INTERMEDIATE EVALUATION

OF THE

SAFER INTERNET ACTION PLAN

CONDUCTED FOR

THE EUROPEAN COMMISSION

VOLUME TWO

CONTEXT AND APPENDICES

31 MAY 2001

BUSINESS DEVELOPMENT RESEARCH CONSULTANTS
KINGSBOURNE HOUSE, 229 – 231 HIGH HOLBORN
LONDON WC1V 7DA
TEL: +44 207 400 1000. FAX +44 207 405 4778
www.bdrc.co.uk

Contents

INTRODUCTION

Structure of this Report

This report is arranged in two volumes.

Volume One is structured into the following main sections:

- **Section A** provides broad background information, including the evaluation's terms of reference.
- **Section B** covers the findings from the primary research amongst project participants and stakeholders.
- **Section C** brings together the conclusions and recommendations.

Volume Two comprises:

- **Section D**, which provides an overview of the legal and regulatory context of the Safer Internet Action Plan and reviews related technical and market developments.
- **Appendices**

SECTION D LEGAL, REGULATORY AND TECHNICAL CONTEXT

1. LEGAL AND REGULATORY CONTEXT AND DEVELOPMENTS

1.1 Overview of Trends

In the years since the IAP was first formulated there have been a number of developments and initiatives in the legal and regulatory framework directed at protecting against illegal and harmful content. In addition there have also been developments and initiatives against the broad category of international cyber crime.

The technologies of delivery, their levels and degrees of acceptance change quickly, and law reform in this area is much faster than the generality of law reform.

The purpose of this section of the Evaluation Report is to flag for attention the more important of these developments, place them in context, and provide an indicative forecast of what further developments might be expected over the next three to four years.

Voluntary and self-regulatory activity – the core of the IAP – has to operate in the context of knowledge of what law enforcement measures exist, and how effective they are.

Worries about harmful content have gone hand-in-hand with broader concerns about law enforcement in cyberspace. The main aim of legislators and law enforcement has been to achieve a high degree of recognition of substantive laws and procedures. In all jurisdictions agreement to provide assistance to another country requires that there is a rough equivalence of offences and of procedures – doubt about either can lead to considerable delays and refusal. But law enforcement agencies have also sought extensions to their powers of data interception and evidence acquisition. However in so doing they continue to run into conflict with:

- human rights legislation
- data protection legislation
- the aspiration of governments and the Community to keep as low as possible the costs of Internet connection and thereby promote the growth of the knowledge economy

In the last two years law enforcement has recognised that, if it is to carry out successful investigations and to acquire the evidence needed to secure convictions it needs to develop a close working relationship with the ISP (Internet Service Provider) and telecommunications industries. There have been a number of high-level meetings and workshops and the setting of nation-based consultative forums; the setting up of a Europe-wide forum was announced earlier this year. But there are still questions about the status and membership of these forums and there remain significant tensions between law enforcement and industry, which reflect their ultimate positions: law enforcement to catch criminals and businesses to generate profit.

1.2 Earlier history of European legal initiatives against illegal and harmful content

The first general initiatives against illegal content were undertaken by the Council of the European Union. In July 1996, based on article K.3 of the Maastricht Treaty on European Union, the Council adopted a joint action to combat "racism and xenophobia"[1] rather than pornographic or paedophilic material. The specific issue of illegal and harmful content on the Internet had been discussed at an informal Council meeting in April. Further meetings took place that year and in February 1997, the Telecommunications Council adopted a resolution on illegal and harmful content on the Internet[2]. The Commission also published several documents: in October 1996, a communication on illegal and harmful content on the Internet[3] and a green paper on the protection of minors and human dignity in information and audiovisual services[4] (outlined in section 3.1 above); and in late 1997, the proposal for the Safer Internet Action Plan. The Council followed up the green paper with a recommendation on the protection of minors and human dignity[5]. The European Parliament, for its part, adopted a resolution in April 1997[6] on the Commission's 1996 communication, supporting the initiatives undertaken by the Commission and stressing the need for international cooperation, to be initiated by the Commission, in several areas. The Parliament also published a study *Feasibility of censoring and jamming pornography and racism in informatics*[7] that concentrated on the technical possibilities of blocking illegal and harmful content.

1.3 The move to harmonisation of laws relating to computer crime

In the longer run, effective international law enforcement on the Internet requires that nation states take steps to harmonise both their substantive laws and their procedures for requesting warrants for search, seizure, interception and evidence preservation. Proposals for such harmonisation go back almost 20 years. From 1983 to 1985 an ad hoc committee of the OECD discussed the possibilities of an international harmonisation of criminal laws fighting computer-related economic crime. In 1986 the *Select Committee of Experts for Computer-*

[1] OJ L 185/5 of 24.07.1996.

[2] Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council on illegal and harmful content on the Internet, OJ C 70/1 of 06.03.1997.

[3] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the Internet of 16 October 1996, COM(96) 0487. See also in this context European Commission (DG XIII), Interim report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet, WPIC 16/97, Version 7 of 4 June 1997.

[4] COM(96) 0483.

[5] Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity OJ L 270 07.10.1998, p.48. http://europa.eu.int/comm/avpolicy/regul/new_srv/recom-intro_en.htm

[6] COM(96) 0487 – C4-0592/96, http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.ht> (accessed on 24 January 1998).

[7] See European Parliament, STOA, Feasibility of censoring and jamming pornography and racism in informatics, Draft Final Report, May 1997.

Related Crime of the Council of Europe produced a series of proposals which arose of out of pre-occupations with producing a Europe-wide data protection regime. From 1985 to 1989 the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the legal problems of computer crime. The legal questions of computer crime were also discussed by the Legal Advisory Board (LAB) of the Commission. In December 1987, a first report on "The Legal Aspects of Computer Crime and Security" was delivered to the LAB, which discussed it in May 1988. In March 1990 the relevant questions were taken up in a joint conference of the European Commission and of the Council of Europe in Luxembourg. In both meetings, there was a clear support for future international actions of the Council of Europe and the European Community in this field. In 1994, the UN published the "UN Manual on the Prevention and Control of Computer-Related Crime"; a further version was prepared for publication in 1997. Another body active in the area was the Association International de Droit Pénal (AIDP).

Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology recommends the governments of the Member States, when reviewing their internal legislation and practice, to be guided by the principles appended to the recommendation and to ensure publicity for these principles. The principles cover search and seizure, technical surveillance, obligations to cooperate with investigating authorities, electronic evidence, use of encryption, research and statistics, training, and international cooperation.

Early in 1997 the European Committee on Crime Problems (CDPC) set up a new "Committee of Experts on Crime in Cyberspace" (PC-CY). Its terms of reference are to examine problems of criminal law connected with information technology, in particular

- cyberspace offences and other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation;
- the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment;
- the question of jurisdiction in relation to information technology offences;
- questions of international co-operation in the investigation of cyberspace offences.

Within the European Union, activities in the field of procedural law have not been undertaken under the so-called first pillar, but under the third pillar, i.e. intergovernmental co-operation in matters of home affairs institutionalised by the K-Articles of the Treaty on European Union (the Maastricht Treaty). In January 1995, based on articles K.1 (9) and K.2 (2), the European Council adopted a resolution on the international requirements for a lawful interception of telecommunications[8]. Associated with this are a number of working groups [9]. Issues of police and judicial cooperation appear in Title VI in the consolidated version of the Treaty, with article 29 referring both to offences against children and preventing and combating racism and xenophobia. Article 30 refers to the promotion of Europol, and articles 31 to 43 specify forms of cooperation and in particular arrangements for extradition and the compatibility of rules.

[8] OJ C 329/1 of 04.11.1996.

[9] K4 on Police Co-operation, a Working Party on Mutual Legal Assistance and ILETS, an expert group "International Law Enforcement Telecommunications Seminar", which was formed as outgrowth of the expert group on legal question regarding telecommunications surveillance (originally within the framework of TREVI).

