Cyber-Rights & Cyber-Liberties (UK)

Fifth Year Statement

1997-2002

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 January 1997 and has been actively involved with the Internet policy-making processes of the UK Government, the European Union, Council of Europe, OECD, and the United Nations. It has also been an active member of the Global Internet Liberty Campaign (http://www.gilc.org) since March 1997, and was involved with the formation of the UK Internet Users Privacy Forum ("IUPF") in March 1999. The organisation also launched the Cyber-Rights.Net project (http://www.cyber-rights.net) in association with HushMail in November 2000.

This statement has been written to mark the fifth birthday of Cyber-Rights & Cyber-Liberties and to highlight the importance of cyber-rights in the Information Age.

The Internet as an empowering tool

The Internet is a social, cultural, commercial, educational and entertainment global communications system whose legitimate purpose is to benefit and empower online users, lowering the barriers to the creation and the distribution of expressions throughout the world. Governments, the Internet industry, the NGOs, and the online users have each an important role to play in building and keeping open, consistent with this purpose, global communications networks.

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, articles 12, and 19;
- The International Covenant on Civil and Political Rights, articles 17, and 19;
- European Convention on Human Rights, articles 8, and 10;
- European Union Charter of Fundamental Rights, articles 7, 8, and 11

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 at an international level (e.g. with the CoE Cyber-Crime Convention) should also offer the best protection for individual rights and liberties.

We believe that the principles within these important international instruments should not be forgotten or put aside even in the aftermath of horrific crimes such as the attacks on America on September 11, 2001. Respect for human rights includes respect for freedom of expression, and respect for privacy of communications and personal data. 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 within systems like Echelon.

We dispute that the UK's Regulation of Investigatory Powers Act 2000 is compatible with articles 6 and 8 of the European Convention on Human Rights. Statements which describe the RIP Act as the "greatest safeguard that exists in any democracy in the world…. for protecting our rights" (*Per David Blunkett, the Home Secretary, House of Commons Hansard Debates for 15 October, 2001, at column 935*) are in our view simply untrue. Even a comparison within Western Europe shows that the United Kingdom has the most intrusive legislation.

The Government should also be criticised for promoting new legislation such as the Anti-Terrorism, Crime, and Security Act 2001 and extending its powers before the inadequacy of its existing powers has been established.

Openness and Transparency in the Policy Making Process

Transparency, openness and accountability are important features of a healthy society. Within the five years of our work, we have not witnessed openness, transparency, and accountability in the work of the following forums, task forces, and organizations at the UK level while formulating or discussing Internet related policies:

- Home Office Task Force on Child Protection and the Internet
- Home Office Encryption Co-ordination Unit
- Internet Crime Forum
- Association of Chief Police Officers ("ACPO"), the ISPs and the Government Forum
- Internet Watch Foundation

Furthermore, there was no openness, nor transparency involved with the drafting of the Council of Europe Cyber-Crime Convention, and in relation to G8 initiatives to fight cyber-crimes. In most cases, "co-operation" meant co-operation between government bodies, law enforcement bodies, and the industry.

National and international forums that discuss Internet related policy issues do not include the representatives of NGOs and public interests groups. It is important to consult all interested parties, and such organisations should be included within the policy making process.

We therefore call for openness, and transparency in relation to Internet policy making processes by the UK government, supranational, regional, and international organisations.

European Convention on Human Rights and privacy of communications

The monitoring of communications including interception of content data under the Regulation of Investigatory Powers Act 2000, and the retention of communications data under the Anti-Terrorism, Crime, and Security Act 2001 can constitute an interference with the right to respect for private life and correspondence in breach of Art. 8(2) of the European Convention on Human Rights, unless these surveillance activities are carried out in accordance with a legal provision capable of protecting against arbitrary interference by the state with the rights guaranteed. However, the exceptions provided for in Article 8(2) are to be interpreted narrowly, and the need for them in a given case must be convincingly established.

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. However, in September 2001, the European Parliament in a resolution concluded that "the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the US, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt."

The European Parliament also urged the Member States to review and if necessary to adapt their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights as laid down in the ECHR and with the case law of the European Court of Human Rights.

Secret surveillance and interception of all forms of communications including Internet communications cannot be acceptable in democratic societies. By welcoming the resolution of the European Parliament on the existence of Echelon, we call for accountability in the global interception of communications.

Council of Europe's Cyber-Crime Convention

The Council of Europe Cyber-Crime Convention, recently opened to signature, includes provisions related to interception of communications, preservation and disclosure of traffic data, production orders, search and seizure of stored computer data, and mutual assistance between the law enforcement agencies of the Convention signing states regarding these measures.

However, the provisions of the Cyber-Crime Convention seem incompatible with article 8(2) of the European Convention on Human Rights and the related judgments of the European Court of Human Rights. Although the Cyber-Crime Convention states in the preamble that a proper balance needs to be ensured between the interests of law enforcement agencies and respect for fundamental human rights, the balance is certainly in favour of the law enforcement agencies.

We note a serious lack of commitment to data protection principles within the Cyber-Crime Convention despite the existence of the 1981 CoE Data Protection Convention and the CoE 1999 Recommendation R(99)5. The conditions and safeguards throughout the Convention should have referred to data protection principles and privacy guidelines.

Resist censorship of the Internet

New media historically face suspicion and are liable to excessive regulation as they spark fears as to the potential detrimental effects they may have on society. Now, the Internet is receiving the same kind of treatment with various attempts to censor and control its content. However, as the European Court of Human Rights stated "... freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress," and censorship should be resisted at all costs.

We note that freedom of expression via the Internet can be further threatened if the law imposes heavy responsibilities on ISPs for the third party content they carry. ISPs should not be forced into being the defendant, judge, and the jury at the same time. In Europe, in the long term, laws including notice & takedown provisions could turn ISPs into proxy censors as a risk avoidance measure while deflecting the blame from governments

Government Access to Encryption Keys

Apart from the UK Government introducing legal powers for accessing encryption keys or plaintext under the Regulation of Investigatory Powers Act 2000 only a few countries have existing laws mandating such lawful access. 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.

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.

Conclusion

We call on the governments, the European Union, the Council of Europe, the United Nations, the OECD, and the G8 to encourage freedom of expression, privacy of communications, data protection, and security on the Internet.

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 at the national level. Responses to problems that are associated to the Internet need to be proportionate and effective. Otherwise, far from free and unregulated, the Internet may end up as the most regulated medium in history.

Written By Yaman Akdeniz, Director, Cyber-Rights & Cyber-Liberties (UK)

Board Members of Cyber-Rights & Cyber-Liberties (UK): Mr Yaman Akdeniz, director (lawya@cyber-rights.org), Dr Brian Gladman, Technology Policy Adviser (brg@cyber-rights.org), Mr Nicholas Bohm, E-Commerce Policy Adviser (nbohm@cyber-rights.org), Professor Clive Walker, Deputy Director (lawcpw@cyber-rights.org), Dr Louise Ellison, Deputy Director (lawlee@cyber-rights.org).

Fifth Year Logo has been designed by Michael Tsekouras (mt@cyber-rights.net) who has also developed the Cyber-Rights.Net project's website.

Cyber-Rights.Net Project: Following the introduction of the Regulation of Investigatory Powers Act 2000, 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 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 project based upon the Hushmail technology in November 2000. The project is fully supported by Hush Communications. Any Internet user can get a free account through the http://www.cyber-rights.net website.