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** **Directorate General for Research** **Directorate A** **The STOA Programme**
Author:	**Mr Nikos Bogolikos - Zeus E.E.I.G**
Editor:	**Mr Dick HOLDSWORTH,** **Head of STOA Unit**
Date:	**October 1999**
PE number:	**PE 168. 184 Vol 5/5**

TABLE OF CONTENTS

PART A: OPTIONS **3**

INTRODUCTION 3
KEY FINDINGS 4
OPTIONS: 5

PART B: ARGUMENTS AND EVIDENCE **7**

PART C: TECHNICAL FILE . . . . . **I**

1. DEFINITIONS . . . . . **I**

2. SURVEILLANCE: TOOLS AND TECHNIQUES - THE STATE OF THE ART . . . . . **I**

1. PHYSICAL SURVEILLANCE I
2. COMMUNICATIONS SURVEILLANCE I

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

1. CALEA SYSTEM II
2. ECHELON CONNECTION II
3. INHABITANT IDENTIFICATION SCHEMES III

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

EXAMPLES OF ABUSE OF ECONOMIC INFORMATION IV

5. PROTECTION FROM ELECTRONIC SURVEILLANCE . . . . . **VII**

6. SURVEILLANCE TECHNOLOGY SYSTEMS IN LEGAL AND REGULATORY CONTEXT . . . . . **VII**

LAW ENFORCEMENT DATA INTERCEPTION - POLICY DEVELOPMENT IX

7. REFERENCES . . . . . **XIII**

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.

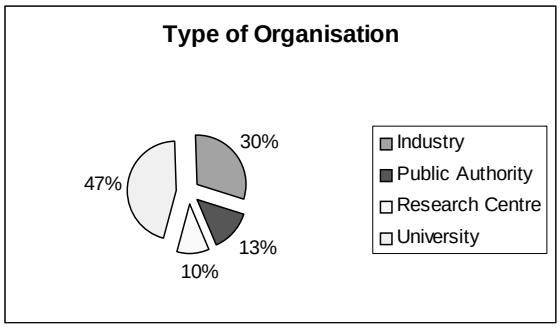
✓ Continuing the analysis of the results, it was found that the opinions on whether "*the information industry should be primarily self-regulated*", share the same percentage, i.e. approximately 42% positive, 41% negative, while the rest 17% couldn't give a certain answer.

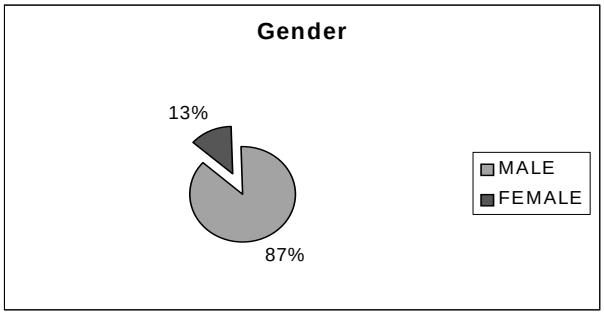
✓ Concerning the point that "*major governments are routinely utilising communications intelligence to provide commercial advantages to companies and trade*", in one third of the cases we had no concrete reply, 40% were sure that this is done, whereas 27% were sure that this is not the case.

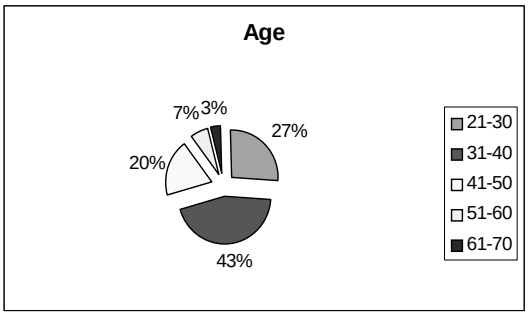
✓ Finally, with regard to the point that "*recent diplomatic initiatives by the USA government seeking European agreement to the "key-escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the 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.