In the current Consolidated Version of the TEU, issues of police and judicial co-operation appear in Title VI.

1.4 Formal Moves towards Harmonisation

1.4.1 COUNCIL OF EUROPE

The main venue for the formal process of harmonisation has been the Council of Europe, which has been working on a Convention on Cybercrime since 1997.[10] This draft Convention can be signed by countries that are not members of the Council of Europe. The United States, Canada, Japan and South Africa are already actively participating in the drafting process. However it was only in April 2000 that the Council made available the drafts on its website and explanatory notes only became available in February 2001. The current draft is no 25. The final version is said to be ready by June 2001. The chapter dealing with measures to be taken at a national level covers substantive criminal law, and includes an article concerning offences relating to child pornography. It also deals with procedural law and includes coverage of the preservation of stored computer data, the preservation and partial disclosure of traffic data, production orders, the search and seizure of stored computer data, real-time data collection, and data interception. A further chapter deals with international cooperation, including extradition and mutual assistance, and includes an article requiring the establishment of a 24/7 network (that is, a series of contacts who are available round the clock every day of the year).

No nation is compelled to sign the Convention or sign it within a particular time frame. The Convention is said to have come into force three months after the first five signatories have formally committed themselves.

The initial drafting was carried out by nominated individuals from participating nations and they tended to be drawn from Justice and Home Affairs Ministries and law enforcement; there were no representatives from industry, consumer interests or privacy advocates. Early objections from computer security professionals about the apparent illegality of possessing tools that might be used to test computer security were largely overcome, but a number of major concerns remain:

- several commentators have said that the Draft Convention conflicts with other existing important international agreements[11].
- A number of influential industry groups have complained about the cost burdens.[12]

[10] http://conventions.coe.int/treaty/en/projets/cybercrime.htm

[11] These include the Council of Europe's European Convention on Human Rights, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Recommendation N° R (87) 15 regulating the use of personal data in the police sector, Recommendation N° R (95) 4 on the protection of personal data in the field of telecommunications services, in particular as regards telephone services, the EU Charter on Fundamental Rights, the EU Data Protection Directives and the 1966 United Nations International Covenant on Civil and Political Rights. The Working Party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 produced its *Opinion 4/2001on the Council of Europe's Draft Convention on Cyber-crime* on 22 March 2001, (http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp41en.htm). .A further indication of the difficulties the Convention may face at a European level can be found in a Working Document from Article 29, the Data Protection Working Party. Document 5063/EN/Final/WP37 adopted in November 2000 provides *An Integrated EU Approach to OnLine Data Protection* and this examines in some detail problems associated with the preservation of personal/traffic data (as in Article 6 of Directive 95/46/EC and Article 6 of Directive 97/66/EC).

[12] notably the US Chamber Of Commerce in December 2000 (http://www.computeruser.com/news/00/12/11/news17.html)

- Particular concerns include controls over warrants of interception, who will bear the costs of interception equipment and servicing and "data retention" – the desire of law enforcement that ISPs should be required to hold traffic data (and perhaps also content data) for a considerable number of years against the possibility that a law enforcement agency may wish to apply for a warrant in the course of an investigation.

Opinions vary as to the speed with which the Convention will be taken up. During informal opinion-gathering for this Report, some respondents said the process could take up to ten years and could fail almost completely. Most of the difficulties have arisen because of law enforcement lobbying to extend their powers and the promoters of the Convention thus face a paradox: easy agreements on definitions of crime and simple matters of mutual assistance could be lost because they are co-mingled with more contentious issues of extended powers for law enforcement.

Each of the 41 nations who are currently participating in the drafting will have to seek agreement from their own legislatures and overcome local objections before they can ratify.

1.4.2 ACTIONS TOWARDS HARMONISATION WITHIN THE EUROPEAN COMMUNITY

Within the Community the Maastricht Treaty provides the framework of the extent to which member nations can be compelled to harmonise legislation. As already noted, Title VI covers the provisions on police and judicial co-operation in criminal matters, including arrangements for extradition and compatibility of rules. They advance the notion of framework decisions, which are binding on Member states as to the result to be achieved but leave to national authorities the choice of form and methods. Measures implementing conventions are to be adopted within the Council by a majority of two-thirds of the contracting parties.

The Tampere Council in October 1999 agreed on a number of policy orientations and objectives in the field of judicial co-operation including a "Unionwide Fight Against Crime" (Part C). However the focus of the meeting was more on organised crime, money laundering and a common EU asylum and migration policy.

In May 2000 there was a Council Decision to combat child pornography on the Internet13 This included, among other things, requirements that Member States take the necessary measures to encourage Internet users to inform law enforcement authorities, either directly or indirectly, on suspected distribution of child pornography material on the Internet, the setting-up of specialised units within law enforcement authorities, the setting up of constantly available points of contact between national law enforcement agencies (including the use of Europol and Interpol), engagement with industry, the monitoring of changing technologies, and the promotion of filtering. The measures contained in this Decision were to be implemented by the Member States at the latest on 31 December 2000.

In January 2001 there was a Communication from the Commission which contained a proposal for a Council Framework Decision on combating the sexual exploitation of children and child pornography.[14] The aim was to improve the provisions of the Joint Action of February 1997. The proposal for a Framework Decision concerns approximation of the laws and regulations of the Member States in the area of police and judicial co-operation in criminal matters. It also concerns "minimum rules relating to the constituent elements of criminal acts and to penalties in the field of organised crime". The Articles include basic

[13] OJ L136, 09/06/2000

[14] COM(2000)854 final/2

definitions, requirements for offences with individual jurisdictions and associated penalties and sanctions, and requirements on prosecution and jurisdiction. Article 10 covers mutual legal assistance. The aim is for Member States to take the necessary measures to comply with the Framework Decision not later than 31 December 2002.

The Commission, by looking a minimal standards rather than ideal ones, thus has a more gradual approach towards harmonisation than the Council of Europe's Cyber Crime Convention and the first area of activity it has selected relates to child pornography.

1.5 Law Enforcement Co-operation with Industry

1.5.1 HISTORIC DEVELOPMENT

In the last two years law enforcement has realised that, if it is to carry out successful investigations and to acquire the evidence needed to secure convictions it needs to develop a close working relationship with the ISP and telecommunications industries. The main reasons are:

ISP and telecommunications companies are a critical source of evidence to:

- identify perpetrators from their records
- show who was active at any one time
- capture conversations, transmissions and transactions
- ISP and telecommunications companies are frequently the target for warrants and co-operation in execution is essential if matters are to proceed efficiently
- ISP and telecommunications companies can be a source of expertise for law enforcement agencies

The problem for ISP and telecommunications companies has been:

- law enforcement requirements may involve significant cost to them
- as businesses they have to observe the whole of the law, and that may include *inter alia* data protection and privacy legislation
- public perceptions of the relationship between the companies and law enforcement agencies

The main international model for such co-operation so far has been the UK's Internet Crime Forum (ICF)[15]. Its main tasks are:

- identify and review the legal requirements to be met to provide information
- identify information that can be provided from a technical perspective
- to research and identify the areas of legal uncertainty relating to the use of information from the Internet as evidence and to make recommendations to resolve any ambiguities
- develop an accepted practice for requesting and providing information
- put in place procedures for paying for resources used
- co-ordinate with and demonstrate leadership towards similar activities worldwide

The forum continues to evolve; membership is by invitation from law enforcement and currently does not include individuals from consumer and civil liberties/privacy interests. The

[15] http://www.internetcrimeforum.org.uk/

body is informal and consultative and does not aim to be "representative". It has been accused of being cosy and that industry members are selected on the basis that they will be particularly helpful to law enforcement. However law enforcement and government members say that such a body, if it is to be effective, cannot operate fully in the public domain, particularly in relation to precise investigatory methods and discussion of current cases, nor could such a body be anything other than purely consultative. Law enforcement rejects the accusation that it is too "cosy" a body.

