christopher Drew, Public Affairs, New York, 1998.
**30.** *Ibid.*
[31.] *Ibid*
[32.] A specimen of the IVY BELLS tapping equipment is held in the former KGB museum in Moscow. It was used on a cable running from Moscow to a nearby scientific and technical institution.
[33.] TCP/IP. TCP/IP stands for Terminal Control Protocol/Internet Protocol. IP is the basic network layer of the Internet.
[34.] GCHQ website at http://www.gchq.gov.uk/technol.html
[35.] Personal communication from DERA. A Terabyte is one thousand Gigabytes, i.e., 1012 bytes.
**36.** Personal communication from John Young.
**37.** "Puzzle palace conducting internet surveillance", Wayne Madsen, Computer Fraud and Security Bulletin, June 1995.
**38.** *Ibid.*
[39.] "More Naked Gun than Top Gun", Duncan Campbell, *Guardian,* 26 November 1997.
[40.] "Spyworld", Mike Frost and Michel Gratton, Doubleday Canada, Toronto, 1994.
[41.] The National Security Agency and Fourth Amendment Rights, Hearings before the Select Committee to Study Government Operations with Respect to Intelligence Activitities, US Senate, Washington, 1976.
**42.** Letter from, Lt Gen Lew Allen, Director of NSA to US Attorney General Elliot Richardson, 4 October 1973; contained in the previous document.
[43.] Private communication.
[44.] World in Action, Granada TV.
[45.] This arrangements appears to be an attempt to comply with legal restrictions in the Interception of Communications Act 1985, which prohibit GCHQ from handling messages except those identified in government "certificates" which "describe the intercepted material which should be examined". The Act specifies that "so much of the intercepted material as is not certified by the certificate is not [to be] read, looked at or listened to by any person". It appears from this that, although all messages passing through the United Kingdom are intercepted and sent to GCHQ's London office, the organisation considers that by having British Telecom staff operate the Dictionary computer, it is still under the control of the telecommunications network operator unless and until it is selected by the Dictionary and passes from BT to GCHQ.
[46.] Private communications.
[47.] "Naval Security Group Detachment, Sugar Grove History for 1990", US Navy, 1 April 1991.
[48.] Missions, functions and tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia", NAVSECGRU INSTRUCTION C5450.48A, 3 September 1991.
[49.] Report on tasks of Detachment 3 , 544 Air Intelligence Group, *Air Intelligence Agency Almanac*, US Air Force, 1998-99.
[50.] *Ibid,* Detachment 2, 544 Air Intelligence Group.
[51.] Information obtained by Bill Robinson, Conrad Grebel College, Waterloo, Ontario. CDF and CFS documents were obtained under the Freedom of Information Act, or published on the World Wide Web.
[52.] Career resume of Patrick D Duguay, published at: http://home.istar.ca/~pdduguay/resume.htm.
[53.] CSE Financial Status Report, 1 March 1996, released under the Freedom of Information Act. Further details about "ECHELON" were not provided. It is therefore ambiguous as to whether the expenditure was intended for the ECHELON computer system, or for different functions (for example telecommunications or power services).
[54.] "Secret Power", *op cit.*
[55.] *Twenty/Twenty*, TV3 (New Zealand), October 1999.
[56.] Interview with David Herson, Head of Senior Officers' Group on Information Security, EU, by staff of *Engineering Weekly* (Denmark), 25 September 1996. Published at http://www.ing.dk/arkiv/herson.htm
[57.] Council Resolution on the Lawful Interception of Telecommunications, 17 January 1995, (96C_329/01)
[58.] "International Harmonisation of Technical Requirements for Legal Interception of Telecommunications", Resolution 1115, Tenth Plenary meeting of the ITU Council, Geneva, 27 June 1997.
[59.] ENFOPOL 98, Draft Resolution of the Council on Telecommunications Interception in respect of New Technology. Submitted by the Austrian Presidency. Brussels, 3 September 1998.
[60.] ENFOPOL 19, 13 March 1999.
[61.] European Parliament, 14 September 1998.
[62.] "Uncle Sam's Eavesdroppers", Close Up North, BBC North, 3 December 1998; reported in "Star Wars strikes back", *Guardian*, 3 December 1998
[63.] "Dispatches : The Hill", Channel 4 Television (UK), 6 October 1993
[64.] *Ibid.*
[65.] "Mixing business with spying; secret information is passed routinely to U.S.", Scott Shane, *Baltimore Sun*, 1 November 1996.
[66.] "UK Eyes Alpha", *op cit,* p235.
[67.] Private communication.
[68.] See note 62.

[69.] Raytheon Corp press release: published at: http://www.raytheon.com/sivam/contract.html
**70.** "America's Fortress of Spies", Scott Shane and Tom Bowman, Baltimore Sun 3 December 1995.
[71.] "Company Spies", Robert Dreyfuss, *Mother Jones*, May/June 1994.
[72.] *Financial Post*, Canada, 28 February 1998.
[73.] European Parliament, 16 September 1998.
[74.] See note 56.
[75.] Equivalent communications may be known as Synchronous Transport Module (STM) signals within the Synchronous Digital Hierarchy (ITU standard); Synchronous Transport Signals (STS) within the US SONET system; or as Optical Carrier signals (OC).
[76.] The information about these Sigint systems has been drawn from open sources (only).
[77.] In April 199, the peak data rate at MAE West was less than 1.9 Gbps.
[78.] Redundant Arrays of Inexpensive Disks.
[79.] Very Small Aperture Terminal; SCPC is Single Channel Per Carrier.
[80.] "Collected Signals Data Format"; defined in US Signals Intelligence Directive 126 and in NSA's CSDF manual. Two associated NSA publications providing further guidance are the Voice Processing Systems Data Element Dictionary and the Facsimile Data Element Dictionary, both issued in March 1997.
[81.] The Data Workstation processes TCP/IP, PP, SMTP, POP3, MIME, HDLC, X.25, V.100, and modem protocols up to and including V.42 (see glossary).
[82.] "Practical Blind Demodulators for high-order QAM signals", J R Treichler, M G Larimore and J C Harp, *Proc IEEE,* **86**, 10, 1998, p1907. Mr Treichler is technical director of AST. The paper describes a system used to intercept multiple V.34 signals, extendable to the more recent protocols.
[83.] The tasks were set in the second Text Retrieval conference(TREC) organised by the ARPA and the US National Institute of Science and Technology (NIST), Gaithersburg, Maryland. The 7th annual TREC conference took place in Maryland in 1999.
[84.] "Method of retrieving documents that concern the same topic"; US Patent number 5418951, issued 23 May 1995; inventor, Marc Damashek; rights assigned to NSA.
[85.] Address to the Symposium on "National Security and National Competitiveness : Open Source Solutions" by Vice Admiral William Studeman, Deputy Director of Central Intelligence and former director of NSA, 1 December 1992, McLean, Virginia.
**86.** For example, IBM *Via Voice*, Dragon *Naturally Speaking,* Lemout and Hauspe *Voice Xpress.*
[87.] "A Hidden Markov Model based keyword recognition system", R.C.Rose and D.B.Paul, *Proceedings of the International Conference on Accoustics, Speech and Signal processing*, April 1990.
[88.] Centre de Recherche Informatique de Montreal.
[89.] "Projet detection des Themes", CRIM, 1997; published at http://www.crim.ca/adi/projet2.html.
[90.] Private communication.
[91.] NSA/CSS Classification Guide, NSA, revised 1 April 1983.
[92.] "Rigging the game: Spy Sting", Tom Bowman, Scott Shane, *Baltimore Sun*, 10 December 1995.
[93.] "Wer ist der Befugte Vierte?", *Der Spiegel*, **36**, 1996, pp. 206-7.
[94.] "Secret Swedish E-Mail Can Be Read by the U.S.A", Fredrik Laurin, Calle Froste, *Svenska Dagbladet*, 18 November 1997.

EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

# STOA

# DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

**Vol 3/5**
**Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues**

Working document for the STOA Panel

Luxembourg,November 1999 PE 168.184/Vol 3/5/EN

*Cataloguing data*:

Title: **Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues**

Workplan Ref.: EP/IV/B/STOA/98/14/01

Publisher: European Parliament
Directorate General for Research
Directorate A
The STOA Programme

Author: Dr Franck Leprevost - Technische Universität Berlin

Editor: Mr Dick HOLDSWORTH,
Head of STOA Unit

Date: November 1999

PE number: **PE 168. 184 Vol 3/5**/EN

**This document is part of a series published in five volumes.**
**(Vols. 1/5 - 5/5).**
**The original language of this publication is French.**

# Chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie
# Résumé


Les objectifs de ce rapport sont :

- rappeler aux Membres du Parlement Européen les risques, concernant la surveillance électronique, inhérents à l'utilisation des moyens modernes de communication ;
- fournir aux Membres du Parlement Européen un document de référence concernant les technologies de cryptage, et les statuts actuels des démarches de standardisation de ces techniques ;
- décrire les directions futures possibles en ce qui concerne, tant les communications sécurisées, que les méthodes de surveillance électronique ;
- donner aux Membres du Parlement Européen une traduction, à la fois précise et claire pour les non-experts, et montrer les implications pratiques, de documents techniques relatifs à la sécurité de l'information, constituant des amendements récents à des organismes de contrôle internationaux ;
- proposer des options aux Membres du Parlement Européen permettant de préserver les intérêts des citoyens, entreprises et organisations européennes.

Le rapport contient six parties principales.
La première est une description succinte des moyens de communications modernes utilisés et de leurs risques ; la deuxième fournit un survol des techniques cryptographiques actuelles : cryptographie à clef secrète, cryptographie à clef publique, cryptographie quantique, qui sont détaillées dans les trois parties suivantes. La troisième partie donne une description précise de la cryptographie à clef secrète, un état de l'art concernant la situation en termes de sécurité informatique de protocoles très largement utilisés, et un point actuel sur les procédures de standardisation du futur standard fédéral américain, qui devrait s'imposer comme standard mondial. La quatrième partie donne une description très précise de la cryptographie à clef publique, un état de l'art concernant les procédures de standardisation au niveau mondial des protocoles à clef publique, une lecture technique d'un document de la DG XIII de la Commission Européenne. La mise en oeuvre pratique de la cryptanalyse et de la cryptographie quantique peuvent avoir des conséquences particulièrement importantes au niveau international sur le plan politique, diplomatique ou financier : la cinquième partie décrit l'état de l'art concernant ces deux directions. Le Wassenaar Arrangement concerne les contrôles sur les exportations d'armes conventionnelles et les produits technologiques sensibles, et regroupe 33 pays, dont ceux de la Communauté Européenne et les signataires de l’accord UKUSA. La sixieme partie est une lecture technique des amendements concernant la sécurité de l’information du 3/12/1998 au Wassenaar Arrangement. La derniere partie du document est une liste de suggestions de nature a protéger les citoyens européens, et à préserver les intérêts des entreprises et organisations européennes. Elle donne également des projets de recherches complémentaires, afin de mieux mesurer l'impact de certains accords internationaux sur le plan de la surveillance électronique en Europe. Le rapport inclu une bibliographie, donnant une liste des documents référencés.

# Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues

**FRANCK LEPREVOST**

## 1. Introduction

Electronic surveillance is generally considered to be a weapon with which to fight organised crime or terrorism ([**32**], Foreword, p. iii). It can, however, have a darker side, namely that of industrial espionage, violation of privacy, or both.
The report [**35**] published by STOA in January 1998 refers to the role played by the ECHELON network in electronic surveillance (see [**8**] for a list of links to this subject). It is a global network which can intercept all telephone, fax or e-mail communications.
Although it is very difficult to quantify the losses caused by industrial espionage (many cases are not reported, either because the company fears losing face or simply because the damage goes undetected), the losses incurred by firms in the European Union can reasonably be put at several billion euros per year. The extent of the problem can be surmised from a study published by PricewaterhouseCoopers Investigation LLC ([**27**]) on 22 March 1999; the study shows that over 59% of all firms with a significant presence on the Internet were spied on in 1998. Furthermore, it is quite conceivable that information acquired by such means is exploited by the international stock markets. It is an issue which thus affects shareholders, companies and national economies alike.
The initial purpose of this report is to illustrate the main techniques whereby EU citizens, firms and institutions can protect themselves, to a certain extent, against what is now known as economic intelligence.
In Section 2, we outline the various means of communication generally used. We also describe some of the techniques, of varying degrees of sophistication, by means of which information can be unlawfully accessed, and some countermeasures which can be taken. Technological measures allowing data to be transmitted confidentially require the use of cryptosystems, which are briefly defined and illustrated in Section 3. In Sections 4, 5 and 6 we outline the latest developments in secret-key, public-key and quantum cryptographic protocols. As regards the first two, we give an update on standardisation procedures. In Section 7 we conduct a technical appraisal of the information security aspects of the Wassenaar Arrangement, which concerns export controls for conventional arms and sensitive technological products. We conclude the report by making recommendations to the European bodies.

This document does not necessarily represent the views of the European Parliament. Nevertheless, in this report commissioned by STOA, and particularly in Sections 2, 7 and 8, we systematically viewed things from a standpoint which we judged to be the most favourable vis-à-vis the defence of European interests.

### 2. Means of communication used and risks involved

In this section we look at relatively hi-tech methods of communication; direct oral transmission and traditional mail are therefore not dealt with. For the sake of clarity and in keeping with standard practice in this field, we have designated Alice and Bob as two hypothetical individuals wishing to communicate.

**2.1 Standard telephones.** Standard telephone systems can be tapped without any technical difficulties: a microphone can be placed inside the telephone set; alternatively, the wires of the telephone exchange of the building where the target is located can be tapped, as can those of the telephone company's central exchange. These techniques are largely undetectable by the target.

**2.2 Voice-scrambling telephones.** Secure telephones and fax machines are now available on the market. Their level of security may be very modest, depending on the legislation currently in force in their country of origin (see Section 7).

**2.3 Fax machines.** As things stand, fax machines should be considered as insecure as telephones. Fax-encrypting machines do exist, but their security level is contingent on legislation in their country of origin, as above.

**2.4 Cordless telephones**. Some older models transmit just above the AM broadcasting band and can thus be easily intercepted. Commercially-available scanners enable the more recent models to be tapped. Sometimes certain sound wave inversion techniques are recommended in order to combat tapping, but these solutions only provide a very low level of confidentiality. As regards cellular phones, the situation is more complex. Early models transmit in the same way as radios and so do not provide a high level of confidentiality, since conversations can be intercepted using inexpensive scanners (equally low-priced equipment can be purchased to increase the frequencies accessible to the scanners currently on the market). It is worth mentioning here the US Administration's attempt to impose the Clipper standard on all portable phones developed in the United States. This would have allowed government agencies to retain keys enabling them to eavesdrop on conversations. Moreover, details of the encryption algorithm 'Skipjack', developed by the NSA, have not been made public.

The GSM system, the international standard for digital cellular phones, was developed by the GSM MoU Association (which became the GSM Association on 30 November 1998) in collaboration with the European Telecommunications Standard Institute ([**13**]), an international umbrella organisation bringing together public authorities, operator networks, manufacturers, service providers and users. GSM uses cryptographic techniques at various levels. As regards identification, GSM uses several algorithms, although in practice most operators use a protocol named COMP128. However, in April 1998 the Smartcard Developer Association ([**28**]), in collaboration with David Wagner and Ian Goldberg, researchers at UC Berkeley (USA), announced that it had developed a system whereby phones using the GSM standard could be cloned . But on 27 April 1998, Charles Brookson, chairman of the security group of the GSM MoU Association, stated that this would not be of any practical use to fraudsters.

With regard to confidentiality, GSM uses a protocol known as A5. There are two versions of this system: A5/1 and A5/2, which meet different needs. According to some experts, A5/2 is less secure than A5/1, which we will now discuss. The A5/1 protocol in theory uses 64 bits. But Wagner told us that in practice ([**33**]), in every phone he had seen, 10 bits had been systematically replaced with zeros, thus reducing the theoretical security of the system to 54 bits. The system is therefore even less secure than the 56 bits offered by DES, which can now be cracked all too easily (see 4.4). Work conducted before this discovery ([**11**]) had already reduced the real security of the system to 40 bits. It is therefore quite possible that by using similar methods, i.e. assuming that 10 bits are equal to zero, the actual security level of A5/1 – and hence the confidentiality of conversations - can be reduced even further.

On 24 February 1999, at the GSM World Congress in Cannes (France), Charles Brookson announced that GSM security had been reviewed and in particular that COMP128 had been revised.

**2.5 ISDN.** It is technically possible to tap an ISDN telephone with the help of software that remotely activates the monitoring function via the D channel, obviously without physically lifting the receiver. It is therefore easy to eavesdrop on certain conversations in a given room.

