CYBER-RIGHTS & CYBER-LIBERTIES
A NON PROFIT CIVIL LIBERTIES ORGANISATION

Statement for the European Parliament, Temporary Committee on the ECHELON interception system, meeting of Thursday, 22 March, 2001, Brussels.

Session on exchange of views on "Legal Affairs, Human Rights and Privacy"

By Yaman Akdeniz, Director of Cyber-Rights & Cyber-Liberties (UK)[1]

Cyber-Rights & Cyber-Liberties (UK) (http://www.cyber-rights.org) is a non profit organisation established to protect the interests of all honest, law abiding Internet users with the aim of promoting free speech and privacy on the Internet. It was founded in 1997 and has been actively involved with the Internet policy making process of the UK Government, the European Union, Council of Europe, OECD, and the United Nations.

Following the introduction of the Regulation of Investigatory Powers Act 2000,[2] security and privacy of communications has become a real concern for Internet users in the UK. Restrictive measures for intercepting all forms of communications are also proposed by the Council of Europe, and unaccountable interception of communications is already taking place through the Echelon interception systems. Therefore concerns for private communications extend to an international stage. For raising public awareness of these important policy issues and to encourage Internet users to use secure and encrypted communications, Cyber-Rights & Cyber-Liberties (UK) decided to launch the Cyber-Rights.Net (http://www.cyber-rights.net) project based upon the Hushmail technology.

Respect for Human Rights

Privacy and freedom of expression are fundamental human rights recognised in all major international and regional agreements and treaties:

- Universal Declaration of Human Rights, article 12, article 19;
- The International Covenant on Civil and Political Rights, article 19
- European Convention on Human Rights, article 8 and article 10;

These important international instruments should be taken into account by governments and regional and international organisations in the development of their policies. Any co-ordinated policy initiative at a supranational level (e.g. in the European Union or within the Council of Europe in relation to the adoption of the draft Convention on

---

1 Lecturer, CyberLaw Research Unit, Faculty of Law, University of Leeds, Leeds LS2 9JT, United Kingdom. Note also Akdeniz, Y, Walker, C., Wall, D., (eds), *Internet, Law, and Society*, Addison Wesley Longman, December 2000. A full list of publications is available through <http://www.cyber-rights.org/yamancv.htm>. Tel: +44 (0)7798 865116, Fax: +44 709-2199011. E-mail: lawya@cyber-rights.org. Url: http://www.cyber-rights.org and http://www.cyber-rights.net

2 See generally Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, (2001) *Criminal Law Review*, (February), pp. 73-90 at <http://www.cyber-rights.org/documents/crimlr.pdf>.

Cyber-crime), or at an international level (e.g. within the OECD, or within G8) should also offer the best protection for individual rights and liberties.

Echelon interception systems and the UK government

As a civil liberties organisation based in the UK, we are particularly concerned with the alleged involvement of the UK Government, a member of both the European Union and the Council of Europe, with the Echelon interception systems. So far, the UK government's preferred practice in relation to the existence and use of Echelon systems has been not to comment on such allegations.[3]

European Union and the respect for human rights

If the current allegations are true, all law abiding European citizens and companies are at risk of being monitored every day without any legal basis. Therefore, Cyber-Rights & Cyber-Liberties (UK) would like to remind the European Parliament Temporary Committee on Echelon interception systems that the European Union is founded on respect for human rights, and that this is a requirement for membership of the European Union. This includes respect for privacy of communications and personal data. With the Treaty on European Union (as amended by the Amsterdam Treaty), the EU member states have confirmed their attachment to the principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law. Article 6 (ex Article F) of the Treaty states that:

> 1. The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.
>
> 2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.

It is possible for the Council of the European Union to decide to suspend certain of the rights deriving from the application of this Treaty to a Member State[4] following the "existence of a serious and persistent breach by a Member State of principles mentioned in Article 6(1), (after inviting the government of the Member State in question to submit its observations)".[5] If the current allegations are true in respect to Echelon interception systems, there may be a serious breach of article 6(1) by the UK government which need to be scrutinized by the Council of the European Union.

Need for accountability in the Global Interception of Communications

---

3 See for example, House of Commons Hansard Written Answers for 1 Nov 1999 (pt 9) - Foreign and Commonwealth Affairs (Echelon System); House of Commons Hansard Written Answers for 14 Jun 1999 (pt 5) - Prime Minister (Echelon System); House of Commons Hansard Written Answers for 7 May 1998 (pt 15) (Echelon System); House of Commons Hansard Written Answers for 20 Jun 2000 (pt 14) Echelon Surveillance System; House of Commons Hansard Written Answers for 12 Mar 2001 (pt 6) Echelon Surveillance System; House of Commons Hansard Written Answers for 4 May 2000 (pt 5) Echelon Surveillance System.