1.5.2 G8 ACTIVITIES

G8 activities over cyber-crime have been concentrated in the so-called Lyon sub-group. In December 1997 there was a 10-point action plan from Justice & Home Affairs Ministers. This was endorsed at the Birmingham Summit in June 1998 and in June 2000 there was a high level meeting in Paris involving government, law enforcement and industry. This was followed by a more detailed workshop held in Berlin in October 2000; the next meeting in the series is in Japan in May 2001.

G8 activities have followed the same path as the UK discussions though with added difficulties:

- national differences and priorities become apparent; a number of G8 countries have yet to form their own analogues to the UK's ICF
- G8 has no permanent secretariat so that although a G8 meeting might reach decisions there is not necessarily any immediate means to enact them
- G8 procedures can sometimes be quite formal

However, G8 is perceived as important, and since many of the delegation members overlap with those who might be involved in other aspects of the harmonisation of international laws and procedures – in the Council of Europe or in the Commission – G8 is at the least an important lobbying venue.

1.5.3 COMMISSION ACTIVITIES

The Commission launched the *e*Europe initiative in December 1999 in order to ensure that Europe can reap the benefits of the digital technologies and that the emerging information society is socially inclusive. In June 2000, The Feira European Council adopted a comprehensive *e*Europe Action Plan and called for its implementation before the end of 2002. The Action Plan highlighted the importance of network security and the fight against cybercrime.

The Feira Council led to the publication of a Communication from the Commission: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[16]. This document, which was published at the end of January 2001, had been preceded by a small workshop in Sevilla. The first public event, which included an announcement that there was to be a Euroforum along the lines of the UK's ICF, took place in Brussels in March 2001.

The document is an important one and sets out the current problems of law enforcement in a much more comprehensive fashion than is possible in this Intermediate Evaluation Report of

[16] COM(2000) 890 final: http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html

the IAP. It covers issues of substantive law, procedural law and such non-legislative measures as statistics collection, specialised law enforcement units, specialised training, and co-operation with industry.

The Euroforum is still in the course of formation but the intention is to try and include members from consumer and civil liberties/privacy organisations.

We note that various forms of research are being mooted and believe that strong co-operation between the promoters of this scheme and the IAP would be very helpful and would avoid duplication.

1.5.4 US LEGISLATIVE POSITION

In the United States there has been a series of legislative attempts to limit the spread of harmful material on the Internet and to place obligations on Internet Service Providers. Because of US domination of the Internet and because of differences between the US and Europe in legal doctrine over such matters as freedom of speech, privacy and data protection, it is particularly important the European policy makers track events in the US. The US attempts to limit the spread of harmful material have been attacked by civil liberties groups, partly on the basis of First Amendment rights but also because the ambit of what was being described as "harmful", or the tests of what constituted "harmful content" were widely drawn.

One set of current arguments is around the Child Online Protection Act (COPA) which was first introduced by then Attorney-General Janet Reno in 1999. There have been a series of actions by the American Civil Liberties Union. The most recent position is that the Department of Justice has filed a petition for *certiorari* asking the U.S. Supreme Court to reverse the decision of the Third Circuit Court of Appeals that found the Child Online Protection Act to be unconstitutional. The case is now known as Ashcroft v. ACLU.

A further area of dispute has been over the Children's Internet Protection Act (CIPA). This new law mandates that all public schools and libraries that receive federal E-rate funds install Internet filtering technology on their computers. In a complaint filed in federal court in Philadelphia on March 20, 2001, two civil liberties bodies, EPIC and the American Civil Liberties Union are challenging the Act as unconstitutional.

1.6 Liability of Internet Service Providers (ISPs)

One of the barriers to effective law enforcement is the commercial interests of Internet Service Providers and telecommunications companies. ISPs need to balance the public responsibilities with the need to produce a profit. Internet Services Providers have historically sought to claim that they are mere conduits for data and as such should be regarded as "common carriers", with no liability for the content of data or the activities of their customers. They have argued that they are not "publishers" and that in any event it is technically infeasible for them to monitor traffic. The 'unfeasibility' argument has sometimes been strengthened by claims about the costs of any monitoring – costs which would have an impact on another ambition of governments and the Commission – that citizens should have very cheap and easy access to the Internet.

As pointed out in the Communication on illegal and harmful content, the term "Internet service provider" is often used generically, without a clear distinction being made between the *service of providing access to the Internet* and the *service of hosting content*. The same organisation can of course fall within both categories. Since June 2000 we have the Electronic Commerce Directive [17]. Article 12 defines the circumstances in which a service provider can claim to be acting as a "mere conduit"; Article 13 covers the position of "caching" data (that is, the use of automatic, intermediate storage of data to improve service performance); Article 14 describes ISP liabilities where a "hosting" service is provided but where the ISP has no actual knowledge of illegal activity; Article 15 says that Member Nations shall not impose a general obligation on providers to monitor. However legislation in a number of European countries now imposes a requirement for ISPs, under warrant, to provide certain forms of assistance to law enforcement, including the furnishing of details about customers and the facilitation of surveillance.

In practice, ISPs offer a bundle of services to their customers and attract different sorts of liability for each. The basic service is simple connection to the Internet. The ISP does no more than connect the subscriber's computer to the main Internet: what the user does thereafter depends on the user's knowledge, resources and skills. In this form the ISP claim for "conduit" status is most easy to sustain. But few ISPs offer only this service, and where they do it is usually for corporate customers who are linked by permanent leased line. ISPs aiming at the retail market typically also provide email receipt and dispatch, newsgroup receipt and dispatch, proxy or caching server for World-Wide Web receipt, and minimal web-hosting facilities. In addition, ISPs may also offer games servers, chat room facilities, more sophisticated web-hosting facilities (for example for e-commerce), a "portal" environment of information and services, and web-based email access. As a broad guide, the liabilities of ISPs work out as follows, but note that there are a number of national variants:

- **ISP liability in respect of email** Here also the ISP has a strong claim to being a mere conduit; the analogy with the postal and voice-based telephone services is very strong.
- **ISP liability in respect of web access** By "web access" is meant access for customers to the whole of the World Wide Web. Again the ISP has a strong claim to being a mere conduit.
- **ISP liability in respect of web-hosting** This is the situation where the ISP rents his customer space on a computer which is permanently connected to the Internet and is running web-server software. Typically the ISP has no moment-by-moment control over what his customers publish on the web via these means; the customer has access to the web-server via FTP and can load up what he likes. The ISP is only able to exercise control after the event and once matters have been brought to its notice. The means then open to the ISP are to close down the specific web-publishing facilities and/or to terminate the customer's contract.
- **ISP liability in respect of access to newsgroups** The newsgroups exist internationally; once a message is posted to one news-server, universal software ensures that it is transmitted to all other news-servers. The process carries on without human intervention. Individuals "subscribe" to those newsgroups that interest them and client software on the user's computer captures new messages for viewing on the individual's own computer. Historically newsgroups have provided a means for paedophiles to make contact with

[17] Directive 2000/31/EC of 8 June 2000

each other and to exchange pictures. At a technical level most ISPs provide their customers with news-servers; access to each ISP's news-server is controlled either by looking at the poster's IP address (which will be within a restricted set) or by username/password. ISPs have sought to claim that in this instance too they act as "mere conduits" and this view has been upheld in the United States; however in the UK it has been held that, for the purpose of the law of defamation, the ISP is a "publisher", bound to carry out "reasonable actions" once notified. (Godfrey v Demon). The reasonable action will usually mean deleting a message from the local news server controlled by the ISP; the ISP can do little about all the copies that will subsist on other servers[18]. More relevantly to the IAP, ISPs can control *which* of several thousand newsgroups they take and law enforcement agencies have sought to persuade ISPs not to take newsgroups which feature obviously illegal material. It is one of the main functions of hotlines to collect data on offending newsgroups. In most European jurisdictions it is thought that an ISP who, after notice, continued to make certain newsgroups available would be open to criminal charges of distribution.