**2.6 Internet communications**. In a nutshell, the traditional mail equivalent of an e-mail on the Internet is a postcard without an envelope. Basically, such messages can be read. If they are in plaintext, they can be understood and any 'secret reader' can take measures which are detrimental to the two parties wishing to communicate. For example, if Alice sends a message to Bob and if

Charles is a passive attacker, Charles knows what message has been sent but he cannot modify it. If, on the other hand, he is an active attacker, he can modify it. One way of circumventing this problem is by encrypting the messages (see Section 3). However, the solutions developed by Microsoft, Netscape and Lotus for encrypting e-mails are configured in such a way that the NSA can systematically read all e-mails thus exchanged outside the United States (although it is probably the only agency that is able to do so).

**2.7 The TEMPEST effect.** TEMPEST is the acronym for Temporary Emanation and Spurious Transmission, i.e. emissions from electronic components of electromagnetic radiation in the form of radio signals. These emissions can be picked up by AM/FM radio receivers within a range varying from a few dozen to a few hundred metres. Building on these data it is then possible to reconstruct the original information. Protective measures against such risks consist of placing the source of the emissions (central processors, monitors, but also cables) in a Faraday cage, or jamming the electromagnetic emissions. The NSA has published several documents on TEMPEST (see [**25**]).

All computers work by means of a micro-processor (chip). The PC chip market is dominated by Intel, which has a market share of over 80%. On 20 January 1999 Intel unveiled its new PSN-equipped Pentium III processor.

**2.8 PSNs.** Pentium III processors have a unique serial number called PSN (Processor Serial Number). Intel devised this technique in order to promote electronic commerce. The aim of the serial number is to enable anybody ordering goods via the Internet to be identified. Intel maintains that all users will be able to retain control over whether or not to allow their serial number to be read. However, software techniques enabling the number to be read have already been discovered (see [**26**]) . It is therefore possible to obtain the PSN secretly and to track the user without his or her knowledge.

The PSN is very different from the IP (Internet Protocol) address, even though a user's IP address can be revealed to any webpage he or she chooses to visit. IP addresses are not as permanent as PSNs: many users have no fixed IP address that can be used to track their movements, as they may use masks via the proxy servers of Internet service providers. ISPs normally assign a different IP number per session and per user. Users can also change ISP, use a service which guarantees their anonymity, etc.

As it stands, the PSN can therefore be used for electronic surveillance purposes. Moreover, it is still not known for sure whether PSNs can be cloned. If so, their use for identification purposes in electronic commerce would have to be ruled out.

## 3. An overview of cryptographic techniques

Cryptography is the study of the techniques used to ensure the confidentiality, authenticity and integrity of information and its origin. Cryptography can be broadly divided into three categories: private-key, public-key and quantum cryptography. Several of these techniques make extensive use of hash functions. Here we give a brief outline of the techniques, explaining them in more detail in Sections 4, 5 and 6. However, it should be stressed that a high degree of confidentiality can be attained only by combining these techniques with measures to counter TEMPEST effects. Basically, it is no use encrypting data if, for example, they can be read in plaintext while being transferred from the keyboard to the central processor. Assuming that the information to be processed is in binary code, the fundamental unit of information referred to in all sections of this report is the bit, apart from in Sections 3, 4 and 6, where its quantum equivalent, the qubit, is used.

**3.1 Hash functions**. These are tools which have multiple applications; amongst other things, they can be used to create secret keys and electronic signatures. Their basic function is to rapidly map a file (of any size) to a fixed-size value, such as 160 bits, as in the European hash function RIPEMD-160. If the

value is known it should be impossible to reconstruct an initial text that would match the hash value. Essentially, it is very hard to invert. A hash function should also avoid collisions. In other words, it should not be possible to construct two distinct files giving the same hash values.

**3.2 Secret-key cryptography.** With this method, a single key is used both for encrypting and decrypting. This key should be known only to Alice and Bob. It can be of varying length. Secret-key cryptography can be divided into two categories: Stream Ciphers and Block Ciphers. With Stream Ciphers the length of the key is the same as that of the message to be transmitted. The 'right' size, i.e. that which can be used as a basis for recreating a key the same size as the message, can be reduced to a fixed size with the help of cryptographically secure pseudorandom bit generators. These generators have to pass very stringent statistical tests. As regards Block Ciphers, the size of the key is fixed (56 bits for DES, 128 bits for AES, see 4.3, 4.4). The main problems with this technique lie in the management and distribution of the keys.

**3.3 Public-key cryptography.** Unlike the secret-key algorithms, public-key algorithms require two keys per user. Alice (and Bob respectively) chooses a secret key, $X_A$ (respectively $X_B$) and publishes (e.g. in a directory) a public key $Y_A$ (respectively $Y_B$). Bob encodes his message with $Y_A$ and sends it to Alice. Only Alice, with her secret key $X_A$, can decode the message. The security of public-key algorithms has a mathematical basis (see Section 5).
See [**21**] and [**23**] for details of a report (updated to 31 December 1998) on the standardisation procedures for AES secret-key protocols (see 4.5) and IEEE-P1363 public-key protocols (see 5.3).

**3.4 Quantum cryptography.** This method is dealt with in 6.2.

**3.5 Cryptanalysis.** Cryptanalysis is the perfection of techniques or attacks to reduce the theoretical security of cryptographic algorithms. This should not be confused with the hackers' approach, since they, as a rule, exploit weaknesses not in the algorithms themselves, but in the security architecture. In 4.4 we describe a number of attacks on secret-key cryptosystems and in 5.1 and 6.1 on public-key cryptosystems.

**3.6 Security quantification.** In general security is evolutive, as it often depends on the scientific knowledge of a given period. It may be absolute. For example, the only known form of attack for breaking various Block Ciphers is that of trying out all possible keys (Brute-Force Attack). Hence, if such a system uses a 56-bit key, security equals $2^{56}$ operations. It can also be relative: theoretically, a cryptosystem is considered to be insecure if it can be cryptanalysed in polynomial time according to the size of the data. Its degree of security can be considered satisfactory if it takes a sub-exponential, or better still, exponential period of time to cryptanalyse. More precise measurements can be provided in terms of MIPS/year. This unit of measurement is equivalent to a computer's computational capacity, carrying out a million instructions per second over a year (approximately $3.10^{13}$ instructions in all).

## 4. Secret-key cryptography

Secret-key cryptography can be divided into two categories: Stream Ciphers and Block Ciphers.

**4.1 Stream Ciphers.** These technologies are only rarely published. Where Block Ciphers encrypt in blocks, Stream Ciphers encrypt on a bit-by-bit basis. The most well-known of these, and the most cryptographically secure, is the One-Time Pad, which requires a key of the same length as the message to be transmitted. This key must also be created randomly. For practical purposes, the One-Time Pad is often simulated by means of cyptographically secure pseudorandom bit generators, often abbreviated to CSPRBG (Cryptographically Strong Pseudo-Random Bit Generator). Starting with an initial data item $X_0$ (seed), CSPRBG is used to create deterministically bits which appear to be random. This is then double-checked by subjecting the CSPRBG candidate to extremely stringent statistical

tests.

**4.2 Block Ciphers.** With Block Ciphers a message is cut into fixed-length blocks. With the aid of an algorithm and secret key K of fixed length, but possibly of a different length to the blocks, each block is encrypted and sent. The recipient decrypts each block with the same key K. All he or she then has to do is to 'stick' the blocks back together to recover the original message. The *de facto* standard for algorithms in the Block Cipher category is DES (see 4.4).

**4.3 Problems**. At least two problems may arise with these methods (Stream Ciphers and Block Ciphers):

> (a) How do Alice and Bob communicate the secret key K to each other?
> (b) In a network with *n* users where n(n – 1))/2 secret keys are needed (e.g. 499 500 secret keys in a network of 1 000 users), obvious problems of storage and security need to be addressed.

Public-key (see 5, particularly 5.2) and quantum (see 6.2) cryptography techniques provide partial solutions to these problems.

**4.4 DES: state of the art.** The symmetric algorithm most widely used at present is undoubtedly DES (Data Encryption Standard). In 1997 it was recognised as an FIPS (Federal Information Processing Standard) and registered as FIPS 46-2. DES uses a 56-bit key. There are therefore $2^{56}$ possible keys. The block length is 64 bits.
DES has enjoyed the political backing of the United States for a very long time. As recently as 17 March 1998, for example, Robert S. Litt (Principal Associate Deputy Attorney-General) maintained that the FBI did not have the technological and financial capacity to decrypt a message encrypted with a symmetric 56-bit secret-key algorithm. He concluded by stating that 14 000 Pentium PCs would need to be used for four months in order to achieve such a feat (see also statements by Louis J. Freeh (Director of the FBI) and William P. Crowell (Deputy Director of the NSA, [**10**], p. 1-2).
Nevertheless, the Electronic Frontier Foundation built a DES cracker and presented it at an informal (Rump) session of the Crypto '98 conference in Santa Barbara. The machine (worth USD 250 000, including the design) is described in [**10**]. Better still, the book explains how to scan the plans in order to reproduce the machine for a maximum outlay of USD 200 000 (basically there is no need to pay over again for the design). This machine is capable of finding a secret DES key in an average of four days. In January 1999 a team led by the Electronic Frontier Foundation won the RSA Laboratories' Challenge (pocketing USD 10 000 for their efforts) by managing, with the aid of a large computer network, to break a 56-bit key in 23 hours 15 minutes. This has both political and diplomatic implications: it appears that it is now financially feasible for all nations to decode all DES-encoded records that may have been built up over the years. From now on all DES-based systems should therefore be considered insecure. In practice, it is now advisable to use Triple-DES at the very least (though even here caution is needed). The NIST (National Institute for Standards and Technology), mindful of the risks relating to DES, has called on the cryptographic community to work on its successor – AES (Advanced Encryption Standard [**24**]).

**4.5 AES.** The required features for AES are: a) the algorithm should be a secret-key Block Cipher type algorithm, and (b) it should support the following combinations of cryptographic key-block sizes: 128-128, 192-128 and 256-128 bits. The algorithms used in AES will be royalty-free worldwide. The algorithm should also be sufficiently flexible, for example, to allow other combinations (64-bit block lengths); it should be efficient on various platforms and in various applications (8-bit processors, ATM networks, satellite communications, HDTV, B-ISDN, etc.) and it should be usable as a Stream Cipher, MAC (Message Authentication Code) generator, Pseudo-Random Number Generator, etc.
The first AES conference was held on 20 August 1998 (just before the Crypto '98 conference). During the conference, presentations were given of the 15 (out of 21) candidates that had been

accepted: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOK197, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT and TWOFISH.
At present, it seems that the DEAL, LOK197, FROG, MAGENTA and MARS (in the extra-long key version) proposals are subject to attacks of varying intensity.
The second AES conference will be held in Rome on 22-23 March 1999, after which five algorithms will be chosen out of the 15 candidates. The debate on the 15 candidates has already begun ([**3**]). A third AES conference will be held from six to nine months later, when the winner will be announced. Following a final examination period of another six to nine months, the winning algorithm will be put forward as an FIPS. It is likely that AES will become an FIPS in around 2001.

## 5. Public-key cryptography

**5.1 A description of public-key cryptography.** The security of public-key algorithms has a mathematical basis:

- Factoring of large integers: RSA (Rivest-Shamir-Adleman) and Rabin-Williams.
- Discrete Log Problem: DSA (Digital Signature Algorithm), Diffie-Hellman key exchange, El Gamal cryptosystem and electronic signature and Schnorr and Nyberg-Rueppel electronic signatures.
- Discrete Log Problem for elliptic curves: the above algorithm equivalents also apply to elliptic curves. Given an elliptic curve E defined over a finite field Fp or $F2^n$, it is essential to be able to rapidly calculate the number of rational points on the elliptic curve over the finite field in question. The Schoof-Elkies-Atkin method (now known as SEA) is normally used for this purpose. In some cases (Koblitz curves or complex multiplication curves) this number is very easy to calculate.

Public-key cryptosystems are prone to attacks:

- Factoring of large integers: the ECM (Elliptic Curve Factoring Method) is used to find small factors. At present QFS (Quadratic Field Sieve) or NFS (Number Field Sieve) are used to find large factors. There is a limit to the numbers that can be considered. Very recently, Professor Shamir of the Weizmann Institute perfected an approach known as the 'Twinkle Attack' which enables 512-bit numbers to be factored with great rapidity. The cost of the attack is also very modest. At present, therefore, RSA-512 bits should no longer be considered secure.
- Discrete Log Problem: to solve this problem, the index-calculus method or the NFS method can be used. There is a limit to the numbers that can be considered.
- Discrete Log Problem for elliptic curves: a well-known attack is Pollard's rho method (which can also be parallelised). Here too, only certain curves can be considered: the so-called supersingular or anomalous elliptic curves should be avoided (a very rapid practical test can show whether a given elliptic curve is suitable).

The techniques based on the problem of factoring, on the one hand, and the discrete logarithm, on the other, are fundamentally different. For the former, large prime numbers have to be secretly produced and stored. As it is not humanly possible to remember large prime numbers, they have to be stored on a physical medium, which could give rise to security problems.
The approach to the discrete logarithm problem is different. For example, the user can freely choose a text that is easy to memorise (e.g. a poem). The text is then translated into binary code and hashed with a tried-and-tested hash function, such as the European proposal RIPEMD160, which has an output of 160 bits (see. 3.1). These 160 bits, being impossible to memorise, form the user's secret key. This approach has the advantage of limiting storage problems.
These two approaches solve different problems, according to the parameters involved. Elliptic curve-based techniques are now the focus of attention, since unlike other proposals, no subexponential algorithm has as yet been discovered to resolve the discrete logarithm problem for these groups. Consequently, elliptic curves over fixed-size fields provide the same degree of security as other algorithms for fields or modules of a larger size. For example, the security provided by elliptic curves for a 163-bit module is equivalent to that provided by RSA for 1024 bits.

**5.2 Symmetric or public-key cryptography?** Symmetric and public-key cryptosystems are not mutually exclusive . On the contrary, for the secure transmission of a document through an open channel (e.g. Internet), they are most useful if combined.
For example, Alice lives in Paris and wishes to send a 15-page report by e-mail to Bob, who lives in Brussels. It is out of the question for Alice to go to Brussels to give a secret AES key to Bob. If she were to choose this expensive method, she might just as well deliver the document in person! Naturally, Alice and Bob could choose to communicate using public-key cryptographic techniques, as described above, the only problem being that encryption with these techniques is about 1000 times slower than encryption using secret-key cryptosystems.
The most practical solution could be the following:

- Alice sends a 128-bit message K to Bob using public-key cryptography. The use of public-key techniques is warranted, as the message is very short (128 bits). Alice and Bob thus share the secret K.
- As agreed between them according to standard practice, K is the secret key to a secret-key algorithm, AES.
- Alice and Bob forget the public-key technology. To continue communicating they use AES with the K key. Alice can now send her 15-page document to Bob for the price of a phone call.

Alice's and Bob's systems must, however, be compatible: indeed, the aim of the standardisation drive described below is to harmonise communications.

**5.3 IEEE-P1363 and other standards.** The P1363 project began in 1993 under the auspices of the IEEE (Institute of Electrical and Electronics Engineers) Standardisation Committee. Its aim is to improve communications between several families of public-key cryptosystems: RSA, El Gamal, Diffie-Hellman and elliptic curves. Since the end of 1996, the techniques considered by P1363 have changed little and have been summarised in ([**16**]). The P1363A project contains additional techniques.
The standard project (draft version 9) is now ready to be revised by a group of experts from the IEEE Standards Association. The group started its work in February 1999 and will deliver its initial conclusions on 2 April 1999. According to the most optimistic estimate, the draft will be approved as a standard on 25 June 1999.
The IEEE-P1363 standard will have a huge influence on other standards, such as ANSI X9.42, ANSI X9.62 and ANSI X9.63 in the banking industry. It will also be the cornerstone of the X.509 ([**17**]) and S-MIME ([**18**]) protocols. These multiple protocols are essential for
electronic commerce.

**5.4 A technical interpretation of the Commission (DG XIII) document COM(97) 503.** This document [**12**] sets out Community-wide requirements with regard to secure electronic communications. It focuses on both electronic signatures and confidential methods of electronic communication. Below we suggest a few updates to Technical Annexes I (Digital Signature) and II (Symmetric and asymmetric encryption) to this document.

**Annex I.** It would be preferable to avoid citing MD2 and MD5 as examples, since cases of collision in the former and pseudo-collision in the latter have been brought to light. It would also be advisable to replace SHA by SHA-1 (based on [**14**]) and to write RIPEMD-160 (based on [**7**]) instead of RIPEM 160. It is currently recommended that one of these two hash functions be used to replace the MD2, MD4 and MD5 functions wherever possible.
**Annex II. Symmetric encryption systems.** It would be preferable to avoid citing DES and SAFER as examples. We suggest that IDEA, which so far has shown no serious flaws, be retained and that the candidates that passed the first AES round be mentioned.
**Annex II. Asymmetric encryption systems.** Once again, as regards the examples provided, it would be advisable to be more specific, e.g. by taking up the approach described at the start of 5.1, which is currently being standardised.
**Annexe II. Systems security.** We suggest deleting the last sentence of the second paragraph: 'In a symmetric system like DES or IDEA, keys of 56 to 128 bits provide similar protection as a 1024-bit public key'. This assertion is totally

false.