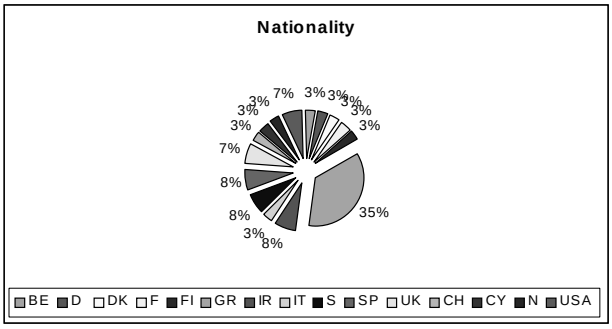
As a result, we could say that experts do agree on all these points and they see that actions have to be taken in order to balance the explosion of the information flow and the need for secure communications. No additional points were proposed.

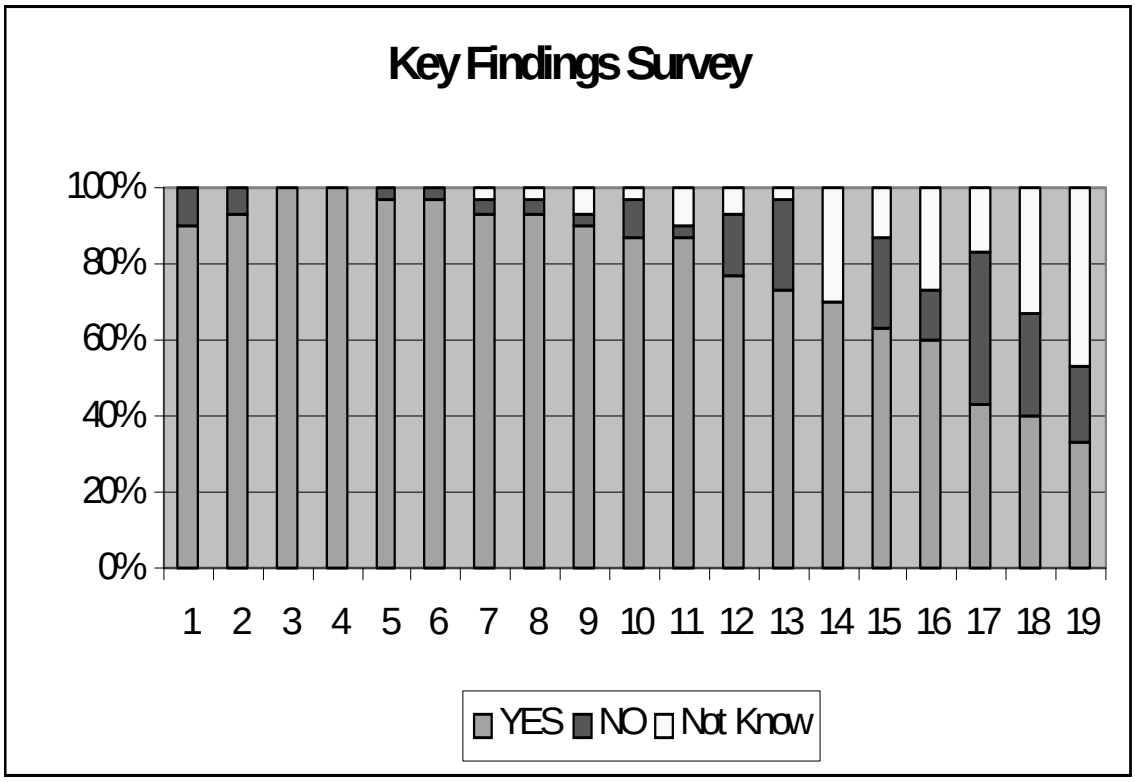
The graphical representation of the experts' data and their responses, are given in the following figures.


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