- **ISP liability in respect of access to chat-rooms** As can be seen from the next section of this Report, there are several sorts of chat-room:
- **Chat-room runs to IRC specification, but is not hosted or facilitated by ISP** Here the ISP has a good claim to say that he is acting as a mere conduit
- **Chat-room runs to IRC specification, and is hosted by ISP but not moderated** Here again the ISP has a good claim to say that he is acting as a mere conduit and, unlike the position of newsgroups, where messages are held for a time on a news-server computer controlled by the ISP, here all conversations are in real-time and are not stored in any form. A chat-room with an obviously illegal theme might attract a charge of incitement or "aiding and abetting" an offence
- **Chat-room runs to IRC specification, and is hosted by ISP and is moderated** The fact of the possibility of real-time intervention is likely to make the ISP liable if illegal content is exchanged, but since most of these chat-rooms are hosted from the US, there may be a conflict with free speech rights under the First Amendment – the ISP may find it difficult to intervene
- **Chat-room runs to proprietary specification but is not moderated** The ISP may have a claim to say that he is acting as a mere conduit because all conversations are in real-time and are not stored in any form. A chat-room with an obviously illegal theme might attract a charge of incitement or "aiding and abetting" an offence
- **Chat-room runs to proprietary specification and is moderated** The fact of the possibility of real-time intervention is likely to make the ISP liable if illegal content is exchanged
- **Web-based chat-room, not moderated** The ISP may have a claim to say that he is acting as a mere conduit because all conversations are in real-time and are not stored in any form. A chat-room with an obviously illegal theme might attract a charge of incitement or "aiding and abetting" an offence
- **Web-based chat-room, moderated** The fact of the possibility of real-time intervention is likely to make the ISP liable if illegal content is exchanged, but since most of these chat-

[18] It is possible to issue a cancel message – in fact almost too easy to do so because of the weakness of the newsgroup protocols; but the Internet convention is that only the *author* of a message should cancel it.

rooms are hosted from the US, there may be a conflict with free speech rights under the First Amendment – the ISP may find it difficult to intervene

- **Liabilities of auction sites and others allowing customers to update inform without intervention** The situation here is similar to that of a proprietary chat-room which is not moderated. Controversy has arisen in France and Germany where customers have uploaded offers for sale of Nazi memorabilia. In the case of Yahoo, the French courts have sought to order Yahoo to find a means of preventing such items being offered for sale in France. Yahoo, however, is an international company and in its home jurisdiction of the US, the sale of such material is quite legal and is upheld by the First Amendment of the US Constitution.

- **Liabilities of ISPs and telecommunications companies to assist law enforcement** As we have seen, these provisions either already exist in a number of European countries (the Netherlands and the UK have recently updated their legislation to extend the scope and to require ISPs to maintain certain facilities to aid data interception) and they are in any event envisaged in the Council of Europe Cybercrime Treaty. Any of these powers have to be subject to the ECHR where among other things, a test of *proportionality* must be applied.

2. TECHNOLOGICAL AND MARKET DEVELOPMENTS

2.1 Introduction

The purpose of this section is to flag significant technological developments that appear to be important and have an impact on the future path of the general aims of the IAP as well as, more specifically, its three Action Lines. Forecasts are limited to the next three to four years; this period takes us beyond the current IAP.

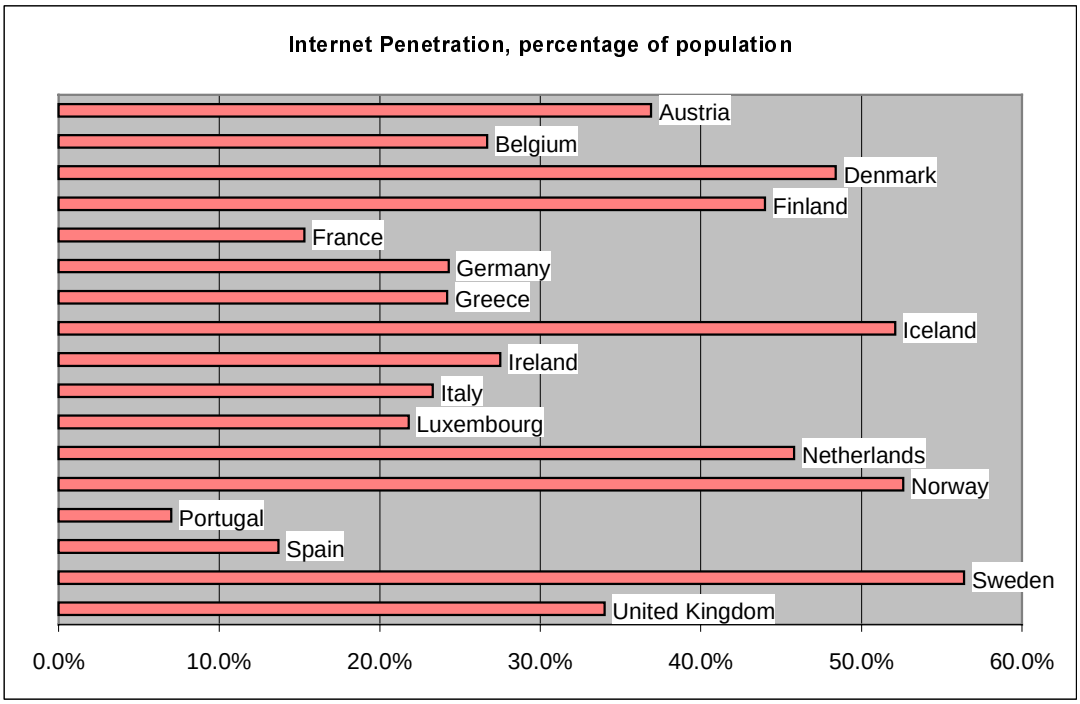
The information has come from other work in the public policy and commercial arenas carried out by members of the evaluation team, from publicly available reports. The assessments are partly those of the team and partly those of a limited number of respondents.

The assessments aim to assist the IAP to consider the following questions

- have the assumptions about technology made in mid-1997 for the first stage of the IAP proved correct?
- what assumptions about future directions in technology should be built into any revised intervention logic?

2.2 Demographics

We begin by looking at current demographic patterns as this must influence, country-by-country, policy development.



The chart above shows the level of penetration selected European countries [19]

[19] source: www.nua.ie, April 2001 – note the dates for data for individual nations may vary; some of the figures may be almost 12 months old.

In general terms, it seems to reasonable to assume the larger the percentage the greater the chance that there will be a significant proportion of users who are less sophisticated in terms of their computer fluency and their general level of education. In turn this must have some impact on, for example, judgements about the ability of parents to use filtering software and to understand some forms of "awareness" advice.

Data about the numbers of children accessing the web is a little more difficult to come by:

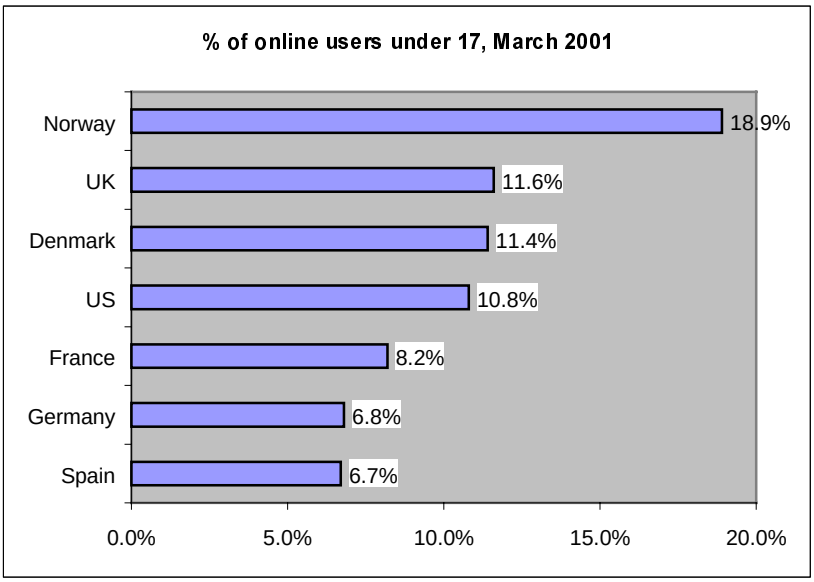
- In Italy, research from Eurispes reported in February 2001 that 1.5 million Italian children between 6 and 11 use the web.