## 6. Quantum cryptanalysis and quantum cryptography

Quantum cryptanalysis and quantum cryptography may have a considerable impact in the political, diplomatic and financial terms.

**6.1 Quantum cryptanalysis.** The term quantum cryptanalysis refers to the set of techniques whereby the secret keys of cryptographic protocols can be found by means of quantum computers. It is an area in which research is thriving, as in August 1998 one of the system's founders, Peter Shor of AT & T Bell Labs, won the Nevanlinna Prize, which was awarded to him at the International Congress of Mathematicians in Berlin. He has developed methods based on quantum physics to factor large numbers in polynomial time ([**29**], [**30**]) or to solve the Discrete Log Problem even when formulated within the general context of Abelian varieties ([**31**], see [**32**] for a summary of these results).

**Consequence**: if these results were to be put into practice, the immediate consequence would be that the security of the public-key cryptographic protocols described in Section 5 would be permanently undermined. In addition, cryptosystems based on Abelian varieties would then be cryptanalysed via quantum computing. A parallel can be drawn between these consequences and the comments in 7.3 relating to the Wassenaar Arrangement.

Despite this, IEEE-P1363 is still valid: the Shor algorithms require a powerful quantum computer, whose existence is still hypothetical. Various experimental proposals have been made (qubits are the quantum equivalent of bits and are basically dual-state quantum systems):

- To use the electronic states of ions as qubits in an electromagnetic ion trap and to manipulate them with lasers (see [**4**]).
- To use nuclear atom spins in a complex molecule as qubits, and to manipulate them using nuclear magnetic resonance (see [**6**] and [**9**]).
- To use the nuclear spins of silicon chip impurities as qubits and to manipulate them using the chip's electronics (see [**19**]).

None of these proposals has been tested for anything other than small numbers of qubits.

This field of research is particularly well-regarded in the United States and is funded by the DARPA, the Pentagon's research department. A similar project has been set up in Europe: nine research groups have joined together to form the Quantum Information European Research Network. Nonetheless, according to Shor ([**31**]) it would be unreasonable to expect a quantum coprocessor to be developed within the next few years.

Should such a quantum computer ever exist, the public-key cryptography described in Section 5 would become obsolete. Nevertheless, there is a theory of quantum cryptography, more specifically of quantum key-sharing ([**1**], see [**2**] for a bibliography on the subject), which offers an alternative to public-key cryptography.

**6.2 Quantum cryptography.** The problems are similar to those described in 5.2: Alice and Bob once again wish to share a secret, which they can then use as a secret key for a symmetric protocol (such as AES). If they use only a telephone line, they have no choice but to employ public-key cryptography. If an attacker with a powerful quantum computer eavesdrops on their conversation, they are open to the attacks described earlier. However, if they can use an optical fibre to transmit quantum states, they can employ quantum cryptography. It can be designed in such a way that an attacker listening in on the conversation can capture only one 'bit' of the conversation at the most. Furthermore, any information that he does manage to capture will disturb the states, so Alice and

Bob will immediately know what is happening. All they would then have to do then is reject the states in question.

Although the theory dates back to 1982-84 ([**1**]), it was not put into practice until the 1990s. In 1990-92 IBM began an initial free-space experiment over a 30 cm length. In 1993-95 British Telecom conducted an experiment on optical fibres over a 10-30 km length. In 1996 Swiss Telekom conducted similar experiments on a 23 km fibre under Lake Leman. In 1997 Los Alamos National Lab successfully conducted the same experiments on a 48 km optical fibre, and in 1998 it conducted an experiment through free space over 1 km.

## 7. A technical interpretation of Category 5 of the Wassenaar Arrangement

**7.1 The Wassenaar Arrangement.** Acknowledging the end of the Cold War, on 16 November 1993 in The Hague representatives of the 17 member states of COCOM decided to abolish the committee and replace it with a body which reflected the new political developments. The decision to wind up COCOM was confirmed in Wassenaar (Netherlands) on 29-30 March 1994 and came into effect on 31 March 1994.

The foundations of the agreement on COCOM's successor were laid on 19 December 1995, once again in Wassenaar, and the inaugural meeting was held on 2-3 April 1996 in Vienna, which since then has become the site of the Permanent Representation of the Wassenaar Agreements.

The Arrangement concerns export controls for conventional arms and sensitive technological products. Participating countries are: Germany, Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Denmark, United States, Russian Federation, Finland, France, Spain, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Norway, New Zealand, the Netherlands, Poland, Portugal, Republic of Korea, Slovak Republic, Czech Republic, Romania, United Kingdom, Sweden, Switzerland, Turkey and Ukraine.

This list of 33 countries includes, in particular, those of the European Community and the signatories to the UKUSA agreement.

The Arrangement is open to those countries which fulfil certain criteria (see [**34**] for a full description) and decisions are based on consensus. Observers are not admitted.

As regards the security of information, some important amendments were made during the last meeting of the representatives of the signatory countries to the Arrangement on 2-3 December 1998 in Vienna ([**34**]). These amendments, of which we give a technical interpretation below, concern Category 5, part 2, entitled *Information Security.*

**7.2 Category 5, part 2: Information Security.** Part 5.A.2 stipulates in particular that controls are to be imposed on systems, equipment and components using the following (either directly or after modification):

1. a symmetric algorithm using a key longer than 56 bits; or
2. a public-key algorithm, in which the security of the algorithm is based on one of the following:
   (a) the factorisation of integers higher than 512 bits (e.g. RSA);
   (b) discrete log computations in the multiplicative group of a finite field larger than 512 bits;
   (c) discrete log computations in a group other than those mentioned above, and which is larger than 112 bits.

However (Note 5.A.2.d), cryptographic equipment specially designed and intended solely for use in machines for banking or money transactions is not subject to controls.

**7.3 Comments.** The gist of Point (1) is that unrestricted exports are authorised

only for those techniques which offer the same degree of security as DES. As explained in 4.3, this type of system offers a very limited degree of security. The techniques referred to in Point (2) were illustrated in 5.1. The main groups targeted in (2c) are those associated with elliptic curves. However, in actual fact (2c) covers a far vaster area, as it concerns all groups. It thus includes, *inter alia,* rational points of Abelian varieties over a fnite field (in particular elliptic curves, which are Abelian varieties of dimension 1), which are known (see 6.1) to be open to quantum cryptanalysis.
As stated in 5.1, according to current know-how elliptic curves over fixed-size fields offer equivalent security to that provided by RSA with far larger modules or with the discrete logarithm over a far larger finite field. In other words, (2a), (2b) and (2c) offer equivalent degrees of security, in that, on average, more or less the same effort is required to recover the secret data from the different algorithms. This explains the slight difference in size between (2a, 2b) and (2c). Moreover, as seen in 5.2, these public-key techniques are generally combined with secret-key cryptosystems.

**7.4 Note.** Watermark techniques are not included in the systems subject to controls. Such techniques, which are also known as data hiding or steganography, enable one piece of information to be hidden in another, e.g. a fax, photo, video or sound files. The hidden information generally protects the intellectual ownership of the data (see [**20**]), but nothing prevents users from hiding other things, such as a 128-bit key for a symmetric system, which the two correspondents have agreed on in advance (possibly via information that has been embedded in another document using a stenographic method). The state of the art is that documents which contain information hidden using steganographic techniques cannot – without special software - be distinguished from the original; moreover, the information can withstand numerous compressions/decompressions (necessary for the rapid transmission of such documents over the Internet) and can only be recovered by means of a special software product and a password. This technique is also very cheap. It seems that it is not therefore subject to export restrictions, but in practice it does allow confidential data to be exchanged. Likewise, the approach entitled 'Chaffing and Winnowing: Confidentiality without Encryption', developed by Professor Rivest, also enables a high degree of confidentiality to be achieved, whilst avoiding any entanglement with the Wassenaar Arrangement.

**7.5 Impact on criminal organisations.** It would be naïve to imagine that criminal or terrorist organisations conduct their business in compliance with international import/export rules, or that they do not have not the means to perfect highly confidential methods of communication. Algorithms do not stop at borders. Moreover, numerous algorithms are freely accessible. It is also difficult to see how the authorities could prove that a suspect binary sequence was created using an unauthorised system if, for example, it was actually created with a public-key cryptosystem using a 4096-bit module. Just because an intercepted binary sequence does not make sense, even if it has hypothetically used a 'lawful' cryptographic system (which can be ascertained, but at considerable cost), this does not mean that it has been created 'unlawfully' (which, above a certain level of sophistication, cannot be ascertained). Lastly, even if cryptographic products are subject to tight export controls, the fact remains that they are still freely used in many countries, including the United States. However, it does not appear that criminal or terrorist organisations operate only outside these countries; but neither do the authorities of these countries appear to lack effective means of investigation on their national territory.

**7.6 Impact on the European Union.** From a Community point of view, the consequences of the Wassenaar amendments are manifold.
Prior to the amendments, EU firms were free to conquer the data security market as long as the laws of their country of origin authorised them to do so. In particular, European firms in this sector could export solutions with a very high degree of security, the only restrictions being those imposed by national legislation (which could nevertheless be extremely tight, as in the case of France until recently).

Now, however, the only products that European data security firms are allowed to export without restriction are of a far lower quality.
By virtue of these amendments, at the time of publication of the agreement European data security firms, unlike their US counterparts, could not automatically realise economies of scale and target large markets. Even if, from the viewpoint of the Wassenaar Arrangement, they were on an equal footing with US firms, this apparent equality was deceptive and overall they were at a disadvantage.
Fortunately, bilateral agreements reached in Europe now allow European firms to sell high-quality solutions freely throughout the continent. However, this freedom ends abruptly at Europe's external borders.
But even if the use of cryptography is such as to prevent industrial espionage by bodies with limited financial clout, the Wassenaar Arrangement resolutions do not protect firms from all risks. In the light of the existence of the DES Cracker, it is not unreasonable to estimate that an institution with a USD 300 million budget could recover a 56-bit key within a few seconds. With the same budget, it would take a few tenthousandths of a second (see 2.4, where this is the maximum level of security provided by several GSM cellphones) to find a secret 40-bit key. Hence those firms, bodies or individuals that equip themselves with a cryptosystem which fulfils the criteria set out in 7.2 should be fully aware that the Echelon network is in all likelihood still able to intercept and decode their information.

## 8. Recommendations

It is our view that the recommendations (Section 4.5, p. 21-22) contained in the previous report [**35**] are still valid. Here, however, we seek to provide the European Parliament with some alternative solutions.

A.- Experts should be commissioned to provide updates on a regular basis, or as required, to the technical documents published by Community bodies. For example, it would be advisable to examine whether and to what extent the comments made in 5.4 (which are by no means exhaustive) have been taken into consideration; it would also be advisable to monitor the conferences on AES, IEEE-P1363 and P1363A concerning secret-key and public-key cryptography and the experimental developments with regard to quantum processors.

B. – Bearing in mind the legal risks run by European telephone industries (groups of users could be roused to action by the fact that the level of security provided does not systematically correspond to the level claimed), European bodies should encourage European telephone operators to:

- update their implementation of the COMP128 authentication algorithm;
- clearly specify the actual level of security of their implementation of the encryption algorithm A5.

C – In view of the fact that the NSA has managed to bring about a considerable reduction in the degree of security offered to non-US users of solutions developed by Microsoft, Netscape and Lotus for encrypting electronic messages, with the express intention of being systematically able to read the messages exchanged by these users (and probably being the only agency in the world able to do so), the European Parliament should actively promote the use, amongst European organisations, firms and citizens, of e-mail encrypting solutions that actually provide the confidentiality promised. At the same time, Proposal 5 of the 'Policy issues for the European Parliament' contained in the STOA IC 2000 report by Duncan Campbell should be taken into consideration.

D. – In view of:

- the launch of the worldwide advertising campaign for the PSN*-equipped Pentium III by the market leader (80%+) for PC chips,
- the risks of the PSN being used for electronic surveillance purposes,
- the concern shown by the highest US authorities with regard to this precise subject (see the declaration [**15**] made on 25 January 1999 by Mr Al Gore, Vice-President of the United States),
- the risk that PSNs may be cloned and be unsuitable for e-commerce, hence the risk that this new industry may be held back, particularly in Europe,

the relevant committees of the European Parliament should:

- call on American government agencies, including the NSA and FBI, to provide information on their role in the creation of the PSN developed by Intel,
- at the same time commission a group of independent technical experts to conduct a precise assessment of the risks connected to this product: electronic surveillance, PSN falsification, etc. The group should issue its report as soon as possible.

Building on the initial results of the above, if appropriate, the relevant committees of the European Parliament, should be asked to consider legal measures to prevent PSN-equipped (or PSN-equivalent) chips from being installed in the computers of European citizens, firms and organisations. We wish to underline most strongly that the above suggestions have no connection whatsoever with any particular firm, but are motivated purely by the characteristics of a product which, unless rapid action is taken at Community level, may become a de facto industrial standard in Europe within the next few months.

E. – As regards Category 5, Part 2 of the Wassenaar Arrangement, dealt with in Section 7 of this report, the following should be noted:

- Since high-security secret-key and public-key algorithms are freely accessible, for example via the Internet, and in view of Note 7.4 and the implications of such accessibility (see 7.5), it appears that export restrictions in no way constitute a serious impediment for criminal and terrorist organisations. Nevertheless, by following the example of the United States the police can take effective action, even when top-quality cryptographic products are freely used.
- However, in the light of 7.6, such export restrictions pose a serious obstacle to European data security firms and hinder the development of the international
e-commerce industry.
- On 19 January 1999, following the inter-ministerial committee meeting on the information society ([**5**]), the French Government, in agreement with President Chirac, pledged to liberalise the use of cryptography by raising from 40 bits to 128 bits the security threshold which may be freely used. This latest development is apparently only the first step towards a total deregulation of the use of cryptography on French territory. Until then, French rules on cryptography had been among the most stringent in the world.
- The Echelon network is most probably able to intercept, decode and process the information transmitted with products on the market that fulfil the criteria mentioned in 7.2.

In order to strengthen Community cohesion, the European Parliament should strive initially to persuade EU countries to adopt a common position at the meetings organised under the Wassenaar Arrangement. Subsequently, in view of the aforementioned points, and in order to boost electronic commerce on a worldwide scale, it should suggest that the Community simply with from Category 5, Part 2 of the list of products subject to controls under the Wassenaar Arrangement.

F. – The committee should commission a more detailed report on the implications

* Processor Serial Number

of the risks in terms of electronic surveillance that the Wassenaar Arrangement brings with it. For example, under Item 5.B.1.b.1 (Part 1, on Telecommunications) certain equipment using ATM (Asynchronous Transfer Mode) digital techniques is subject to controls. This data transfer technology is far more difficult (but not impossible, see [**32**], part 2, and the aforementioned STOA report by Duncan Campbell) to monitor electronically than conventional TCP/IP systems. It would also be very useful to ascertain whether products that are authorised for export provide effective responses to TEMPEST (see 2.7 and introduction to point 3), since the usefulness of cryptosystems is somewhat limited if the data can be read in plaintext before encryption or after decryption, with the aid of electromagnetic radiation.

## Bibliographie


**1** *C. H. Bennett, G. Brassard :* Quantum cryptography: public key distribution and coin tossing. In Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984).