4 Article 7(2) (ex Article F.1) of the Treaty.

5 Article 7(1) (ex Article F.1) of the Treaty.

Secret surveillance, and interception of all forms of communications including Internet communications, cannot be acceptable in democratic societies. By welcoming the decision of the European Parliament to set up a temporary committee to verify the existence of the communications interception system known as Echelon to assess the compatibility of such a system with Community law,[6] we call for accountability in the global interception of communications.

We note that privacy is not an absolute right, and do not oppose lawful interception of communications based on clear legal powers and subject to effective judicial control and adequate remedies for abuse. However, we are particularly concerned about the lack of democratic oversight on data being intercepted, stored and processed with systems like Echelon.

European Convention on Human Rights and privacy of communications

The monitoring of communications can constitute an interference with the right to respect for private life and correspondence in breach of Art. 8(2), unless it is carried out in accordance with a legal provision capable of protecting against arbitrary interference by the state with the rights guaranteed.[7] However, the exceptions provided for in Article 8(2) are to be interpreted narrowly,[8] and the need for them in a given case must be convincingly established. Furthermore, the relevant provisions of domestic law must be both accessible and their consequences foreseeable, in that the conditions and circumstances in which the state is empowered to take secret measures such as telephone monitoring should be clearly indicated[9] as "where a power of the executive is exercised in secret the risks of arbitrariness are evident."[10] In particular, the avoidance of abuse demands certain minimum safeguards, including the conditions regarding the definition of categories of persons liable to have their telephones tapped, and the nature of offences that could give rise to such an order. The European Court of Human Rights in the *Amann v. Switzerland* judgment,[11] stated that

> "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."

It is essential to have clear, detailed rules on the subject, especially as the technology available for use is constantly becoming more sophisticated."[12]

---

6 (in particular Article 286 of the EC Treaty and Directives 95/46/EC and 97/66/EC, and with Article 6(2) of the EU Treaty)

7 Malone v United Kingdom (A/82) (1985) 7 E.H.R.R. 14; *Valenzuela Contreras v Spain*, Application No. 27671/95, (1999) 28 EHRR 483.

8 See *Klass and Others v. Germany* (A/28): (1978) 2 E.H.R.R. 214, para. 42.

9 *Kruslin v France* (A/176-B) (1990) 12 E.H.R.R. 547; *Huvig v France*, A/176-B, (1990) 12 EHHR 528; *Halford v. United Kingdom*, (Application No. 20605/92), Judgment of June 25, 1997, 24 E.H.R.R. 523; *Valenzuela Contreras v Spain*, Application No. 27671/95, (1999) 28 EHRR 483.

10 *Valenzuela Contreras v Spain*, Application No. 27671/95, (1999) 28 EHRR 483.

11 *Amann v. Switzerland*, App. No. 27798/95, Judgment of 16 February 2000.

12 *Huvig v France*, A/176-B, (1990) 12 EHHR 528; *Kruslin v France*, A/176-A, (1990) 12 EHRR 547; *Kopp v Switzerland*, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91.

Council of Europe's draft Cyber-Crime Convention

It is very important to note regulatory initiatives elsewhere and one which is closely related to the work of the Temporary Committee on Echelon interception systems is the draft Cyber-Crime Convention by the Council of Europe.[13] The draft Convention includes provisions related to interception of communications, preservation and disclosure of traffic data, production orders, search and seizure of stored computer data, real-time collection of traffic data, interception of content data, and mutual assistance between the law enforcement agencies of the Convention signing states regarding these measures. However, the provisions of Council of Europe's draft Cyber-Crime Convention[14] seem incompatible with article 8(2) of the European Convention on Human Rights and the related judgments of the European Court of Human Rights as explained above.[15]

In the words of Judge Pettiti, of the European Court of Human Rights, "the mission of the Council of Europe and of its organs is to prevent the establishment of systems and methods that would allow 'Big Brother' to become master of the citizen's private life."[16]

We note a serious lack of commitment to data protection principles within the draft Cyber-Crime Convention despite the existence of the 1981 CoE Convention and the CoE 1999 Recommendation R(99)5. The conditions and safeguards throughout the Convention should refer to data protection laws and privacy guidelines. For example, such safeguards are included within the European Union's Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[17] Furthermore, Council of Europe Recommendation N° R(87) 15 regulating the use of personal data in the police sector (17 September 1987),[18] Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector, and second evaluation report of the Recommendation adopted in 28 October 1999 should also be taken into account,[19] and this should be extended to security services in addition to law enforcement bodies.

---

13 Council of Europe Draft Cyber-Crime Convention, version no 25, at <http://conventions.coe.int/treaty/EN/projets/cybercrime25.doc>. See also the draft Explanatory Memorandum through <http://conventions.coe.int/treaty/EN/projets/CyberRapex7.doc>, February 2001.

14 *Ibid*.

15 Malone v United Kingdom (A/82) (1985) 7 E.H.R.R. 14; *Valenzuela Contreras v Spain*, Application No. 27671/95, (1999) 28 EHRR 483; *Camenzind v Switzerland* (Application No. 21353/93), (1999) 28 EHHR 456 and *Funke v. France*, A/256-A, (1993) 16 EHRR 297; *Kopp v Switzerland*, (Application No. 23224/94), Judgment of 25 March, 1998, (1999) 27 EHHR 91; *Amann v. Switzerland*, App. No. 27798/95, Judgment of 16 February 2000.