- In the UK polling agency NOP reported in December 2000 that 4.8 m children aged 7-16 were using the web, though a significant proportion of these were doing so from school, as opposed to home.

- Survey company Jupiter MMXI said that in the UK in October 2000, 2-14 year olds were 10.7% of the UK Internet-using population but that this had risen to 15.2% by February 2001, possibly the effect of Christmas purchases.

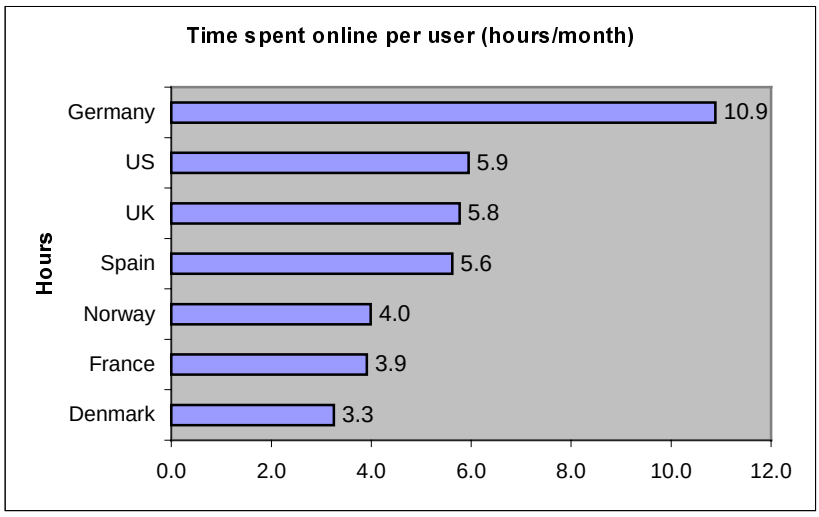
- The Austrian Internet Monitor said in April 2001that 80% of Austrian "young people" had web access.

- In May 2001, a NetValue study based on work carried out up to the previous March said that in the UK more than one in nine children under 17 connects to the Internet at home. It said that the number of under 17s online in the UK has grown by 44 per cent over the previous six months, from more than one million users in October to almost 1.5 million in March. Under 11s account for 249,000 users in the UK, with 1,236,000 users aged between 11 and 16. It went on to assert that more than a quarter of all UK youngsters visited gambling sites (382,000), remaining for an average of 11.3 minutes and one in five (290,000) visited pornography websites, remaining for an average of 28 minutes. Half of all under 17 users visited music and literature websites in March and 40 per cent visited games sites.



Of the countries included in the survey, Norway has the highest proportion of users (18.9 per cent of Internet population) under 17. The UK has the second largest, ahead of the US and other major European countries (Denmark, France, Germany and Spain).

German youngsters spent almost 11 hours online in March, more than twice the average for the rest of Europe. They also connect most often, logging on to the Internet for an average of 2.8 sessions per day. US kids are in second place, connecting for an average of 2.3 times per day with Danish youngsters connecting the least, for an average of 1.7 sessions per day. American and British kids spent just under 6 hours online [20].



These figures, from commercial sources, are probably not detailed enough or gathered sufficiently frequently to provide all the assistance the IAP needs, **yet reliable figures about the usage children make of the Internet are essential to the establishing the rationale of the IAP and its various action lines.**

[20] Sources: NetValue: http://www.netvalue.com; http: www.zdnet.co.uk/news/2001/18/ns-22732.html

2.3 The Universal Service Issue

In the consumer market the cost of Internet access is seen as a barrier to wide take-up. In 1999 the Committee of Ministers of the Council of Europe in Strasbourg adopted Recommendation (99) 14 on universal community service concerning new communications and information services. Member States are recommended to support the establishment of public access points and the provision of universally accessible information and services for the public at large[21].

When consumer-orientated Internet services were first launched the tariff pattern was that consumers would pay a flat monthly rate to an ISP, typically around 15-20 Euro per month. But the consumer also had to pay telephone call costs which were on a time basis and which might also involve a set-up charge. As a result of the combination of competition between ISPs, privatisation and deregulation of telephone companies and government pressure to bring the "knowledge economy" to their citizens, other tariff schemes have appeared, e.g.:

- "free" ISPs: companies that do not charge any monthly fee to subscribers but hope to make income from advertising (and sometimes a commission on the use of telephone calls). The customer still has to pay a local phone call and if he wants help from the ISP has to obtain it via a premium rate telephone call.

- "complete tariff" ISPs, who combine the ISP connection fee with a discounted rate for the telephone call.

- "pay as you go" ISPs, where the customer has no long-term contractual commitment to the ISP but pays a per-minute rate which combines both the ISP-access and telephone elements.

The largest of the "free" ISP services appear to continue to prosper, with some suggestions that in the UK almost 90% of all consumer Internet connections take place through them. One difficulty in the statistics is in detecting those who hold multiple "free" ISP accounts.

The problem for those policies designed to use ISPs as a means of limiting the spread and availability of harmful content is that nearly all of them involve costs to the ISP – filtering, moderation, "know your customer" checks, co-operation with law enforcement. Given the current strong competition between ISPs for customers it seems possible that many are operating on very narrow margins: ISPs may be unable to "give away" family- and child-friendly services.

On this basis, the desire of European governments to promote low cost near-universal Internet service may conflict with the aim of those same governments to provide a "safe" Internet.

[21] (http://www.coe.fr/cm/ta/rec/1999/99r14.htm)

2.4 Broadband

Broadband services, for this purpose, refer to high-speed telecom services delivered to the home and office. Typical home-offered services provided a down-stream speed of 512k and up-stream of 256k, though some services can offer 2MB both up-stream and down-stream.

The two main technologies are xDSL[22], which is transmitted along suitably modified conventional "copper" telephone wire (and which coexists with the regular telephone service) and cable, which is an adjunct to cable television distribution. Other technologies such as the use of dedicated localised radio transceivers and satellite downlinks, have not yet made any impression on the market-place.

European governments are generally keen to advance the growth of broadband as a means of making high quality Internet access ubiquitous to citizens. Commission figures released in March show that less than 8 percent of EU homes access the Internet via cable modems, while 1.1 percent have ADSL connections. A world-wide survey from NetValue in April, said that 57 percent of Korean households with Internet access were using a broadband connection, while only 3.1 percent of UK households were, although this was up from 1.6 percent in November 2000. The US had the second highest level of broadband use at 11 percent, followed by Hong Kong at 8 percent and Singapore at 7 percent. Other countries in the top ten were Taiwan, France, Denmark, Germany, and Spain. As far as ISDN use is concerned, Germany leads the way with almost 38 percent of Web-enabled households using ISDN. Denmark is next with 19.5 percent followed by Hong Kong with 5.2 percent and China with 3.9 percent.

For the IAP there are two areas of significance:

- broadband permits the fast transmission of large files and/or large quantities of small files and also allows streaming of high quality video. It is thus reasonable to expect that, whatever benefits ensue, the publication and distribution of harmful and illegal material will grow.

- although it is not of the essence of the service, in practice, broadband tariffs are sold at a flat rate and not per minute. The service is described as "always on"[23]. The effect is that most broadband users change their Internet-usage habits markedly and spend much more time online. In general terms this is seen by most as an advantage, both for education and e-commerce. But it also means that children in broadband homes, freed from the restrictions of worrying about a telephone bill, are able to spend much more time in chat-rooms, on web-sites etc where there is a risk that they will become exposed to harmful content. Parents will not have the arrival of the phone bill to signal to them that their child's usage may have suddenly increased.