**2** *G. Brassard :* Quantum cryptography: a bibliography. SIGACT News 24:3 (1993). Une version plus récente est accessible online à http://www.iro.umontreal.ca/crepeau/Biblio-QC.html

**3** *cAESar Project :* http://www.dice.ucl.ac.be/crypto/CAESAR/caesar.html

**4** *J. I. Ciriac, P. Zoller :* Quantum computations with cold trapped ions. Phys. Rev. Lett. **74**, p. 4091-4094 (1995)

**5** *Comité interministériel pour la société de l'information, conférence de presse de Mr. Lionel Jospin, Premier Ministre :* http://www.premier-ministre.gouv.fr/PM/D190199.HTM
Voir les decrets No. 99-199, 99-200 du 17 mars 1999, ainsi que l'arrete du 17 mars 1999 (Journal Officiel Numero 66 du 19 mars 1999)

**6** *D. G. Cory, A. F. Fahmy, T. F. Havel :* Ensemble quantum computing by nuclear magnetic resonance spectroscopy. Proc. Nat. Acad. Sci. **94**, p. 1634-1639 (1997)

**7** *H. Dobbertin, A. Bosselaers, B. Preneel* : RIPEMD-160: a strengthened version of RIPEMD. D. Gollmann, editor, Fast Software Encryption, Third International Workshop, Lecture Notes in Computer Science **1039** (1996). Une version corrigee et acutalisee est accessible online: http://www.esat.kuleuven.ac.be/bosselae/ripemd160.html

**8** *Echelon : une liste de liens :* http://www.saar.de/bong/archiv/echelon.html, http://serendipity.nofadz.com/hermetic/crypto/echelon/echelon.htm, http://serendipity.nofadz.com/hermetic/crypto/echelon/nzh1.htm, http://www.telegraph.co.uk/et?ac=000602131144806&rtmo=0sksx2bq&atmo=0sksx2bq&pg=/et/97/12/16/ecspy16.html, http://www.freecongress.org/ctp/echelon.html, http://www.disinfo.com/ci/dirty/cidirtyprojectechelon.html, http://www.dis.org/erehwon/spookwords.html (spookwords)

**9** *N. A. Gershenfeld, I. L. Chuang :* Bulk spin resonance quantum computation, Science **275**, p. 350-356

(1997)

**10** *Electronic Frontier Foundation :* Cracking DES, Secrets of Encryption Research. Wiretap Politics & Chip Design, O'Reilly (1998)

**11** *J. Dj. Goli● :* Cryptanalysis of alleged A5 stream cipher. In Advances in Cryptology, Eurocrypt'97, Lecture Notes in Computer Science **1233**, Springer-Verlag Berlin Heidelberg New York, p. 239-256 (1997)

**12** *European Commission - Directorate General XIII :* Communication from the commission to the European Parliament, the council, the economic and social committee and the committee of the regions ensuring security and trust in electronic communication (COM 97-503). Egalement accessible online : http://www.ispo.cec.be/eif/policy/97503toc.html

**13** *European Telecommunications Standards Institute (ETSI) :* http://www.etsi.fr/

**14**:*FIPS PUB 180-1* : Secure Hash Standard, Federal Information Processing Standards Publication 186, US Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, Springfield, Virginia (1994). Accessible online sous: http://www.itl.nist.gov/div897/pubs/fips180-1.htm

**15** *A. Gore, Vice-Président des Etats-Unis :* Interview au San Jose Mercury News (25/1/1999)

**16** *IEEE-P1363 :* http://grouper.ieee.org/groups/1363/index.html

**17** *IETF-PKIX, Public-Key Infrastructure (X.509) :* http://www.ietf.org/html.charters/pkix-charter.html

**18** *IETF-S/MIME, Mail Security (smime) :* http://www.ietf.org/html.charters/smime-charter.html

**19** *B. E. Kane :* A silicon-based nuclear spin quantum computer. Nature **393**, p. 133-137 (1998)

**20** *M. Kutter, F. Leprévost :* Symbiose von Kryptographie und digitalen Wasserzeichen: effizienter Schutz des Urheberrechtes digitaler Medien. A paraître in Tagungsband des 6. Deutschen IT-Sicherheitskongresses des BSI (1999)

**21** *F. Leprévost :* Les standards cryptographiques du XXI-eme siecle : AES et IEEE-P1363. A paraitre in *La Gazette des Mathématiciens* (1999)

**22** *F. Leprévost :* Peter W. Shor, prix Nevanlinna 1998. A paraitre in *La Gazette des Mathématiciens* (1999).

**23** *F. Leprévost :* AES und IEEE-P1363, die kryptographischen Standards des 21. Jahrhunderts. A paraitre in Tagungsband des 6. Deutschen IT-Sicherheitskongresses des BSI (1999)

**24** *NIST AES Home Page :* http://csrc.nist.gov/encryption/aes/aes_home.htm

**25** *NSA Tempest Documents :* NACSIM 5000, 5004, 5100A, 5201, 5203

**26** *Ch. Persson :* Pentium III serial number is soft switchable after all. In c't Magazin für Computer Technik (1999)

**27** *PricewaterhouseCoopers Investigations LLC :* The Corporate Netspionnage Crisis. Informations accessibles online : http://www.pricewaterhousecoopers.fm/extweb/ncpressrelease.nsf/DocID/B81092772821633B8525673C006AFA91

**28** *Smartcard Developper Association :* http://www.scard.org/

**29** *P. W. Shor :* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal of Computing **26**, p. 1484-1509 (1997)

**30** *P. W. Shor :* Quantum Computing. Proceedings of the International Congress of Mathematicians, Berlin, Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung (1998)

**31** *P. W. Shor :* Communication personnelle (1998)

**32** *U.S. Congress, Office of Technology Assessment :* Electronic Surveillance in a Digital Age. OTA-BP-ITC-149, Washington, DC: U.S. Government Printing Office (July 1995)

**33** *D. Wagner :* Communication personnelle (1999)

**34** *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies :* http://www.wassenaar.org/

**35** *S. Wright :* An appraisal of technologies of political control. Interim Study for the STOA (19/1/1998)

# DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

**Vol 4/5**

**The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law**

Working document for the STOA Panel

Luxembourg, October 1999 PE 168.184/Vol 4/5

*Cataloguing data*:

| | |
|---|---|
| Title: | **The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law** |
| Workplan Ref.: | EP/IV/B/STOA/98/1401 |
| Publisher: | European Parliament<br>Directorate General for Research<br>Directorate A<br>The STOA Programme |
| Author: | Prof. Chris Elliot |
| Editor: | Mr Dick HOLDSWORTH,<br>Head of STOA Unit |
| Date: | October 1999 |
| PE number: | **PE 168. 184 Vol 4/5** |

# The legality of the interception of electronic communications:

a concise survey of the principal legal issues and instruments under international, European and national law

Dr Chris Elliott

28 March 1999

## Abstract

Protection of privacy; fundamental human right; UN Declaration, European Convention on Human Rights; EU Directives and Recommendations; National laws; lawful interception of communications; data protection; encryption; duties of telecommunications network operators; interception by foreign governments; possible action by EU to require telecommunications network operators to protect users' privacy


## Executive summary

Privacy of communications is one of the fundamental human rights. The UN Declaration, International Covenant and European Convention all provide that natural persons should not be subject to unlawful interference with their privacy. The European Convention is legally binding and has caused signatories to change their national laws to comply.

Most countries, including most EU Member States, have a procedure to permit and regulate lawful interception of communications, in furtherance of law enforcement or to protect national security. The European Council has proposed a set of technical requirements to be imposed on telecommunications operators to allow lawful interception. USA has defined similar requirements (now enacted as Federal law) and Australia has proposed to do the same.

Most countries have legal recognition of the right to privacy of personal data and many require telecommunications network operators to protect the privacy of their users. All EU countries permit the use of encryption for data transmitted via public telecommunications networks (except France where this will shortly be permitted).

Electronic commerce requires secure and trusted communications and may not be able to benefit from privacy law designed only to protect natural persons.

The legal regimes reflect a balance between three interests:

- privacy;
- law enforcement;
- electronic commerce.

Legal processes are emerging to satisfy the second and third interests by granting more power to governments to authorise interception (under legal controls) and allowing strong encryption with secret keys.

There do not appear to be adequate legal processes to protect privacy against unlawful interception, either by foreign governments or by non-governmental bodies.

A course of action open to the EU is to require telecommunications operators to take greater precautions to protect their users against unlawful interception. This would appear to be possible without compromising law enforcement or electronic commerce.

# Contents

# 1 Context

This study has been prepared by Dr Chris Elliott[1] for the Scientific and Technological Options Assessment programme of the European Parliament. It is a contribution to the project on "Development of surveillance technology and risk of abuse of economic information". This study examines the legality of the interception of electronic communications.

The study is intended to be brief and concise. It concentrates on instruments that exist and not on the debate that led to them. It also avoids speculation as to the evolution of law in this field or the moral and ethical challenges that it poses.

Three levels of instrument are considered:

- International agreements
- EU Decisions and Directives
- National laws (of EU Member states and significant third countries)

Legislation in this field attempts to reconcile three conflicting pressures:

- Respect for privacy - Privacy is a fundamental human right. International agreements and national laws are more concerned with the rights of natural persons than with those of legal persons (companies).
- Capabilities for law enforcement - The lawful interception of communications is important for law enforcement agencies and most countries have legal procedures to authorise and regulate interception.
- Needs of electronic commerce - Secure communication is essential to permit electronic commerce to develop and may require the use of encryption which might conflict with the requirements of law enforcement.

The study extends beyond interception to consider encryption, since this is an important potential counter to interception and is also subject to some legal control. It also considers data protection law regarding the storage and manipulation of personal information where it applies to the transmission of that information.

# 2 International agreements

## 2.1 Universal Declaration of Human Rights

Article 12 states that

> No one shall be subjected to arbitrary interference with his privacy , .... or correspondence, ... Everyone has the right to the protection of the law against such interference ...

A key word in this Article is "arbitrary". Lawful interference is not excluded.

## 2.2 International Covenant on Civil and Political Rights

This UN Covenant[2] builds on the Universal Declaration and is legally binding. By Art. 2.1, the Contracting Parties are obliged to respect and ensure all of the rights recognised by the Covenant, and by Art. 2.2 they are required to take steps to meet their obligations within their own legal systems. Art. 4 allows Contracting Parties to derogate from some of the specific Articles (ie Rights) in a Public Emergency.

Article 17 states that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy ...

and that:

> Everyone has a right to the protection of the law against such interference...

This appears to address only natural, not legal, persons and reinforces the idea that lawful interference is permitted.

## 2.3 European Convention of Human Rights

Article 8 of the Convention[3] states:

> 1. Everyone has the right to respect for his ... correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.

It is not clear whether this offers any protection to legal persons. It has been used to test the legality of national procedures for the official interception of communications (eg Klass[4]) and to force European states to introduce a legal procedure (eg Malone[5]).

## 2.4 OECD Guidelines

OECD has adopted guidelines[6] which, although primarily concerned with encryption, have a bearing on interception. Recommendation 5 states:

> The fundamental rights of individuals to privacy, including secrecy of communications ..., should be respected in national cryptographic policies and in the implementation and use of cryptographic methods.

## 2.5 Council of Europe

Article 7 of the Data Protection Convention[7] requires that appropriate security measures shall be taken for the protection of personal data against unauthorised access or dissemination.

Recommendation R(95)13 of the Committee of Ministers (adopted September 11 1995) "concerning criminal procedural law connected with information technology" recommended:

- that criminal laws should be modified to allow interception in the investigation of serious offences against telecommunications or computer systems; and
- that measures should be considered to minimise the negative effects of cryptography without affecting its use more than is strictly necessary.

# 3 EU legislation and agreements

## 3.1 INFOSEC Green Paper

The Commission resolved to prepare a Green Paper on the security of information systems[8] but, although several drafts were prepared, none has been adopted. The drafts dealt with issues of encryption, digital signatures and privacy enhancement.

## 3.2 Council Resolution

The Council Resolution on the lawful interception of telecommunications[9] notes a list of Requirements of Member States to allow them to conduct the lawful interception of telecommunications. The Resolution continues that Member States should take these Requirements into account when defining national measures and in relation to network operators.

The set of Requirements appears to cover of all aspects of interception. It requires telecommunications network operators or service providers to make available details of the addresses and contents of communications, to do so in a way which is not apparent to the users being monitored and, where the operators use encryption, to provide decrypted (en clair) versions of intercepted communications.

The Requirements closely match those identified by the FBI in the USA, which led to CALEA (see section 4.2 below), and by the Barrett Review in Australia (also section 4.2).

## 3.3 Directive 95/46/EC

This Directive was primarily concerned with the protection of data stored in databases and is of only indirect relevance to interception of communications. However, the Preamble includes:

> (2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

and the Directive starts:

> Article 1: Object of the Directive
>
> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

## 3.4 Directive 97/66/EC

The preamble makes it clear that this Directive, like 95/46, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. It does not affect the right of Member States to take such measures as

they consider necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law.

However, Article 5 states that Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised.

# 4 National legislation

## 4.1 EU member states

There are broadly similar legislative regimes in all countries of the EU. Rather than repeating the analysis of each of them, the regime in the UK will be described in detail and any significant differences of principle in other countries will be noted. The information given here for the UK has been taken from primary sources; less reliable and less up-to-date secondary sources have been used to derive the corresponding information for other EU Member States. The Author would be grateful for any primary information or better secondary information on the legal regime in those countries.

**United Kingdom**

The starting point is section 5 of the Wireless Telegraphy Act 1949, which makes it illegal to use any wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of any message which the user is not authorised to receive, or to disclose any information obtained in that way. This does not apply to interception authorised by the government and to disclosure in legal proceedings.

The Interception of Communications Act 1985 was passed following the case of Malone before the ECHR (see section 2.3 above). Section 1 maintains the rule of section 5 WTA ’49. Section 2 permits the Secretary of State to issue a warrant authorising interception of post or a public telecommunications system if he considers it necessary:

- in the interests of national security
- for the purpose of preventing or detecting serious crime; or
- for the purpose of safeguarding the economic well-being of the UK.

This Act provides a procedure to authorise interception of Internet messages but not messages being transmitted within private networks. Interception of the signal from a cordless telephone to its base is excluded[10], as are the signals emitted by a cellular telephone (but the subsequent transmission of those signals via the cellular network is included because that is a public telecommunications network).

S1 of the Computer Misuse Act 1990 makes it a crime knowingly to cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer. Although it is primarily intended to criminalise "hacking", it would appear to apply to the use of a computer (including one embedded inside interception equipment) to intercept data being transmitted between two other computers.

The Data Protection Act 1984 gives legal effect to eight data protection principles which follow those of the Council of Europe Convention. Principle 8 requires data users to take appropriate security measures against unauthorised access to personal data. "Personal data" refers to living natural persons, not legal persons.

There are no legal restrictions in the UK on the importation, possession or use of encryption equipment. However, in criminal proceedings, section 20 of the Police and

Criminal Evidence Act 1984 permits the authorities, where they may demand evidence derived from a computer, also to require it to be made readable.

**Austria**

There is a general data protection law[11] and further detailed rules which govern the transmission of personal data. The general legal framework for telecommunications (TKG)[12] does not provide specific sanctions for breaching these rules. It does however impose a criminal sanction of up to 3 months imprisonment for illegal interception of transmissions. Telecommunication network operators are required to set up systems to allow the criminal courts to make interceptions (TKG Art 89) and to warn users that the network may not be secure (TKG 90).

**Belgium**

There are criminal sanctions[13] against the ownership or use of equipment for the interception of private communications, other than by an officer of the state. Similar sanctions apply to such an officer who abuses the right to intercept communications or divulges any material that has been lawfully obtained by interception.

**Denmark**

Danish law provides specific penalties for passing on or exploiting third party communications by network operators or their employees[14]. A further law[15] requires mobile communications licensees to keep confidential any communications through their networks.

Operators are required to take all precautions necessary to prevent unauthorised persons gaining access to information.

**Finland**

The Telecommunications Market Act[16] imposes a general duty of confidentiality on telecommunication network operators, their staff and contractors. The wider duties under the Personal Data Act also prevent disclosure. There are criminal sanctions for breach of these duties, unless the disclosure is, with the consent of the subscriber, to appropriate authorities to prevent misuse of the telecommunication system.

Law enforcement officials may demand disclosure of information or recordings of calls if investigating certain crimes listed in the Coercive Measures Act[17]. Telecommunications network operators are required to provide the necessary facilities, which are funded by Government.

**France**

Telecommunications network operators are required to respect the secrecy of correspondence[18] and there are criminal sanctions for deliberate violation[19]. Private conversations may only be intercepted under certain conditions, when authorised by the judiciary or administration[20].

The UK approach of permitting the use encryption for transmission over public networks is shared by all other Member States except France. The current law in France[21] permits the use of cryptography for authentication but requires confidentiality systems to be authorised and for keys to be deposited with a State-designated key escrow. Until recently only 40 bit codes were permitted but, in January 1999, the French government announced that all restrictions would be lifted.

**Germany**

Privacy of the content of telecommunications is guaranteed by the constitution and operators authorised by the TKG[22] are subject to criminal sanctions (s85 TKG) if they breach this duty. The operators must also take appropriate technical precautions or other measures to protect the privacy of telecommunications and personal data. Security requirements are specified by the regulatory authority[23].

The operators are required, by s88 TKG, to set up (at their own expense) facilities to support legally prescribed interception.

**Greece**

The right to privacy of telephone and other telecommunications is protected by Article 19 of the Constitution. This right may be withdrawn on application to the Court of Appeal judge prosecutor from the courts or civil, military or police authorities in the interests of national security or in the detection of specified crimes. Applications are overseen by the National Commission for the Protection of Privacy in Communication[24].

Irelan**d**

There is protection for personal data within the Data Protection Act 1988 but there is no specific provision in Irish law to protect the security and confidentiality of telecommunications services.

**Italy**

Like Ireland, the only protection is within the implementation of the Data Protection Directive in Italian law[25]. This does however extend to data about entities and associations as well as individuals and might provide some protection against unlawful interception.

**Luxembourg**

Again there is only protection in terms of data protection, concerning the storage and transmission of data about an individual[26].

**Netherlands**

There is a general duty on telecommunications network operators to abide by the rules of personal data set out in the Data Protection Act[27]. More detailed rules are given in the Telecommunications Act[28] which was expected to become law late in 1998. This gives effect to Directive 97/66/EC. Article 11.2 of that Act imposes a general duty on telecommunications network operators and service providers to protect the privacy of their

users. This is interpreted by Article 11.3 to require them to have a level of security which is appropriate to the state of technology and implementation costs, and in proportion to the level of threat.