16 Per Judge Pettiti, concurring opinion in *Malone v United Kingdom* (A/82) (1985) 7 E.H.R.R. 14.

17 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union, 2000/C 197/01. See specifically article 23 of the Convention.

18 The recommendation has been referred to in two international agreements. Article 115, first paragraph, of the Schengen Agreement states that control by the supervisory authority should take account of the recommendation. The Treaty of Amsterdam incorporated the Schengen Agreement into the EU Treaty. Likewise, in its article 14, paragraph 1, the Europol Treaty provides that processing of police data should take account of the 1987 recommendation of the Council of Europe. The recommendation is at <http://www.coe.fr/dataprotection/rec/r(87)15e.htm>.

19 The full report is available at <http://www.coe.fr/dataprotection/Etudes_Rapports/evaluation_E98_R(87)15.htm>.

We also recognise that adequate police powers are necessary to allow the police to fulfil their tasks. However, as the CJ-PD report states, "these powers, to be adequate, necessarily interfere with the respect for private life and should therefore be restricted to the extent that is necessary."

A Proportionate and Effective Response?

Moreover, we also recognise that in countering such use it may sometimes be necessary to infringe the rights of honest citizens in order to secure the prosecution and conviction of guilty parties. But in considering such action, we believe that it is necessary to apply the following tests to any proposals that are made:

1) That they provide clear net benefit for society. That is, the benefits are clear and are achievable by the measures proposed, with a detrimental impact on the rights of honest citizens that is as small as possible and one that is widely accepted as tolerable in the light of the gains secured.
2) That the measures proposed discriminate effectively between criminals and honest, law abiding citizens. Therefore, they should be balanced and should not, in an impetuous desire to counter crime, expose all honest citizens to such risks as government access to encryption keys.
3) That of all the options available they are the best in the sense that they are the most effective in countering criminals while having the least impact on honest citizens and the lowest costs for taxpayers and businesses.
4) They should be based on clearly defined policy objectives which citizens understand and which command widespread public support.
5) They should be enforceable, transparent, and accountable.

Government Access to Encryption Keys

It is our considered opinion that the powers for key seizure and Internet interception in the UK Regulation of Investigatory Powers Act 2000 fail every one of the above mentioned tests.

Firstly, the UK Government has not shown these powers to be either necessary or effective in countering criminal misuse of the Internet. Most experts agree that they will not be effective against serious criminals. Moreover, other countries such as Germany (a partner of the UK within the European Union) have considered and rejected such measures as (a) unnecessary, (b) ineffective, and (c) detrimental to the safety, security and privacy of honest citizens and businesses who make use of the Internet.

Secondly, these measures are indiscriminate and make no distinction between the keys and information owned by criminals and those owned by honest citizens. They are technically ineffective and easy to circumvent from a criminal perspective and yet create potential risks for honest citizens and businesses that are more than sufficient to undermine confidence in Internet use in the UK.

Apart from the UK Government introducing such legal powers for accessing encryption keys or plaintext "only Malaysia and Singapore (and India) have existing laws

mandating such lawful access."[20] We are concerned that UK policy is likely to establish an international standard on access to encrypted data and that copycat legislation may start to appear elsewhere. But it should be remembered that the "government access to encryption keys" issue is also related to human rights concerns and issues for example under the ECHR (article 6) such as a suspect's right to fair trial, right not to self-incriminate himself/herself, and right to silence.[21]

Conclusion

Privacy, Data protection, and Security on the Internet should be encouraged

We call on the member countries of the European Union to encourage privacy of communications, data protection, and security on the Internet.

In developing encryption policies, governments and international organisations should avoid the inclusion of provisions for government access to encryption keys ("GAK"), as such provisions could seriously undermine the security of computers and computer data, e-commerce and the integrity of service providers, as well as causing huge potential costs in global key revocation and change. It could also infringe important human rights.

Governments and supranational and international organisations should co-operate to respect fundamental human rights such as freedom of expression and privacy and should encourage rather than limit the peoples' usage of the Internet through excessive regulation.

---

[20] Note also that at the Denver Summit in June 1997, the G-8 supported such access. It recommended that every country adopt "lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies." See Electronic Privacy Information Center, Cryptography and Liberty 2000: An International Survey of Encryption Policy, (EPIC, Washington, 2000).

[21] *Funke v. France*, 25 February 1993, Series A no. 256-A, p. 22, § 44; *John Murray v. the United Kingdom*, 8 February 1996, Reports of Judgments and Decisions 1996-I, p. 49, § 45; and *Saunders v. the United Kingdom*, 17 December 1996, Reports 1996-VI, p. 2064, § 68; *Serves v. France*, 20 October, 1997, Reports 1997-VI.