2.5 Chat Rooms

[22] xDSL is the generic term; most current offerings are actually ADSL – Asymmetric Digital Subscriber Line

[23] This is not strictly true in that a broadband connected home-based computer may not enjoy a permanent connection to the Internet and may not automatically acquire a fixed IP address

Chat is a communication involving small numbers of people in a "room" or on a "channel". There are large numbers of such rooms that operate on a theme basis. Participants type messages to each other in real time. This is in contrast to the old-established Usenet or Newsgroups and the slightly newer list-server schemes [24]

Chat-rooms as potential sources of abuse have recently come to public attention following a number of widely reported cases in which adults have persuaded children met in chat rooms to go to a "real-life" meeting at which the child has been in danger. In March 2001 the UK Internet Crime Forum (ICF, described in section 4.5.1 of this report) published a guide to the problem together with series of suggested counter-measures entitled *Chatwise, Streetwise*[25] It is the real-time element that can give chat-rooms their addictive quality and also make them much more difficult to monitor. One of the main areas of danger is that participants can and do assume fictitious and misleading personalities; this may simply be a harmless game, but can also be used by predators.

At the level of technology there are three broad categories of chat-room:

- "IRC" chat-rooms based on an open Internet standard called Internet Relay Chat. All that a provider needs is a computer permanently connected to the Internet running server software that complies with the standard. Client software is widely available to ordinary users. At any one time there are about 400 IRC servers available on open access on the Internet, connected into networks and sub-nets. Some IRC servers are provided by regular ISPs, but many are not. The ICF guide referred to above states that "The dynamic nature of IRC means that it is impossible to give an accurate figure for the number of servers or channels available at any one time" and also states that "of a list of nearly 400 servers visible on IRC on 15 October 2000, only 10 appeared to be located in the UK, of which just half were run by UK ISPs. Additionally, any individual with sufficient knowledge can set up an IRC server for a relatively modest financial outlay - currently just the price of a PC and about £1500 [2300 euro] per annum for the hosting costs". This fragmentation and the possibility of near-anonymity make regulation and law enforcement more difficult.

- Proprietary chat-rooms, typically owned and run by a large ISP such as AOL. Admission is only via membership and the chat-rooms likely to be used by children are often moderated.

- Web-based chat-rooms, typically owned and run by large ISPs such as Yahoo and Microsoft Network. Access to the service is via an ID, which is acquired after filling in a simple form. In most cases, the details on the form are not checked.

In terms of the potential for controlling access and activity in chat-rooms:

[24] A list-server is a program which allows participants to share ideas with each other via email; each message is sent to all members of the “list”; a “list” can be either moderated or unmoderated but has the advantage over newsgroups is that there is usually far less “noise”. A list-server can be set up on any computer with a permanent Internet connection or via an advertising-supported facility such as OneList (http://www.onelist.com)

[25] available from http://www.internetcrimeforum.org.uk/

- IRC chat-rooms: unless an IRC server is owned by an ISP within the jurisdiction of an offence, law enforcement measures are likely to have limited effect. Most general-purpose ISPs have no means of restricting the activities of their customers and hence cannot by technical measures prevent their use of third-party IRC servers, even if they wanted to.

- Proprietary chat-rooms: the large sponsoring ISPs appear to be open to persuasion in terms of: moderated chat-rooms, and possibly the use of real-time content filtering programs and "know your customer" policies.

- Web-based chat-rooms: sponsoring ISPs are here in a slightly weaker position in developing a "know your customer" policy, as the web-service is not linked to any other service which requires, for example, that an accurate address and credit-card details be provided. Since web-based chat-rooms use the same technology as the World-Wide Web, there are no technical measures to prevent people from using them. Furthermore, the most popular web-based chat systems are based in the United States, which means that a purely European-based enforcement arrangement would be ineffective. However, providers of such services may be open to international pressure to accept higher levels of self-regulation.

In the near future we may see the widespread adoption of variants of the chat-room which use web-cams so that the faces and voices of participants replace typing

For many purposes, protection of children, therefore, would seem to have to depend on education and awareness actions. **However, the IAP may wish to consider commissioning research into the possibilities and value of technical measures for chat-rooms.**

2.6 Instant Messaging Services

Instant messaging is sometimes described as a cross between a telephone call and e-mail. Users install a piece of software on their PC and enter a list of “online buddies” into the program. Once they log on to the Internet, they can exchange instantly displayed messages with buddies who are also connected.

In mid 1999, AOL dominated instant messaging, controlling roughly 90% of the traffic with its AOL Instant Messenger (which everybody on the Internet, not just AOL subscribers, can use and which is usually automatically installed along with the Netscape Navigator / Communicator program) and ICQ, an Israeli firm that AOL bought in 1998. Competing services are Microsoft Messenger, Yahoo! Messenger or PowWow; the various services are technically incompatible though AOL has been under considerable pressure to agree to and meet a world-wide standard. MSN and Yahoo had increased their market share by the end of 2000, with some evidence that enthusiasts join more than one service. By May 2001 AOL were claiming 100 million registered members world-wide; however it was not clear how far this business was profitable.[26]

In terms of the IAP, the potential avenues for abuse are that:

[26] http://news.cnet.com/news/0-1005-202-5874501.html. “Registered” users is not the same as “active” users. The main potential income is from advertising

- on joining, children reveal more of themselves than is sensible.
- the systems do not check the details of the members so that masquerading is relatively easy.
- the technical possibilities of tracing abusers depend on the co-operation of the major service providers, none of which is based in Europe.[27]

2.7 Peer-to-Peer Networking

Peer-to-peer networking (P2P) refers to the situation where individual computers on a network communicate with each other directly, without going through a central server. Shortened to P2P, it is currently being written up in computer journals as one of the next big things in computing. One of the triggers for this interest has been the story of Napster, which is a good illustration of how the technology works in practice.

Under Napster, which was set up to facilitate the exchange of music encoded in the MP3 format, the central Napster resource simply provides lists of music files which are available from various Napster members. Once one member identifies a file and a computer location for it, the Napster software installed on their computer automatically initiates a direct connection with the computer where the desired file is located, and downloads it. Thus the central Napster resource never holds copies of the desired files –and this was the basis of Napster's case when challenged by copyright holders. Napster can be thought of as some sort of referring agency - a common feature of some P2P services.[28].

In Internet terms, P2P services should be seen in contrast to those coming from a world wide website (where information is centrally held) or a FTP server (where a central computer holds collections of files which it releases to users on request) or newsgroups (where messages are distributed via a network of servers that distribute messages to allow ho subscribe and keep each other up to date by means of feeds) and IRC-based chat, where a server mediates the conversations. Under IRC it is possible for participants, having identified each other, to go off and have a private conversation by initiating a so-called DCC – Direct Computer to Computer Connection. The DCC is then an example of P2P

P2P is currently being advanced as a possible anti-censorship, anti-central control technology.[29]

---

[27] ICQ has attempted to shut out adults posing as children. (http://news.cnet.com/news/0-1005-200-1810683.html?dtn.head) but, for a service that is given away "free" against the possibility of being able to target advertising at its customers and which allows membership from all over the world, there seems very little that a Instant Messaging service can do to verify the accuracy of the information members provide.

[28] A more general explanation of the technology and its supposed advantages can b e found at:
http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html. See also the Gnutella project: http://www.gnutella.co.uk/ and also http://www.infoanarchy.org/ and http://www.slyway.com/

[29] See for example the Freenet project: http://www.freenetproject.org/ and also http://www.infoanarchy.org/ and http://www.slyway.com/

For the purposes of this evaluation report, however, we need to concentrate on the impact, if any, that P2P may have on Internet governance and the potential for the spread of illegal and harmful content. **The main problem for the IAP is to decide how far P2P technologies might change the landscape.** The assessment of the evaluators is that:

- In many P2P services there is no real organisational centre, or if there is, its legal status and liability may not be obvious. Thus law enforcement may be difficult.