**Portugal**

Personal data is protected[29] but there is no explicit protection for the privacy of communications.

**Spain**

The only specific protection is the general data protection law[30] but the telecommunication legislation[31] [32] contain statements on the duty to preserve the confidentiality and secrecy of communications

**Sweden**

The Telecommunications Act 1987[33] imposes an obligation of confidentiality on individuals who obtain access to telecommunications messages in the course of their duties. There are well-defined circumstances under which this obligation may lawfully be breached.

The Data Protection Act[34] also applies to data transmitted by telecommunications systems.

## 4.2 Third countries

**United States of America**

Interception is generally illegal in the United States but is permitted in most States under stringent rules designed to protect privacy but allow the investigation of crime, including a requirement to obtain a court order before conducting an interception. There are two basic pieces of Federal legislation: ECPA[35] which concerns criminal investigations and FISA[36] which concerns intelligence and counterintelligence operations.

ECPA works like many European legal frameworks, in that it sets in place a procedure to authorise lawful interception. Network operators and service providers are required by CALEA[37] to have the necessary technical facilities and to render assistance to law enforcement agencies. The requirements of CLEA are similar to those of the Council Resolution (see section 3.2 above).

FISA authorises electronic surveillance of foreign powers and agents of foreign powers to obtain foreign intelligence information. FISA defines this in terms of U.S. national security, including defence against attack, sabotage, terrorism, and clandestine intelligence activities. The targeted communications need not relate to any crime. FISA surveillance actions are implemented operationally by the FBI. Electronic surveillance conducted under FISA is classified.

There are two limbs to FISA:

- Communications to or from US persons (natural or legal) but not U.S. persons who are overseas (unless the communications are with a U.S. person who is inside the U.S.). A court order is required to authorise interception;

- Communications exclusively between or among foreign powers or involving technical intelligence other than spoken communications from a location under the open and exclusive control of a foreign power. An intercept may be authorised by a Presidential order.

**Australia**

Australia is of interest to Europe because it has recently examined in some detail the requirements for lawful interception capability. The Barrett Review[38] concluded that telecommunications interception is highly cost-effective when compared with other forms of surveillance. The Review supported the development of "international user requirements" as the most effective means of international cooperation to ensure that law enforcement's needs are taken into account in the development of new technology. The conclusions were similar to those of the Council Recommendation (see section 3.2 above) in that they call for network operators to be required to support lawful interception whilst at the same time strengthening the duty of the operators to protect confidentiality against unlawful interception.

The Review calls for international agreed standards. It concludes that unilateral action by Australia to demand interceptable and secure national technology might lead to less than world-class technology being used and hence to a major economic disadvantage. It continues "the sooner an international requirement for interception is standardised and accepted, the more likely there will be the automatic provision of a telecommunications intercept capability in new technology with similar implications for all users".

# 5 Observations

Several main points and trends are clear:

- Human rights legislation, particularly ECHR, clearly provides a robust protection for natural persons against unlawful interception by the State of communications. It is not clear to what extent this legislation would protect legal persons;

- Most EU Member States have, and it might be expected that all soon will have, a procedure to authorise lawful interception by the State;

- The EU, USA and Australia appear to be converging on a common set of interception requirements which ensure that network operators do everything necessary to permit lawful interception;

- Many EU Member States already require telecommunications network operators to take technical precautions to protect privacy of communications (ie against unlawful interception);

- The economic benefits of encryption to allow secure e-commerce are seen as outweighing the social losses to law enforcement, and soon all EU Member States will have no restrictions on the use of encryption.

The position is less clear with regard to interception by foreign powers, particularly because of the fundamental technological change from switched circuits to packet switching. The former allows the network operator to control the route by which communications pass between subscribers. The latter reflects the underlying principle of the Internet, in that packets of data go by whatever route is convenient. It may for example be easier to route a packet from the south to the north of France via the USA at 09.30 French Time if most US assets are underused at that time and the French national network is at peak demand.

Consider two subscribers within country A, communicating with each other via a network operating in country A. Interception of communications by a person in country B while the communications are passing within country A would appear to be unlawful. Under these circumstances the subscribers would have a right of recourse to ECHR and country B would be in breach of ICCPR. Even if the interception is lawful in country B (for example FISA could make the interception lawful if country B is the USA), it is not lawful in country A unless country B has express permission by the authorisation procedure of country A.

Now consider the case where their communication is routed via country B. It is possible that the lawful procedure for interception could be followed in country B. In particular, FISA could make the interception lawful if country B is the USA; the network operator in the USA would be obliged to comply with a lawful request to support that interception. Similarly IOCA could make it lawful if country B was UK.

It is claimed that some countries have the technological capability to intercept communications been carried entirely on a network within another country and it is the policy of many countries to be able to do so when the communication is (even temporarily)

within that country. Legal protection against the former is weak or inconvenient; against the latter it is non-existent.

A possible course of action for the EU to protect privacy without compromising law enforcement would be to extend and enforce the requirement for network operators to protect the privacy of communications. Technical means exist which could achieve this at three levels:

1. Telecommunications network operators to apply strong encryption to the content of communications. As the operators would hold the keys to this encryption, they could meet the Requirements of the Council Resolution.

2. Anonymous re-routing services to provide encryption of the addresses of communications. Again they could meet the Requirements but this would provide additional protection against unlawful interception leading to what is know in military intelligence as "traffic analysis" - even where the content of messages cannot be decrypted, the names of the sender and recipient can provide valuable intelligence.

3. Readily available private encryption to allow those who require greater security to encrypt their messages with a private key. An approach to reconciling this with law enforcement has been proposed in Denmark[39]. This in effect reverses the burden of proof in criminal cases. Where there is:

   - circumstantial evidence of guilt;
   - encrypted material which might prove guilt;
   - the defendant chooses not to decrypt that material;

   then the Court may draw an inference of guilt. This is analogous to the UK law on the right to remain silent[40] when questioned.

# 6 Bibliography and endnotes

## 6.1 Books


- Lloyd I J, "Information Technology Law", Butterworths, 1997 ISBN 0 406 89515 5
- Madsen W, "Handbook of personal data protection", Macmillan, 1992 ISBN 0-333-56920-2
- Michael J, "Privacy and human rights - an international and comparative study, with special reference to information technology", UNESCO, 1994 ISBN 92-3-102808-1
- Scherer J, "Telecommunications laws in Europe", Butterworths, 1998


## 6.2 Journals

The following journals frequently address the issue of telecommunications security:

- Computers and Law
- Computer Law and Security Report
- Computer and Telecommunications Law Review

## 6.3 Web sites

Information derived from web sites should be treated with caution. Although those of reputable bodies are probably reliable, there is no quality assurance and many of the web sites concerned with privacy and interception do not appear to come up to even the lowest standards of objectivity. A few of the sites examined in the course of this study are listed below; search engines yield many more.

- OECD has a site with several relevant pages; including http://www.oecd.org/news_and_events and http://www.oecd.org/dsti/sti/it/secur
- A useful survey of cryptographic policies around the world is offered on the site of the Global Internet Liberty Campaign http://www.gilc.org/crypto/crypt-survey
- The Electronic Privacy Information Centre provides what appears to be objective and valuable information on http://www.epic.org
- EU law and announcements are on http://www2.echo.lu/legal/en/dataprot/dataprot.html
- There is a thorough review of the US legislation on http://www.cdt.org/digi_tele.

## 6.4 References and footnotes

[1] Dr Elliott is an English barrister and an engineer specialising in telecommunications and computing technology. Contact: Chambers of Marie-Claire Sparrow, 95A Chancery Lane, London WC2A 1DT or chris.elliott@pitchill.demon.co.uk

[2] came into effect in 1976, 129 states are parties to the Covenant

[3] European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950

[4] Klass v Germany [1978] 2 EHRR 214

[5] Malone v UK [1984] 7 EHRR 14

[6] Recommendation of the OECD Council concerning Guidelines for the Security of Information Systems, adopted on November 26-27 1993 C(92) 188/Final

[7] Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data

[8] Council Decision March 13 1992 in the field of information security, [1992] OJ L 123

[9] Council Resolution OJ 4/11/96 C329 pages 1 - 6

[10] R v Effik & Mitchell [1994] 3 All ER 458

[11] Datenschutzgesetz

[12] Telekommunikationsgesetz BGBL 1997/100

[13] Art 259 Code Pénal, 30 June 1994

[14] Ministerial Order No 712, 25/7/96

[15] Act No 468, 12/6/96

[16] Telemarkinalaki 1997/396

[17] Pakokeinokai

[18] L 32-3 PTC

[19] Articles 226-13, 226-15 and 432-9 of the penal code

[20] Law of 10 July 1991

[21] Loi de la Réglementation des télécommunications, 18/6/96

[22] Telekommunikationsgesetz 25/7/1996

[23] Bundersanzeiger 208(a) 7/11/97

[24] Ethniki Epitropi Prostasias tou Aporritou ton Epikoinonion

[25] Law 675/96

[26] Law of 31 March 1979

[27] Wet Persoonsregistraties, 28 December 1988, 665

[28] The Bill for the Telecommunications Act (Regels inzake de telecommunicatie (Telecommunicatwiet) - Voorstel van wet) of 15 September 1997, TK 1996/97, 25533, 1-2

[29] Law 10/91, 24/4/91, amended by Law 28/94, 29/8/94

[30] Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, 1992 (known as LORTAD)

[31] Ley de Ordenación de las Telecommunicaciones (LOT)

[32] Legislation Proyecto de Ley General de Telecommunicaciones (Draft-LGT) June 1997

[33] Swedish Telecommunications Act 1993:597

[34] 1973:289

[35] Electronic Communications Privacy Act 1986, amending the Omnibus Crime Control and Safe Streets Act 1968

[36] Foreign Intelligence Surveillance Act 1978

[37] Communications Assistance for Law Enforcement Act 1994

[38] Review of the long-term cost effectiveness of telecommunications interception, report ot the Security Committee of the Federal Cabinet, March 1994

[39] Andersen MB and P Landrock, Juristen [1995] 306, summarised in English in Computer Law and Security Report [1996] 12 CLSR 342 at 348

[40] ss 34 to 37, Criminal Justice and Public Order Act 1994

EUROPEAN PARLIAMENT

**SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT**

STOA

# DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

**Vol 5/5**

**The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception**

**Working document for the STOA Panel**

**Luxembourg, October 1999** **PE 168.184/Vol 5/5**

*Cataloguing data*:

| | |
|---|---|
| **Title:** | **The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception** |
| **Workplan Ref.:** | **EP/IV/B/STOA/98/1401** |
| **Publisher:** | **European Parliament**<br>**Directorate General for Research**<br>**Directorate A**<br>**The STOA Programme** |
| **Author:** | **Mr Nikos Bogolikos - Zeus E.E.I.G** |
| **Editor:** | **Mr Dick HOLDSWORTH,**<br>**Head of STOA Unit** |
| **Date:** | **October 1999** |
| **PE number:** | **PE 168. 184 Vol 5/5** |

# TABLE OF CONTENTS

# PART A: OPTIONS

## *Introduction*

The present study entitled *'Development of surveillance technology and risk of abuse of economic information'* presents the outcomes from a survey of the opinions of experts, together with additional research and analytical material by the author. It has been conducted by ZEUS E.E.I.G. as part of a technology assessment project on this theme initiated by STOA in 1998 at the request of the Committee on Civil Liberties and Internal Affairs of the European Parliament. This STOA project is a follow up to an earlier one entitled: "**An appraisal of technologies of political control**" conducted on behalf the same Committee. The earlier project resulted in an Interim Study (PE 166.499) written by OMEGA Foundation, Manchester and published by STOA in January 1998 and updated September 1998.

In the earlier study was reported that within Europe all fax, e-mail and telephone messages are routinely intercepted by the ECHELON global surveillance system. The monitoring is "routine and indiscriminate". The ECHELON system forms part of the UKUSA system but unlike many of the electronic spy systems developed during the cold war, ECHELON is designed for primarily non-military targets: governments, organisations and businesses in virtually every country.

In the present study it was requested to examine the use of surveillance technology systems, for the collection and possible abuse of sensitive economic information.

The initial data came from the following sources:

- The analytical results from the Interim study of this project entitled: **'The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception' (PE 168.184/Int.St/part1/4)**. These results came out from a procedure of data collection and processing based on a modified DELPHI method (to be referred to here as "the first survey")[..].
- The outcomes from the following three brief,parallel studies, initiated by STOA in the first semester of 1999, as contribution to this final study:
  - "**The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law**", written by Prof. Chris Elliot and published by STOA in April 1999 (PE 168.184/Part2/4)
  - "**Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues**", written by Dr Franck Leprevot – Technische Universitaet Berlin and published by STOA in April 1999 (PE 168.184/Part3/4)
  - "**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 capability to COMINT targeting and selection, including speech recognition**", written by Mr Duncan Campbell – IPTV Ltd – Edinburg and published by STOA in April 1999 (PE 168.184/Part4/4)

The procedure of data processing was based on a modified DELPHI method (to be referred to here as 'The final survey").According to this method the main key-points from the first survey and the complementary studies were processed and a sorting examination performed. The next step was the collection of the opinions of the experts on the main topics. This was mostly achieved by direct interviews of the experts, with the use of a brief questionnaire. The views were further processed and a convergence examination performed. The convergence procedure was based on a recursive approach for the exclusion of the non-reliable data (Part B)

The last step was the drawing of the analytical results and the policy options for action from the European Parliament.

The Part C of this report covers in brief the following topics: the developments in surveillance technologies (physical and communications surveillance); the surveillance technology systems in operation (mainly ECHELON Connection); the nature of economic

information selected by surveillance technology systems; presentation of representative examples of abuse of economic information; the protection from electronic surveillance via encryption; and summary of the principal legal issues and instruments under international and European law.

## ***Key findings***

1. Comprehensive systems exist to access, intercept and process almost every important modern form of communication.
2. Cryptography is an important component of secure information and communication systems and a variety of application have been developed that incorporate cryptographic methods to provide data security.
3. Nowadays almost all economic information is exchanged through electronic means (telephone, fax, e-mail). All digital telecommunication devices and switches have enhanced wiretapping capabilities. As a conclusion we have to consider privacy protection in a global international networked society.
4. The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored in those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats such as unauthorised access and use, misappropriation, alteration and destruction.
5. Proliferation of computers, increased computing power, interconnectivity, decentralisation, growth of networks and the number of users, as well as the convergence of information and communication technologies, while enhancing the utility of these systems, also increase system vulnerability.
6. Compliance with rules governing the protection of privacy and personal data is crucial to establishing confidence in electronic transactions, and particularly in Europe, which has traditionally been heavily regulated in this area.
7. Although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities, which can affect public safety, national security, the enforcement of laws, business interests, consumers interests or privacy. Governments together with industry and the general public are challenged to develop balanced policies to address these issues.
8. Since Internet symbolising global commerce, faced with a rapid expansion in the numbers of transactions, there is a need to define a stable lasting framework for business. Internet is changing profound the markets and adjusting new contracts.
9. Common technological solutions can assist in implementing privacy and data protection guidelines in global information networks. The general optimism about technological solutions, the pressure to collect economic information and the need for political and social policy decisions to ensure privacy must be considered.
10. In a world of the Internet, the objectives of protecting both: privacy and free flow of information must be under consideration.
11. An active education strategy may be one of the ways to help achieve on-line and privacy protection and to give all actors the opportunities to understand their common interests.
12. Media could act as an effective watchdog, informing consumers and companies of what information is being collected about them and how that information is being used.
13. Multinational companies could better negotiate for themselves across national boundaries than governments can. Electronic commerce is unlikely to gain popularity until the issues of notice, consent and recourse have been resolved. The market will force companies wishing to participate in this medium to address and solve these concerns.
14. The growth in international networks and the increase in economic data processing have arisen the need at securing privacy protection in transborder data flows and especially the use of contractual solutions. Global E-Commerce has changed the nature of retailing. There were

great cultural and legal differences between countries affecting attitudes to the use of sensitive data (economic or personal) and the issue of applicable law in global transaction had tope resolved. Contracts might bridge the gap between those with legislation and the others.

15. To operate with confidence on the global networks, it is required some sort of governmental intervention to ensure data privacy.
16. There is no evidence that private companies from the countries, that routinely utilise communications intelligence, are able to task economic information collected by surveillance systems to suit their private purposes.
17. Information industry should be primarily self-regulated: the industry is changing too rapidly for government legislative solutions, and most corporations are not simply looking at National or European but at global markets, which national governments cannot regulate.
18. There is wide ranging evidence that major governments are routinely utilise communications intelligence to provide commercial advantages to companies and trade.
19. Recent diplomatic initiatives by the USA government seeking European agreement to the "key-escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non US nationals, including European governments, companies and citizens.

