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 Directorate General for Research Directorate A The STOA Programme
Author:	Prof. Chris Elliot
Editor:	Mr Dick HOLDSWORTH, 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