- Capturing an audit trail of activities between two users may be difficult, as there will be no centre at which a log file can be created. The "referring agency" computer, e.g. the computer similar to Napster's, will only hold details of the identities of participants, not of their interactions or even, necessarily, of the times of their interactions. Thus evidence may depend either on seizing the computers of participants and hoping to find log files from application programs, or requesting interception at an ISP. In the latter case, because P2P bypasses the usual Internet system that identifies computer hosts, an ISP log file would need to be interpreted against information form the "referring agency" computer - which may not be forthcoming.

- On the other hand, because P2P services have no real centre, they may also be much less reliable than more conventional services, and hence less attractive to customers.

- Most P2P technology is still a little difficult for the non-computer-literate to deploy

At time of writing it is probably fair to say that P2P does not represent a large threat in terms of making harmful material easily available to children. However it seems to be increasingly used as a means for the distribution of illegal material between computer users who have fairly sophisticated skills, the attraction being the comparative difficulties law enforcement face in tracing such activity[30]. In this respect the protagonists of P2P have the same problem they have faced with other "libertarian technologies" – "free speech" can often lead to the wide dissemination of harmful and illegal content.

2.8 Mobile Phone Developments, WAP, SMS, I-Mode

WAP, I-Mode and SMS are all extensions of the cellular telephone, which bring to the portable handset data services. In December 1999 Forrester Research said that more than 219 million people, or one-third of the European population, will access Internet services using mobile phones by 2003.

WAP, Wireless Application Protocol, brings a version of the World Wide Web to the screen of a cellular phone. In order to accommodate the very limited screen size, WWW pages have to be reformatted and simplified – there is no room for elaborate layouts, frames, or anything beyond very rudimentary graphics. The content provider must make a very deliberate decision to address the needs of the WAP user.

[30] P2P, in the form of IRC DCC, was used by the W0ndeland Club, an elite global group which swapped large quantities of paedophile images

WAP-enabled cellular phones became widely available during 2000 and were sold at almost the same price as non-WAP cellular phones. Time-based tariffs for using a WAP service as opposed to making a voice-call are sometimes as low as 20% of the full rate but this varies from one cellular phone company to another and between different countries.

WAP was heavily promoted throughout Europe during 2000 but is already being seen as something of a failure or a mere step to more advanced services based on 3G technology – see below. The main problems have been:

- the small screen size which limits the amount of information that can be displayed
- the difficulties of using a phone keypad to enter text
- the slow speed at which information is provided – 9.6 kb as opposed to the 56 kb of the regular dial-up line
- the comparative paucity of information which people feel they *must* have while on the move
- the lack of an immediate widely-available security protocol which might encourage e-commerce transactions such as banking and retail purchasing

Cellular phone companies usually sell their WAP phones with a pre-installed "portal" service, so that favoured sites are available quickly and easily. It is often quite a complex process to add new "favourite" sites. Despite the technical limitations, there are a number of WAP-porn sites.[31] There does not appear to be any way of setting up a self-rating scheme within the WAP browser or installing content filtering software

I-Mode is a service similar to WAP but using different protocols. In May 2001 the system had about 23 million subscribers. First launched in Japan where it appears to have been very successful, in November 2000 NTT DoCoMo said that it would establish a U.K. subsidiary and a research lab in Germany to further strengthen its position in Europe[32]. Plans for launch in the Netherlands, Germany, Italy and Belgium have been announced.[33]

In September 2000 the Japanese police made their first arrest of someone creating a pornographic I-mode website[34] One recent interactive service is one where you pay a small amount each month in order to have a virtual girlfriend or mistress on your mobile.

SMS, Short Message Service, is available from nearly all GSM cellular phones. As the name implies, messages are short, limited 160 characters. Text entry is from the cellular keypad but some cellphones contain firmware with "predictive text" – full words are guessed from the first few characters. Users often adopt informal contractions – "GR8" meaning the English word "Great" for example. In April 2001 the GSM Association reported that 15 billion SMS (short message service) text messages were sent over GSM networks in December 2000. This represented a fivefold increase on the corresponding figure a year before. The average amount of text messages sent per customer per month had grown from 0.4 in 1995 to 35 by the end of 2000. The Association predicted that 25 billion text messages would be sent

[31] See news stories at http://www.wap.com/share/osas/cache/artid550591.html and http://www.wap.com/services/0/80.html
[32] http://www.thestandard.com/article/0,1902,18994,00.html
[33] http://news.bbc.co.uk/hi/english/business/newsi_1124000/1124567.htm
[34] http://asia.internet.com/wireless/2000/9/0921-japan.html

monthly by December 2001 and over 200 billion by December 2002. In the UK, the number of text messages sent per month grew 300 percent in a year to 756 million by December 2000, while 1.8 billion text messages were sent in Germany in the same month. Typical cost for sending an SMS is around.0.15 euro.

There have been a few cases of schoolchildren "harassing" each other by bombarding schoolmates with hateful SMSs.

Related to SMS is the facility, available on some cellular phones, for "logos" to be sent via SMS. The logos replace the normal display on the phone; low-resolution pornographic images are available for commercial download.

In terms of relevance to the IAP:

- WAP is currently delivered in a "walled garden" mode set up by the cellular phone company and significant effort is required by the user to travel beyond the garden. It is limited in its graphical qualities. It lacks a chat mode. It is now widely seen as an intermediate stage in the development of mobile data services. Nevertheless pornographic services are available and there appears to be no means of filtering them out
- I-Mode is not yet available in Europe and precise timings for its rollout are difficult to guess. It is possible that widespread availability in Europe may be delayed until the rollout of 3G services. Although it will be probably be delivered in "walled garden" mode, pornographic sites already exist.
- SMS is essentially at one-to-one service. Just as individuals can initiate abusive phone calls so abusive SMSs can also be sent.

2.9 Third-Generation Mobile Telephony: 3G

Third Generation Mobile telephony is the general name for a range of services that should bring always-on high-speed mobile services with, among other things, colour full-motion video and Internet. In March 2001 the Commission adopted a generally optimistic Communication entitled *The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward.* [35]

The European specification is called UMTS or Universal Mobile Telephone System but the US looks as though it will adopt an alternative called CDMA2000 and the largest Japanese mobile operator, NTT DoCoMo, had said it would launch 3G services in May 2001 but later announced a launch for October 2001[36]. The European version will probably roll out in 2002-3 but as with most rollouts of this kind, the initial applications are likely to be aimed and priced at the business user rather than the domestic consumer.

It seems likely that 3G devices will be developments of the current range of PDAs (Personal Digital Assistants) rather than based on PCs. The various contending operating systems could include PalmOS, Pocket Windows, Symbian and Linux. Among other things, Internet filtering software, if desired, would need to be written especially for these platforms.

[35] http://europa.eu.int/ISPO/infosoc/telecompolicy/en/comm-en.htm
[36] http://news.bbc.co.uk/hi/english/business/news_id13200000/1320821.stm

In any event, there is some debate about the speed with which 3G will appear in Europe and indeed elsewhere:

- there are a number of competing protocols and is doubtful if the major handset manufacturers will want equally to support all protocols and specifications simultaneously
- without handsets which are attractive, light-weight and easy to use, take-up of 3 G could be slow
- a number of European countries chose to auction off licenses to the radio spectrum to be used for 3G. It is now generally conceded that licensee-holders over-bid and are now short of the capital needed to build the infrastructure –particularly local base stations – needed to support the services
- there are no reliable indications of levels of tariff; and even if there were the level of competition they might face at launch from fixed high-speed services is unknown
- there are as yet no obvious "killer applications" which would justify end-users in buying into 3 G services
- in the US, Europe and Far East, there are signs of an economic downturn, which may deter adventurous investment plans.