## ***Options:***

The policy options for consideration by the committee on Civil Liberties and Internal Affairs of the European Parliament, which came out of this study are:

- It would be useful for the governments of the E.U. to:
  - engage in a dialogue involving the private sector and individual users of networks in order to learn about their needs for implementing the privacy guidelines in the global network
  - undertake an examination of private sector technical initiatives
  - encourage the development of applications within global networks, of technological solutions that implement the privacy principles and uphold the right of users, businesses and consumers for protection of their privacy in the electronic environment.
- The current policy-making process should be made open to public and parliamentary discussion in member states and in the EP, so that a proper balance may be struck between the security and privacy rights of citizens and commercial enterprises, the financial and technical interests af communications network operators and service providers, and the need to support law enforcement activities intended to suppress serious crime and terrorism.
- Measures for encouraging the formal education systems of each member state of the E.U. or European Training Institute / Organisation to take up the general task of educating users in the technology and their rights.
- Definition of the transactions which must remain anonymous and the technical capabilities of providing anonymity should be recommended.
- Drafting methods for enforcing codes of conduct and privacy statements ranging from standardisation, labelling and certification in the global environment through third-party audit to formal enforcement by a regulatory body.
- Protective measures may best be focused on defeating hostile Communication Intelligence (Comint) activity by denying access or where it is impractical or impossible, preventing processing of message content and associated trafic information by general use of cryptography.

- Any failure to distinguish between legitimate law enforcement interception requirements and interception for clandestine intelligence purposes raises grave issues for civil liberties.
- Enforcement for the adoption of adequate standards (cryptography and key - encryption) from all E.U. member states. Multilateral agreements with other countries could then be negotiated.
- Drafting of common guidelines of credit information use (in each member state of the E.U. different restriction policies exist). It must be clear how those restrictions could apply to a globally operating credit reference agency.
- Drafting of common specifications for cryptography systems and government access key recovery systems, which must be compatible with large scale, economical, secure cryptographic systems.
- Enforcement for the adoption of special authorisation schemes for Information Society Services and supervision of their activities by National Authorisation Bodies.
- Drafting of a common responsibilities framework for on-line service providers, who transmit and store third party information. This could be drafted and supervised by National PTTs.
- To proceed to regularly updating, the technical documents published by European Institutions.
- European Parliament should carefully consider and possibly reject proposals from US for the elimination of cryptography and the adoption of encryption controls supervised by US Agencies.
- A course of action open to the EU is to require telecommunications operators to take greater precautions to protect their users against unlawful interception. This would appear to be possible without compromising law enforcement or electronic commerce.
- Annual statistics and reporting on abuse of economic information by any means must be reported to the Parliament of each member state of the E.U.

# PART B: ARGUMENTS AND EVIDENCE

The last step of the survey was the evaluation by the experts of the key findings. These key findings (19 in total) had emerged in the interim study and were complemented by the findings of the parallel studies [3], [4], [5]. This was achieved by directly interviewing them by means of a questionnaire and by telephone interrogation. Direct contact over the telephone was entirely used during the convergence stage of the recursive approach that was followed, for the exclusion of the non-reliable data and the clarification of some of the comments made by them. Initially, 47 experts were contacted, but only the 30 of them have contributed to the final survey.

The experts, mainly holding executive positions in their organisations, are working for Universities (47%), Industry (30%), Public Authorities (13%) and Research Centres (10%). In the "Industry" category, all those working in the private sector, independently of the size of the company, have also been included. Thirteen percent of the experts are women. The share of their age is as follows: 27% between 21-31 years old, 43% between 31-40, 20% between 41-50, 7% between 51-60 and 3% over 60 years old. It is seen that the vast majority of the experts are in the age of 31-40. This is because, those belonging to this range of ages, are the main actors in the information technology and at the same time are holding executive positions in their organisations. The next greater percentage belongs to the range of 21-30 years old, which is the generation that has really grown up within the information era. These persons have good knowledge of the technology possibilities and threats, but are still taking decisions in a restricted range. The ages between 41-50 are the third biggest percentage. They are those who decide, but their knowledge in technology, especially in Information Technology, is restricted. The above show that the sample of experts is well balanced, and their views contribute in a balanced way to each key finding. Concerning the nationality of the experts, 80% of them are coming from the E.U. and 20% from non E.U. countries, namely Cyprus, Norway, Switzerland and USA.

✓ The experts were asked whether they know that:
- *Comprehensive systems exist to access, intercept and process almost every important modern form of communication.*
- *Cryptography is an important component of secure information and communication systems and a variety of applications have been developed that incorporate cryptographic methods to provide data security.*

The answers in excess of 90% of them were positive. They know (indirectly) that such systems do exist, and they know or use cryptography as a means of secure communications, e.g. in tele-banking applications.

✓ The experts totally agree (nearly 100%) on the fact that:
- *Nowadays almost all economic information is exchanged through electronic means (telephone, fax, e-mail). All digital telecommunication devices and switches have enhanced wiretapping capabilities. As a conclusion we have to consider privacy protection in a global international networked society.*
- *The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored in those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats such as unauthorised access and use, misappropriation, alteration and destruction.*
- *Proliferation of computers, increased computing power, interconnectivity, decentralisation, growth of networks and the number of users, as well as the convergence of information and communication technologies, while enhancing the utility of these systems, also increase system vulnerability.*
- *Compliance with rules governing the protection of privacy and personal data is crucial to establishing confidence in electronic transactions, and particularly in Europe, which has traditionally been heavily regulated in this area.*

✓ Ninety percent (90%) of the experts agree on the following points:

- *Although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities, which can affect public safety, national security, the enforcement of laws, business interests, consumers interests or privacy. Governments together with industry and the general public are challenged to develop balanced policies to address these issues.*
- *Since Internet, symbolising global commerce, faced with a rapid expansion in the numbers of transactions, there is a need to define a stable lasting framework for business. Internet is changing profound the markets and adjusting new contracts.*
- *Common technological solutions can assist in implementing privacy and data protection guidelines in global information networks. The general optimism about technological solutions, the pressure to collect economic information and the need for political and social policy decisions to ensure privacy must be considered.*
- *In a world of the Internet, the objectives of protecting both: privacy and free flow of information must be under consideration.*
- *An active education strategy may be one of the ways to help achieve on-line and privacy protection and to give all actors the opportunities to understand their common interests.*

✓ The experts were also asked whether they agree or not with the following key-points.

- *Media could act as an effective watchdog, informing consumers and companies of what information is being collected about them and how that information is being used.*
- *Multinational companies could better negotiate for themselves across national boundaries than governments can. Electronic commerce is unlikely to gain popularity until the issues of notice, consent and recourse have been resolved. The market will force companies wishing to participate in this medium to address and solve these concerns.*
- *The growth in international networks and the increase in economic data processing have arisen the need at securing privacy protection in transborder data flows and especially the use of contractual solutions. Global E-Commerce has changed the nature of retailing. There were great cultural and legal differences between countries affecting attitudes to the use of sensitive data (economic or personal) and the issue of applicable law in global transaction had tope resolved. Contracts might bridge the gap between those with legislation and the others.*
- *To operate with confidence on the global networks, it is required some sort of governmental intervention to ensure data privacy.*
- *Private companies from those countries are able to task economic information collected by surveillance systems to suit their private purposes.*

A percentage of 60 to 77 of them replied positively. Those who replied negatively ranged between 15 to 22%, while there was a small number of 4 to 24%, that were unaware of that particular point.

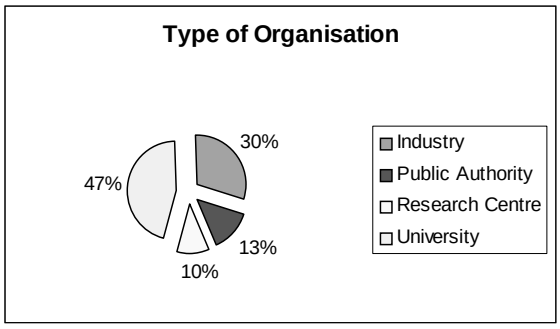
✓ Continuing the analysis of the results, it was found that the opinions on whether "*the information industry should be primarily self-regulated*", share the same percentage, i.e. approximately 42% positive, 41% negative, while the rest 17% couldn't give a certain answer.

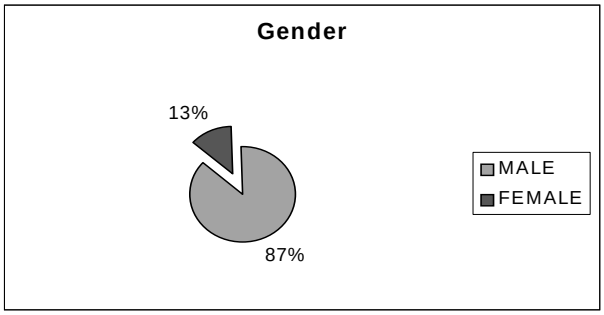
✓ Concerning the point that "*major governments are routinely utilising communications intelligence to provide commercial advantages to companies and trade*", in one third of the cases we had no concrete reply, 40% were sure that this is done, whereas 27% were sure that this is not the case.

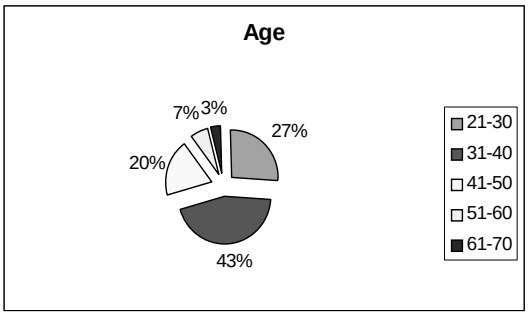
✓ Finally, with regard to the point that "*recent diplomatic initiatives by the USA government seeking European agreement to the "key-escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non US nationals, including European governments, companies and citizens*", almost half of them (approximately 47%) had no clear idea on this. However, 33% of the experts knew that this is the case and only 20% did not agree with the point.

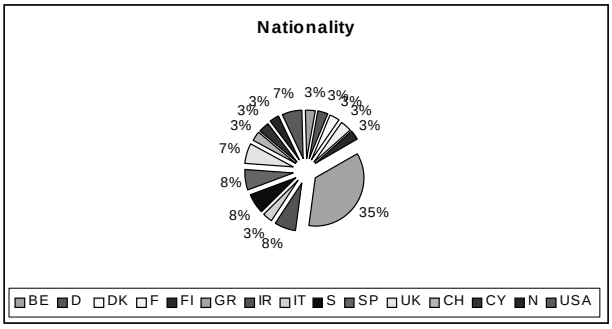
As a result, we could say that experts do agree on all these points and they see that actions have to be taken in order to balance the explosion of the information flow and the need for secure communications. No additional points were proposed.

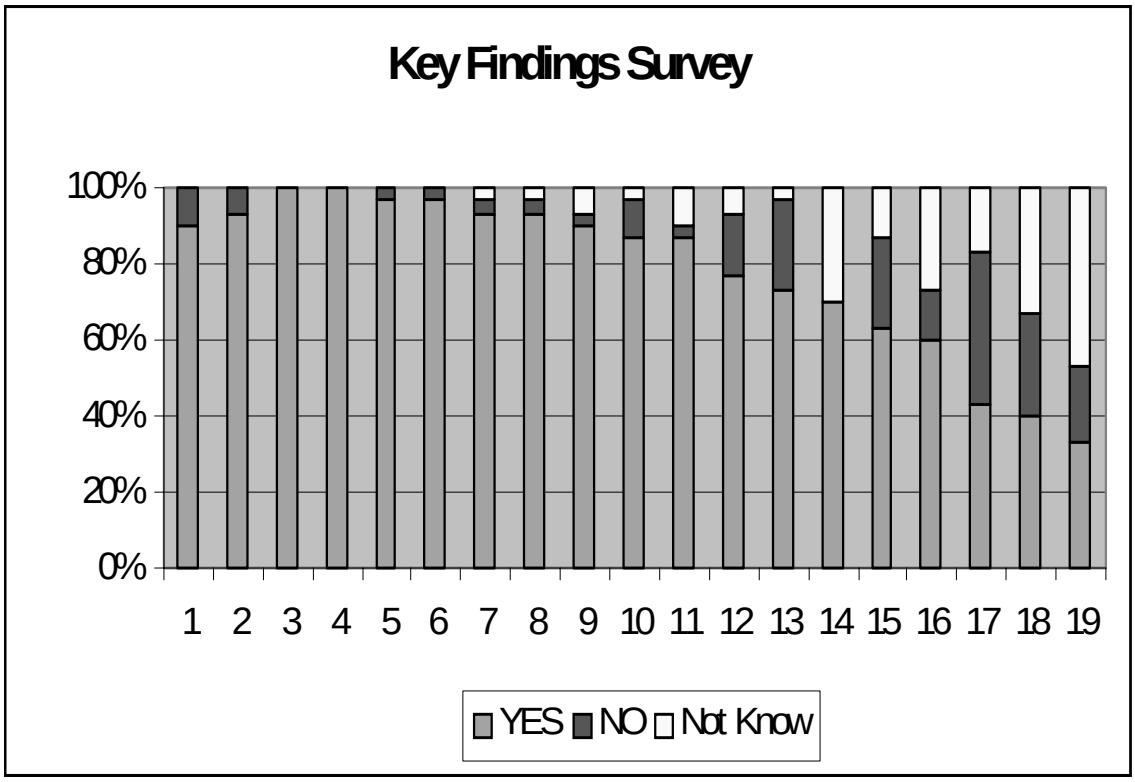
The graphical representation of the experts' data and their responses, are given in the following figures.


Type of Organisation
30%
47%
13%
10%
Industry
Public Authority
Research Centre
University


Gender
13%
87%
MALE
FEMALE


Age
7%
3%
27%
20%
43%
21-30
31-40
41-50
51-60
61-70


Nationality
35%
BE
D
DK
F
FI
GR
IR
IT
S
SP
UK
CH
CY
N
USA


Key Findings Survey
100%
80%
60%
40%
20%
0%
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
YES
NO
Not Know

# PART C: TECHNICAL FILE

## 1. DEFINITIONS

Surveillance is the systematic investigation or monitoring of the actions or communications of one or more persons.

The basic born physical surveillance comprises watching (visual surveillance) and listening (aural surveillance).

In addition to physical surveillance, several kinds of communications surveillance are practiced, including mail covers and telephone interception.

The popular term electronic surveillance refers to both augmentations to physical surveillance (such as directional microphones and audio bugs) and to communication surveillance, particularly telephone taps.

Data surveillance or Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Dataveillance is of two kinds: "personal Dataveillance", where a particular person has been previously identified as being of interest, "mass Dataveillance", where a group or large population is monitored, in order to detect individuals of interest, and / or to deter people from stepping out of line.

Surveillance technology systems are mechanisms, which can identify, monitor and track movements and data.

Privacy is the interest that individuals have in sustaining a "personal space" free from interference by other people and organizations.

Information privacy or data privacy is the interest an individual has in controlling, or at least significantly influencing the handling of data about themselves.

'Confidentiality is the legal duty of individuals who come into the procession of information about others, especially in the course of particular kinds of relationships with them'.

## 2. SURVEILLANCE: TOOLS AND TECHNIQUES - The State Of The Art

### *1. Physical Surveillance*

Electronic devices have been developed to augment physical surveillance and offer new possibilities such as [2]:

- Closed – circuit TV (CCTV)
- Video Coding Recorder (VCR)
- Telephone bugging,
- Proximity smart cards
- Transmitter Location
- E-mail at workplace
- Electronic Databases, etc.

### *2. Communications Surveillance*

Communication Intelligence (Comint) involving the covert interception of foreign communications has been practiced by almost every advanced nation since international communications became available.

NSA (National Security Agency, USA), the largest agency conducting such operations as "technical and intelligence information derived from foreign communications by other than their intended recipient", defines Comint.

Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments. The major English speaking nations of

UKUSA alliance supports the largest Comint organisation. Besides UKUSA, there at least 30 other nations operating major Comint organisations. The largest is the Russian FAPSI, with 54.000 employees. China maintains a substantial Signal Intelligence (Signit) system, two station of which are directed at Russia and operate in collaboration with the USA. Most Middle eastern and asian nations have invested substantially in Signit, in particular Israel, India and Pakistan [5].

Comint organisations use the term International Leased Carrier (ILC) to describe the interception of international communications. [5].

The ILC communication collection (Comint Collection) cannot take place unless the collecting agency obtains access to the communications channels they wish to examine. Information about the means used to gain access are, like data about code breaking methods, the most highly protected information within any Comint organisation. Access is gained both with and without the complicity of the cooperation of network operators.

Different activities for this purpose have been developed [5] like:

- Operation SHAMPROCK
- High frequency radio interception
- Space interception
- Signit satellites
- COMSAT ILC collection
- Submarine cable interception
- Intercepting the Internet
- Covert collection of high capacity signals
- New satellite networks

Apart from global surveillance technology systems, additional tools have been developed for surveillance. The additional tool used for information transferred via Internet or via Digital Global telecommunication systems is the capture of data with Taiga software. Taiga software has the possibility to capture, process and analyse multilingual information in a very short period of time (1 billion characters per second), using key-words.

## 3. THE USE OF SURVEILLANCE TECHNOLOGY SYSTEMS FOR THE TRANSMISSION AND COLLECTION OF ECONOMIC INFORMATION

As the Internet and other communication systems reach further into the everyday lives, national security, law enforcement and individual privacy have become perilously intertwined. Governments want to restrict the free flow of information and software producers are seeking ways to ensure consumers are not bugged from the moment of purchases.

All developing communication technologies, digital telephone switches cellular and satellite phones HAVE SURVEILLANCE CAPABILITIES. On the other hand the development of software that contains encryption, a telephone which allows people to scramble their communications and files to prevent others from reading them gained earth.

### ***1. CALEA system***

The first effort to heighten surveillance opportunities (made by USA) was to force telecommunication companies to use equipment desired to include enhanced wiretapping capabilities.

### ***2. ECHELON Connection***

The highly automated UKUSA system for processing Comint, often known as ECHELON system was brought to light by the author Nicky Hager in his 1996 book, *"Secret Power: New Zealand's role in the International Spy Network"*. For this, he interviewed more than 50 people


ii

who work or have worked in intelligence who are concerned at the uses of ECHELON. It is said, " The ECHELON system is not designed to eavesdrop on a particular individual's e-mail or fax link. Rather the system works by indiscriminately intercepting very large quantities of communications and using computers to identify and extract messages from the mass of unwanted ones".

ECHELON became well known following the previous STOA Interim study (PE 166.499) entitled "An Appraisal of technologies of political control". In this reported to be a world wide surveillance system designed and coordinated by NSA, USA, that intercepts e-mail, fax, telex and international telephone communications carried via satellites and has been operating since the early 1980's – it is part of the post Cold war developments based on the UKUSA agreement signed between the UK, USA, Canada, Australia and New Zealand in 1948.

According to the Interim study (PE 166.499) of 1998, there are reported to be three components to ECHELON:

- The monitoring of Intelsats, international telecommunications satellites used by phone companies in most countries. A key ECHELON station is at Morwenstow in Cornwall monitoring Europe, the Atlantic and the Indian Ocean.
- ECHELON interception of non-Intelsat regional communication satellites. Key monitoring stations are Menwith Hill in Yorkshire and Bad Aibling in Germany
- The final element of the ECHELON system is the surveillance of land-based or under-sea systems, which use cables or microwave tower networks.

Each of the five centers supply to the other four "Dictionaries" of keywords, phrases, people and places to "tag" and tagged intercept is forwarded straight to the requesting country.

The STOA report 1999, prepared as contribution to this study, entitled "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", (PE 168.184/part3/4), is providing new documentary and information evidence about ECHELON. In this is reported that:

- In the mid 1980s, extensive further automation of ECHELON Comint processing was planned by NSA as project P-415.
- The key components of the new system are "Local Dictionary computers" which store en extensive database on specific targets. An important point about the new system is that before ECHELON, different countries and different countries and different stations knew what was being intercepted and to whom it was sent. Now, all but a fraction of the messages selected by Dictionary computers at remote sites are forwarded to NSA or other customers without being read locally.
- A dictionary computer is operating at GCHQ's (Government Communications Headquarters; the Signit agency of the UK) Westminster, London office. The system intercepts thousands of diplomatic, business and personal messages every day. The presence of dictionary computers has also been confirmed at Kojarena, Australia; and at GCHQ's Cheltenham, England.
- There are satellite receiving stations in Sugar Grove/Virginia, Sabana Seca /Puerto Rico and Leitrim / Canada working also as ECHELON interception sites.
- New Zealand signit agency operates two satellite interception terminals at Waihopai covering the pacific Ocean which are working as ECHELON interception sites as well.

## ***3. Inhabitant identification Schemes***

Inhabitant identification schemes are schemes, which provide all, or most people in the country with a unique code and a token (generally a card) containing the code.

Such schemes are used in many European Countries for a defined set of purposes, typically the administration of taxation, natural superannuation and health insurance. In some countries, they are used for multiple additional purposes.


iii

## 4. THE NATURE OF ECONOMIC INFORMATION SELECTED BY SURVEILLANCE TECHNOLOGY SYSTEMS

Advances in information and communication technologies have fostered the development of complex national and international networks which enable thousands of geographically dispersed users to distribute, transmit, gather and exchange all kinds of data. Transborder electronic exchanges -private, professional, industrial and commercial- have proliferated on a global scale and are bound to intensify among businesses and between businesses and consumers, as electronic commerce develops. At the same time developments in digital computing have increased the capacity for accessing, gathering, recording, processing, sorting, comparing and linking alphanumeric, voice and image data. This substantial growth in international networks and the increase in economic data processing have arisen the need at securing privacy protection in transborder data flows.

There is wide ranging evidence indicated that governments from UKUSA alliance countries are using global surveillance systems to provide commercial advantage to companies and trade.

Each UKUSA country authorises national level intelligence assessment organisatios and relevant individual ministries to task and receive economic intelligence for Comint. Such information may be collected for a lot of purposes such as:

Estimation of future essential commodity prices, determining other nation's private positions in trade negotiations, tracking sensitive technology or evaluating the political stability and/or economic strength of a target country.

Any of these targets and many others may produce intelligence of direct commercial relevance. The decision as to whether it should be disseminated or exploited is taken not by Comint but by national government organisation.

On the other hand there is no evidence that companies in any of UKUSA countries are able to task Comint collection to suit their private purposes [5].

The growth in international networks and the increase in economic data processing have arisen the need at securing privacy protection in transborder data flows and especially the use of contractual solutions. Global E-Commerce has changed the nature of retailing. There were great cultural and legal differences between countries affecting attitudes to the use of sensitive data (economic or personal) and the issue of applicable law in global transaction had tope resolved. Contracts might bridge the gab between those with legislation and the others.

Since Internet symbolised global commerce, faced with a rapid expansion in the numbers of transactions, there is a need to define a stable lasting framework for business. Internet is changing profound the markets and adjusting new contracts. To that reality is a complex problem.

Internet is a «golden highway», for those interested in the process of information. On the other hand since Internet symbolised global commerce could be a tool of misleading information and a platform for deceitful advertisement.

### ***Examples of Abuse of Economic Information***

Various examples could be mentioned about abuse of privacy via global surveillance telecommunication systems (like ECHELON). A number of them is given in [58].

Many accounts have been published by reputable journalists citing frequent occasions on which the US government has utilised Comint for national purposes. The examples given below are the most representative.

***Example 1:***

On January 15, 1990, the telephone network of AT&T company, in all the North-east part of USA faced serious difficulties. The network NuPrometheus had illegally owned and distributed the key-code of the operational system of AT&T Macintosh computer (Apple company).


iv

*J.P. Barlow: «A not terribly brief history of the Electronic Frontier Foundation, 8 November 1990»*

***Example 2:***

On January 24, 1990, the Electronic Frontier Foundation (EEF) in USA, accused a huge police operation under the encoded name «Sun Devil», in which 40 computers and 23,000 diskettes were seizure from teenagers, in 15 towns within USA. Teenager Graig Neidorf supported by EEF, not to be punished in 60 years prison and 120,000 USD penalty. Craig Neidorf had published in Phrake (a hackers magazine) part of the internal files of a telephone company.

*M. Godwin: «The EEF and virtual communities», 1991*

***Example 3:***

On June 25, 1998, in Absheim, an aircraft A-320 of the European Company «Airbus Industries», was crushed during a demonstration flight. The accident caused due to dangerous manipulations. One person died and 20 were injured.

Very soon, and before the announcement of the official report, in the aerospace and transport Internet newsgroups, appeared a lot of aggressive messages against company Airbus and against the French company Aerospatiale as well, with which Airbus had close co-operation. Messages declared that, the accident was expectable because European Engineers are not so highly qualified as American Engineers are. It was also clearly stated, that in the future similar accidents are expected.

Aerospatiale's agents were very impressive with these aggressive messages. They tried to discover the sources of messages and they finally realised that senders' identification data, addresses and nodes were false. The source messages came from USA, from computers with misled identification data and transferred from anonymous servers in Finland.

In this case Aerospatiale has arguments to insist in that American BOEING implemented one of the biggest misinform campaigns over the Internet.

*B. Martinet and Y.M. Marti: «L' intelligence econimique. Les yeux et les oreilles de l' enteprise, Editions d' organisation», Paris 1995*

***Example 4:***

In October 31, 1994, in USA, an accident in an ATR aircraft (of the European Consortium Aeritalia and Aerospatiale) happened. Due to this accident, a ban of ATR flights for two months imposed. This decision became catastrophic on commercial level for the company, because ATR obliged to carry out test flights in fog conditions.

During this period, in Internet newsgroups (and especially in AVSIG forum, supported by Compuserve), the exchange of messages was of vital significance. The arguments supported the European company were a few. On the other hand, the arguments against ATR were a lot.

At the beginning of January 1995, appeared a message from a journalist in this forum asking the following: «I have heard that ATR flights will begin soon. Can anybody confirm this information?» The answer came very soon. Three days after, unexpectable, permission to ATR flights was given. The company learned this, as soon as the permission announced. But if they have actively participated in the newsgroups, they would have gained some days to inform their offices and their clients...

*«Des langages pour analyser la poussiere d' info», Liberation, 9 June 1995*

***Example 5:***

The government of Brasil in 1994, announced its intention to assign an international contract for the reconstruction of the overhead supervision of Anazonios. This procurement was of great interest since the total amount available for the contract was 1,4 billion USD. From Europe, the French companies Thomson and Alcatel expressed their interest and from USA, the huge weapon industry Raytheon.

Although, the offer of French companies was technically perfect and better documented, the contract eventually was assigned to the USA company.

This was achieved with a new offensive strategy used by USA:

When the government of Brazil was about to assign the contract to the French companies, American Officials' (with the personal involvement of President Bill Clinton) readjusted their offer, according to the offer of the European companies, asserted that, French companies occurred the committee, an accuse which never proved. On the other hand, European companies have arguments, that, the intention of the government of Brazil to assign the contract to the European companies became known to Americans with the use of FBI's surveillance technologies (ECHELLON system).

*«La nouvelle machine de querre americaine», LeMonde du reseingnement no 158, 16 February 1995.*

***Example 6:***

In January 1994 Edouard Balladur went to Ryad (Saudi Arabia), it was certain to bring back a historical contract for more than 30 million francs in sales of weapons and, especially, Airbus. He re-entered bredouille.

The contract went to the McDonnell-Douglas American company, rival of Airbus. Partly, showed the French, thanks to electronic listening of the Echelon system, which had given to the Americans the financial conditions (and the bribes) authorised by Airbus. This information is collected and analysed by the batteries of hidden supercomputers behind the black panes of a cubic building that is visible the node through the pines, when one rolls on the motorway between Washington and Baltimore. Fort Meade (Maryland), head office of the NSA.

The National Security Agency is most secret and most significant of the thirteen secretes of the United States. It receives about a third of the appropriations allocated with espionage: 8 of the 26,6 billion dollars (160 billion francs) registered voters to the budget 1997. With its 20.000 employee in United States and some thousand of agent throughout le world, the NSA (which form part of ministry for Defence since its creation in 1956) is more important than the CIA, however much more known.

Fort Meade contains, according to sources' familiar of the places, the greatest concentration of data processing power and math student in the world. They are charged to sort and analyse the flood of data aspired by Echelon on the networks of international telecommunications. "There are not only one diplomatic event or soldier concerning the United States in which the NSA is not directly implied ", recognised in 1996 the director of the agency, John McConnel". The NSA plays a very significant role as regards economic espionage", affirms John Pike, expert of the information in Federation of American Scientist, which specifies "Echelon is in the heart of its operations". In 1993, a direct president of the agency, the admiral William Studeman, had recognised, in a confidential document, that " the requests for a total access to information do not cease growing ", while at the same time the Soviet military threat grew blurred. Economic espionage justifies in fact the maintenance of an oversize apparatus since the end of the cold war.

Admittedly, Nicky Hager, who reveal in 1996 the existence of Echelon, said not to have "an evidence that the military circles (terrorism, proliferation of the armaments, espionage economic, note) became priorities for the NSA ".

*«Echelon est au service des interets americains», Liberation, 21 April 1998*


vi

## 5. PROTECTION FROM ELECTRONIC SURVEILLANCE

Electronically managed information touches almost every aspect of daily life in modern society. This rising tide of important yet unsecured electronic data leaves our society increasingly vulnerable to curious neighbors, industrial spies, rogue nations, organized crime, and terrorist organizations.

Encryption is an essential tool in providing security in the information age. Encryption is based on the use of mathematical procedures to scramble data so that it is extremely difficult - - if not virtually impossible - - for anyone other than authorized recipients to recover the original 'plain text'. Properly implemented encryption allows sensitive information to be stored on insecure computers or transmitted across insecure networks. Only parties with the correct decryption 'key' (or keys) are able to recover the plain text information.

Encryption is the practice of encoding data so that even if a computer or network is compromised, the data's content will remain secret. Security and encryption issues are important because they are central to public confidence in networks and to the use of the systems for the sensitive or secret data, such as the processing of information touching on national security. These issues are surpassingly controversial because of governments' interest in preventing digital information from being impervious to official interception and decoding for law enforcement and other purposes.

Cryptography is a complex area, with scientific, technical, political, social, business, and economic dimensions.

For the purpose of this report, 'key recovery' systems are characterized by the presence of some mechanism for obtaining exceptional access to the plain text of encrypted traffic. Key recovery might serve a wide spectrum of access requirements, from a backup mechanism that ensures a business' continued access to its own encrypted archive in the event keys are lost, to providing covert law enforcement access to wiretapped encrypted telephone conversations. Many of the costs, risks, and complexities inherent in the design, implementation, and operation of key recovery systems depend on the access requirements around which the system is designed.

The Global Information Infrastructure promises to revolutionize electronic commerce, reinvigorate government, and provide new and open access to the information society. Yet this promise cannot be achieved without information security and privacy. Without a secure and trusted infrastructure, companies and individuals will become increasingly reluctant to move their private business or personal information online.

## 6. SURVEILLANCE TECHNOLOGY SYSTEMS IN LEGAL AND REGULATORY CONTEXT

Europe is the site of the first privacy legislation, the earliest national privacy statute, and now the most comprehensive protection for information privacy in the world. That protection reflects on apparent consensus within Europe that privacy is a fundamental human right which few in any other rights equal. In the context of European history and civil law culture, that consensus makes possible extensive, detailed regulation of virtually all activities concerning 'any information relating to an identified or identifiable natural person'. It is difficult to imagine a regulatory regime offering any greater protection to information privacy, or greater contrast to U.S. law.

As a result of the variation and uneven application among national laws permitted by both the guidelines and the convention, in July 1990 the commission of the then-European Community (EC) published a draft *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on Free Movement of Such Data.* The draft directive was part of the ambitious program by the countries of the European Union to create not merely the


vii

'common market' and 'economic and monetary union' contemplated by the Treaty of Rome, but also the potential union embodied in the Treaty on European Union signed in 1992 in Maastricht.

**Directive** 97/66/EC of the European Parliament and the Council of the 15 December 1997 concerns the processing of personal data and the protection of privacy in the telecommunications sector.

This directive provides for the harmonisation of the provisions of the member states required to ensure an equivalent level of protection of fundamental rights and freedom, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and telecommunications equipment and services in the Community.

The protection for the information privacy in the United States is disjoined, inconsistent, and limited by conflicting interests. There is no explicit constitutional guarantee of a right to privacy in the United States. Although the Supreme Court has fashioned a variety of rights, 'information privacy' has received little protection [9].

Outside of the constitutional arena, protection for information privacy relies on hundreds of federal and state laws and regulations, each of which applies only to a specific category of information user (such as the government or retailers of videotapes), context (applying for credit or subscribing to cable television), type of information (criminal records or financial information), or use for that information (computer matching or impermissible discrimination). Privacy laws in the United States most often prohibit certain disclosures, rather than collection, use, or storage, of personal information. When those protections extend to the use of personal information, it is often as a by-product of legislative commitment to another goal, such as eliminating discrimination. And the role provided for the government in most U.S. privacy laws is often limited to providing a judicial form for resolving disputes.

Privacy of communicators in one of the fundamental human rights. The UN Declaration, International Covenant and European Convention all provide that natural persons should not be subject to unlawful interference with their privacy. The European Convention is legally binding and has caused signatories to change their national laws to comply.

Most countries, including most EU Member States, have a procedure to permit and regulate lawful interception of communications, in furtherance of law enforcement or to protect national security. The European Council has proposed a set of technical requirements to be imposed on telecommunications operators to allow lawful interception. USA has defined similar requirements (now enacted as Federal law) and Australia has proposed to do the same.

Most countries have legal recognition of the right to privacy of personal data and many require telecommunications network operators to protect the privacy of their users. All EU countries permit the use of encryption for data transmitted via public telecommunications networks (except France where this will shortly be permitted).

Electronic commerce requires secure and trusted communications and may not be able to benefit from privacy law designed only to protect natural persons.

The legal regimes reflect a balance between three interests:

Privacy;
Law enforcement;
Electronic commerce.

Legal processes are emerging to satisfy the second and third interests by granting more power to governments to authorise interception (under legal controls) and allowing strong encryption with secret keys.

There do not appear to be adequate legal processes to protect privacy against unlawful interception, either by foreign governments or by non governmental bodies [2],[3].

## ***Law Enforcement Data Interception - Policy Development***


viii

As the Internet and other communications systems reach further into everyday lives, national security, law enforcement and individual privacy have become perilously intertwined. Governments want to restrict the free flow of information; software producers are seeking ways to ensure consumers are not bugged from the very moment of purchase. The US is behind a world-wide effort to limit individual privacy and enhance the capability of its intelligence services to eavesdrop on personal conversations. The campaign has had two legal strategies: the first made it mandatory for all digital telephone switches, cellular and satellite phones and all developing communication technologies to build in surveillance capabilities; the second sought to limit the dissemination of software that contains encryption, a technique which allows people to scramble their communications and files to prevent others from reading them. The first effort to heighten surveillance opportunities was to force telecommunications companies to use equipment designed to include enhanced wiretapping capabilities. The end goal was to ensure that the US and its allied intelligence services could easily eavesdrop on telephone networks anywhere in the world. In the late 1980s, in a programme known internally as 'Operation Root Canal', US law enforcement officials demanded that telephone companies alter their equipment to facilitate the interception of messages. The companies refused but, after several years of lobbying, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994.

CALEA requires that terrestrial carriers, cellular phone services and other entities ensure that all their 'equipment, facilities or services' are capable of 'expeditiously... enabling the government...to intercept... all wire and oral communications carried by the carrier...concurrently with their transmission.' Communications must be interceptable in such a form that they could be transmitted to a remote government facility.

Manufacturers must work with industry and law enforcement officials to ensure that their equipment meets federal standards. A court can fine a company US$10,000 per day for each product that does not comply.

The passage of CALEA has been controversial but its provisions have yet to be enforced due to FBI efforts to include even more rigorous regulations under the law. These include the requirement that cellular phones allow for location-tracking on demand and that telephone companies provide capacity for up to 50,000 simultaneous wiretaps.

While the FBI lobbied Congress and pressured US companies into accepting a tougher CALEA, it also leant on US allies to adopt it as an international standard. In 1991, the FBI held a series of secret meetings with EU member states to persuade them to incorporate CALEA into European law. The plan, according to an EU report, was to 'call for the Western World (EU, US and allies) to agree to norms and procedures and then sell their products to Third World countries. Even if they do not agree to interception orders, they will find their telecommunications monitored by the UK-USA signals intelligence network the minute they use the equipment.' The FBI's efforts resulted in an EU Council of Ministers resolution that was quietly adopted in January 1995, but not publicly released until 20 months later. The resolution's text is almost word for word identical to the FBI's demands at home. The US government is now pressuring the International Telecommunications Union (ITU) to adopt the standards globally.

Since 1993, unknown to European parliamentary bodies and their electors, law enforcement officials from many EU countries and most of the UKUSA nations have been meeting annually in a separate forum to discuss their requirements for interceptingcommunications. These officials met under the auspices of a hitherto unknown organisation, ILETS (International Law Enforcement Telecommunications Seminar). ILETS was initiated and founded by the FBI.

At their 1993 and 1994 meetings, ILETS participants specified law enforcement user requirements for communications interception. These appear in a 1974 ILETS document called "IUR 1.0". This document was based on an earlier FBI report on "Law Enforcement Requirements for the Surveillance of Electronic Communications", first issued in July 1992 and revised in June 1994.


ix

The IUR requirement differed little in substance from the FBI's requirements but was enlarged, containing ten requirements rather than nine. IUR did not specify any law enforcement need for "key escrow" or "key recovery". Cryptography was mentioned solely in the context of network security arrangements.

Between 1993 and 1997 police representatives from ILETS were not involved in the NSA-led policy making process for "key recovery", nor did ILETS advance any such proposal, even as late as 1997. Despite this, during the same period the US government repeatedly presented its policy as being motivated by the stated needs of law enforcement agencies. At their 1997 meeting in Dublin, ILETS did not alter the IUR. It was not until 1998 that a revised IUR was prepared containing requirements in respect of cryptography. It follows from this that the US government misled EU and OECD states about the true intention of its policy.

This US deception was, however, clear to the senior Commission official responsible for information security. In September 1996, David Herson, head of the EU Senior Officers' Group on Information Security, stated his assessment of the US "key recovery" project:

"*'Law Enforcement' is a protective shield for all the other governmental activities ... We're talking about foreign intelligence, that's what all this is about. There is no question [that] 'law enforcement' is a smoke screen"*

It should be noted that technically, legally and organisationally, law enforcement requirements for communications interception differ fundamentally from communications intelligence. Law enforcement agencies (LEAs) will normally wish to intercept a specific line or group of lines, and must normally justify their requests to a judicial or administrative authority before proceeding. In contract, Comint agencies conduct broad international communications "trawling" activities, and operate under general warrants. Such operations do not require or even suppose that the parties they intercept are criminals. Such distinctions are vital to civil liberty, but risk being eroded it the boundaries between law enforcement and communications intelligence interception becomes blurred in future.

Following the second ILETS meeting in Bonn in 1994, IUR 1.0 was presented to the Council of Ministers and was passed without a single word being altered on 17January 1995.(57) During 1995, several non EU members of the ILETS group wrote to the Council to endorse the (unpublished) Council resolution. The resolution was not published in the Official Journal for nearly two years, on 4 November 1996.

Following the third ILETS meeting in Canberra in 1995, the Australian government was asked to present the IUR to International Telecommunications Union (ITU). Noting that "law enforcement and national security agencies of a significant number of ITU member states have agreed on a generic set of requirements for legal interception", the Australian government asked the ITU to advise its standards bodies to incorporate the IUR requirements into future telecommunications systems on the basis that the "costs of providing legal interception capability and associated disruptions can be lessened by providing for that capability at the design stage".

It appears that ILETS met again in 1998 and revised and extended its terms to cover the Internet and Satellite Personal Communications Systems such as Iridium. The new IUR also specified "additional security requirements for network operators and service providers", extensive new requirements for personal information about subscribers, and provisions to deal with cryptography.

On 3 September 1998, the revised IUR was presented to the Police Co-operation Working Group as ENFOPOL 98. The Austrian Presidency proposed that, as in 1994, the new IUR be adopted verbatim as a Council Resolution on interception "in respect of new technology".(59) The group did not agree. After repeated redrafting, a fresh paper has been prepared by the German Presidency, for the eventual consideration of Council Home and Justice ministers.

The second part of the strategy was to ensure that intelligence and police agencies could understand every communication they intercepted. They attempted to impede the development

of cryptography and other security measures, fearing that these technologies would reduce their ability to monitor the emissions of foreign governments and to investigate crime.

These latter efforts have not been successful. A survey by the Global Internet Liberty Campaign (GILC) found that most countries have either rejected domestic controls or not addressed the issue at all. The GILC found that 'many countries, large and small, industrialised and developing, seem to be ambivalent about the need to control encryption technology'.

The FBI and the National Security Agency (NSA) have instigated efforts to restrict the availability of encryption world-wide. In the early 1970s, the NSA's pretext was that encryption technology was 'born classified' and, therefore, its dissemination fell into the same category as the diffusion of A-bomb materials. The debate went underground until 1993 when the US launched the Clipper Chip, an encryption device designed for inclusion in consumer products. The Clipper Chip offered the required privacy, but the government would retain a 'pass-key' – anything encrypted with the chip could be read by government agencies.

Behind the scenes, law enforcement and intelligence agencies were pushing hard for a ban on other forms of encryption. In a February 1993 document, obtained by the Electronic Privacy Information Center (EPIC), they recommended 'Technical solutions, such as they are, will only work if they are incorporated into all encryption products'.

To ensure that this occurs, legislation mandating the use of government-approved encryption products, or adherence to government encryption criteria, is required.' The Clipper Chip was widely criticised by industry, public interest groups, scientific societies and the public and, though it was officially adopted, only a few were ever sold or used.

From 1994 onwards, Washington began to woo private companies to develop an encryption system that would provide access to keys by government agencies. Under the proposals – variously known as `key escrow', `key recovery' or `trusted third parties' – the keys would be held by a corporation, not a government agency, and would be designed by the private sector, not the NSA. The systems, however, still entailed the assumption of guaranteed access to the intelligence community and so proved as controversial as the Clipper Chip. The government used export incentives to encourage companies to adopt key escrow products: they could export stronger encryption, but only if they ensured that intelligence agencies had access to the keys.

Under US law, computer software and hardware cannot be exported if it contains encryption that the NSA cannot break. The regulations stymie the availability of encryption in the USA because companies are reluctant to develop two separate product lines – one, with strong encryption, for domestic use and another, with weak encryption, for the international market. Several cases are pending in the US courts on the constitutionality of export controls; a federal court recently ruled that they violate free speech rights under the First Amendment.

The FBI has not let up on efforts to ban products on which it cannot eavesdrop. In mid-1997, it introduced legislation to mandate that key-recovery systems be built into all computer systems. The amendment was adopted by several congressional Committees but the Senate preferred a weaker variant. A concerted campaign by computer, telephone and privacy groups finally stopped the proposal; it now appears that no legislation will be enacted in the current Congress.

While the key escrow approach was being pushed in the USA, Washington had approached foreign organisations and states. The lynchpin for the campaign was David Aaron, US ambassador to the Organisation for Economic Co-operation and Development (OECD), who visited dozens of countries in what one analyst derided as a programme of `laundering failed US policy through international bodies to give it greater acceptance'.

Led by Germany and the Scandinavians, the EU has been generally distrustful of key escrow technology. In October 1997, the European Commission released a report which advised: `Restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not, however, totally prevent criminals


xi

from using these technologies.'The report noted that privacy considerations suggest limit the use of cryptography as a means to ensure data security and confidentiality'.

Some European countries have or are contemplating independent restrictions. France had a long-standing ban on the use of any cryptography to which the government does not have access. However, a 1996 law, modified the existing system, allowing a system of "tiers du confidence", although it has not been implemented, because of EU opposition. In 1997, the Conservative government in the UK introduced a proposal creating a system of trusted third parties.

It was severely criticised at the time and by the new Labour government, which has not yet acted upon its predecessor's recommendations. The debate over encryption and the conflicting demands of security and privacy are bound to continue. The commercial future of the Internet depends on a universally-accepted and foolproof method of on-line identification; as of now, the only means of providing it is through strong encryption. That put the US government and some of the world's largest corporations, notably Microsoft, on a collision course. (Report of David Banisar, Deputy director of Privacy International and Simon Davies, Director General of Privacy International).

The issue of encryption divides the member states of the European Union. Last October the European Commission published a report entitled: "Ensuring security and Trust in Electronic Commerce", which argued that the advantages of allowing law enforcement agencies access to encrypted messages are not clear and could cause considerable damage to the emerging electronic industry. It says that if citizens and companies "fear that their communications and transactions are being monitored with the help of key access or similar schemes unduly enlarging the general surveillance possibility of government agencies, they may prefer to remaining in the anonymous offline world and electronic commerce will just not happen".

However, Mr Straw said in Birmingham (JHA Informal Ministers) that: "It would not be in the public interest to allow the improper use of encryption by criminals to be totally immune from the attention of law enforcement agencies". The UK, along with France (which already has a law obliging individuals to use "crackable" software) and the USA, is out on a limb in the EU. "The UK presidency has a particular view and they are one of the access hard-liners. They want access: "them and the French", commented an encryption expert. They are particularly about "confidential services" which ensure that a message can only be read by the person for whom it is intended who has a "key" to access it. The Commission's report proposes "monitoring" Member States laws' on "confidential services" to ensure they do not contravene the rules of the single market.


xii

# 7. REFERENCES


1. STOA, PE 166499: "An appraisal of technologies of political control", 1998.
2. STOA, PE 168.184 /Int.St/part 1/4: "The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception", 1999.
3. STOA, PE 168.184 /Int.St/part 2/4: " The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law", 1999.
4. STOA, PE 168.184 /Int.St/part 3/4: "Encryption and cryptosystems in electronic surveillance: asurvey of the technology assessment issues", 1999.
5. STOA, PE 168.184 /Int.St/part 4/4: "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", 1999.
6. R. Clarke: Dataveillance: Delivering "1984", Xamax Consultancy Pty Ltd, February 1993.
7. R. Clarke: Introduction to Dataveillance and Information Privacy and Definitions of Terms, Xamax Consultancy Pty Ltd, October 1998.
8. R. Clarke: A Future Trace on Dataveillance: Trends in the Anti-Utopia/ Science Fiction Genre, Xamax Consultancy Pty Ltd, March 1993.
9. T. Dixon: Workplace video surveillance - controls sought, Privacy law and Policy Reporter, 2 PLPR 141, 1995.
10. T. Dixon: Privacy charter sets new benchmark in privacy protection, Privacy law and Policy Reporter, 2 PLPR 41, 1995.
11. D. Banisar and S. Davies: The code war, Index online, News Analysis, issue 1998.
12. T. Lesce: They’re Watching You! The Age of Surveillance, Breakout Productions, 1998.
13. W.G. Staples: The Culture of Surveillance, St. Martin’s Press, 1997.
14. D. Lyon and E. Zureik: Computers, Surveillance and privacy, University of Minnesota Press, 1996.
15. D. Lyon: The Electronic Eye – The rise of Surveillance Society, University of Minnesota Press, 1994.
16. F.H. Cate: privacy in the Information Age, Brookings Institution Press, 1997
17. P. Brookes: Electronic Surveillance Devices, Newnes, 1998
18. O.E.C.D.: Privacy Protection in a Global Networked Society, DSTI/ICCP/REG(98)5/FINAL, July 1998.
19. O.E.C.D.: Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet, DSTI/ICCP/REG(97)6/FINAL, September 1998.
20. O.E.C.D.: Cryptography policy: The Guidelines and the issues, OCDE/GD(97)204, 1997.
21. Report By an Ad Hoc Group of Cryptographers and Computer Scientists: The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, 1998.
22. COM(98) 586 final: Legal framework for the Development of electronic Commerce.
23. COM(98) 297 final: Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, OJ C325, 23/10/98.
24. A. Troye-Walker, European Commission: Electronic Commerce: EU policies and SMEs, August 1998.
25. COM(97) 503 final: Ensuring security and trust in electronic communications – Towards a European Framework for Digital Signatures and Encryption.
26. Directive 97/7/EC of the European Parliament and the Council of May 1997 on the protection of Consumers in respect of Distance Contracts, OJ L 144, 14/6/1997.
27. ISPO: Electronic Commerce – Legal Aspects. http://www.ispo.cec.be.
28. Privacy International: http://www.privacy.org.



xiii

29. Newton and Mike: Picturing the future of CCTV, Security Management, November 1994.
30. Gips and A. Michael: Tie Spy, Security Management, November 1996.
31. Clarke and Barry: Get Carded With Confidence, Security Management, November 1994.
32. Horowitz and Richard: The Low Down on Dirty Money, Security Management, October 1997.
33. Cellular E-911 Technology Gets Passing Grade in NJ Tests, Law Enforcement News, July - August 1997.
34. Shannon and Elaine: Reach Out and Waste Someone, Time Digital, July August 1997.
35. Thompson, Army, Harowitz, and Sherry: Taking a Reading on E-mail Policy, Security Management, November 1996.
36. Trickey and L. Fried: E-mail Policy by the Letter, Security Management, April 1996.
37. Net Proceeds, Law Enforcement News, January 1997.
38. Burrell, and Cassandra: Lawmen Seek Key to Computer Criminals, Associated Press, July 10, 1997, Albuquerque Journal.
39. Gips and A. Michael: Security Anchors CNN, Security Management, September 1996.
40. Bowman and J. Eric: Security Tools up for the Future, Security Management, January 1996.
41. E. Alderman and C. Kennedy: The right to Privacy, Knopf 1995.
42. Bennet and J. Colin: Regulating Privacy- Data protection and public Policy in Europe and the United States, Cornell University Press, 1992.
43. BeVier and R. Lillian: Information about Individuals in the Hands of Government – Some reflections on Mechanisms for Privacy Protection, William and Mary Bill of Rights Journal 4, Winter 1995.
44. Branscomb and A. Well: Who owns Information? From Privacy to Public Access, Basic Books 1994.
45. Branscomp: Global Governance of Global Networks, Indiana Journal of Global Legal studies, Spring 1994.
46. Network Wizards, Internet Domain Survey, January 1997, http://www.nw.com/zone/WWW/report.html.
47. Network Wizards, Internet Domain Survey, January 1997, http://nw.com/zone/WWW/lisy-bynum.html.
48. Simon Davis: report, December 1997, http://www.telegrapf.co.uk.
49. Francis S. Chlapowski: The Constitutional Protection of Information Privacy: Boston University Law Review, January 1991.
50. J. Guisnel: Guerres dans le cyberspace, Editions la decouverte, 1995.
51. http://www.dis.org.
52. http://www.telegraph.co.uk

.


xiv