It thus looks as though any impact of 3G on the aims of IAP will only be felt after the end of the period for which this Report is attempting a forecast.

2.10 Interactive TV

Digital television is another medium which potentially can offer connectivity to the Internet and other interactive services.

Many set-top boxes designed to give access to digital television services from satellite or terrestrial sources also contain a modem to enable connection to the telephone. Some contracts, such as the Sky Digital contract in the United Kingdom require that subscribers also connect their set-top box to a phone line. Two reasons for this is to allow updating of software and ordering of pay-per-view broadcasts but another important reason is to create an audience for its interactive shopping/banking/email service originally called Open[37]. This is a "walled garden" – that is, it does not allow full Internet access and shows services (which may be similar to those on the Net) in its own proprietary format, which is more suited to digital TV use.

The UK's terrestrial digital service, Ondigital[38], also supplies a box which, with the addition of a keyboard gives full access to the Internet. In March 2001 Sky had 4.7m digital customers while Ondigital had only 1 million.

[37] http:// www.bib.co.uk. In May 2001 some consolidation of Sky's interactive services took place

[38] http:// www.ondigital.co.uk

The UK is usually regarded as currently the world's most advanced for consumer-orientated digital television.

A number of TV manufacturers are also offering so-called Internet TVs; these are regular analogue terrestrial TV sets that also contain a modem and feature a keyboard. These sets contain, in firmware, a world web browser and email client but they cannot receive newsgroups, chat facilities or other Internet services. It is also possible to buy, for about 110 euro, a set-top box that plugs into an existing television to give the same set of facilities.

A small number of ISPs are producing content specifically for Internet-enabled TVs (whether digital or analogue). In general terms the main change is that the page design recognises that TV displays cannot handle the detail of most computer monitors.

Demographically the significance of interactive services via digital television is that the group of people who subscribe to digital television are thought to be markedly different from those who purchase PCs and acquire an ISP contract. Digital TV attracts an audience interested in sport and entertainment. The Sky marketing strategy in particular is to "give" their subscribers interactivity in the form of shopping and banking whether they want it or not so that when eventually a subscriber decides to make an interactive purchase the whole procedure is effortless.

In terms of the IAP:

- The walled garden approach of Sky means that it is highly unlikely that harmful and illegal material will arrive in the home via its services. Their set-top box has a parental control feature so that if material with a sexual content is ever incorporated in their offer it can be readily limited to adults.

- The position of Ondigital and the Internet TVs which offers unlimited access is more parlous – the service is limited to the world wide web and email and newsgroups and chat are not available. But restrictions on the material from the web depend on parents setting a filter (using RSAC) but of course these will only work if the individual web-publisher has self-rated the pages – see below.

2.11 Internet Content Filtering

It seems quite likely that the much of the public cannot distinguish between the two main means of providing filtered Internet content to PCs – self-rating schemes and content filtering software. If self-rating is shown to lack adequate support from Internet content providers then that places greater expectations on the possibilities of content filtering software.

Initially most of the emphasis was on a self-rating scheme. The essence of the plan was – and is – that web content providers should self-rate their pages on the basic of the RSACi (or some other) scheme and that widely used browsers would recognise the rating through meta-tags (not normally visible data) written on to the pages. Since August 1996 Microsoft Internet Explorer has had facilities to recognise the RSACi scheme and to link them to a "content advisor" option which allows parents to restrict sites according to various criteria. Netscape Navigator, the other very popular browser has had similar facilities since June 1998.

The Commission contracted with INCORE (INternet COntent Rating for Europe) to produce a report on self-rating which was published in April 2000 (see vol I 3.2.2).[39] The main content-rating scheme is now run by ICRA (Internet Content Rating Association)[40], which is the coordinator of the ICRAsafe project funded under the IAP [41] .

However, although the main browser software recognises the PICS/RSCAi/ICRA categories, take-up by web content providers has so far been very slow. ICRA's web-site claims that 120,000 web-sites are registered with their scheme (and can display their seal of compliance); in a phone call in early April 2001 they told us that the figure was now up to 160,000. But as proportion of the number of pages believed to be on the web, this is a tiny number and the growth reported at ICRA's website (www.icra.org) is not keeping up with the growth of the web. According to the search engine www.alltheweb.com, for example, it has indexed 600 million unique web pages. HP in their current advertisements suggests that the size of the World Wide Web is about 2.7 billion pages.[42]

On this evidence and for whatever reasons, self-rating has not so far captured the attention of the vast majority of web content providers; one problem must be that the exercise of rating a page, and making sure that the rating is compliant with ICRA guidelines may involve costs which are difficult to justify commercially; it is interesting to note how few of the web-publishing packages encourage or remind designers to use rating facilities.

Yet public demand for the *idea* of rating schemes appears to be strong. As a result there has been a growth in the provision of add-on computer facilities which can examine content in real-time irrespective of whether it has been self-rated by the originator – *content filtering*. There are a number of different sorts of package. First as to where they are installed:

- they can be installed on an individual computer – obviously the only approach that will work in the home environment but with the danger that a child may be able to circumvent parental control

- they can be installed on a filtering server, which might be at an ISP (if they offer a "walled garden product") or on a network (such as might exist at a school or library)

Second as to how they work:

- they can react to particular words and filter any pages that contain objectionable ones

- they can block access to a number of pre-defined (and changeable) "objectionable" sites. One problem here is that a list of such sites has to be kept constantly up-to-date

- they allow access only to a number of pre-defined (and changeable) "good" sites. This approach is usually only sensible for sites used by the very young. Again there is the that a list of such sites has to be kept constantly up-to-date

[39] http://www.incore.org/final_report.htm
[40] http://www.icra.org
[41] http://europa.eu.int/ISPO/iap/projects/icrasafe.html
[42] Figures taken in April 2001; ICRA's statistics are based on *sites* not pages; one site may of course contain several hundred pages.

Some filtering software vendors claim that they can use more sophisticated forms of real-time content filtering and some also claim that they can filter out objectionable images. Both the US *Consumer Reports* and the UK's Consumer Association *Which?* have recently conducted research into the effectiveness of prominent content filtering packages and found the results disappointing.[43]

The Commission-supported Benchmarking Study from the Joint Research Centre, as presented, looks as though it will provide an extremely useful and rigorous evaluation process.

The original INCORE Report said: "Most consumers are attracted by the principles and potential benefits of self-rating and filtering. Such systems can allow each user to apply their own cultural values, even though there are considerable differences between their values at language group, national and individual levels. Existing systems do not however fulfil the promise of such systems. The main problem is limited access to content because insufficient sites are labelled. European consumers naturally look for sites in their own languages and very few non-English language sites are labelled…. We do know, from more direct contacts, that some major European content providers have reservations about the implications of labelling in terms of cost and potential barriers to access for those who do not label. Others are very supportive"

From the perspective of the IAP, it will be obviously important to be able to distinguish between the widespread support that exists for both content-rating and filtering and the practicalities of delivering them.

[43] According to *Consumer Reports*, filtering software generally fails to block about a fifth of objectionable content. The magazine tested six software packages on 139 sites that were known to contain objectionable material such as sexual content and the promotion of crime, bigotry, violence, tobacco and drugs. It found that Cyber Snoop and Net Nanny offered poor protection, while Cyber Patrol, Cybersitter 2000, Internet Guard Dog, and Norton Internet Security 2001 offered fair or good protection. AOL's parental control settings were also tested by the magazine. It found the Young Teen settings "pretty effective," as they blocked 86 percent of undesirable sites. The Mature Teen settings, however, only blocked 70 percent of objectionable sites. Further information on: http://www.consumerreports.org/Special/ConsumerInterest/Reports/0103fil0.html and also at http://www.getnetwise.org/americalinksup/parentstips/browsers.html. A paper from the UK Consumer's Association was circulated at the Filtering Awareness Day in Brussels on 15 February 2001.

APPENDIX 1 – LIST OF RESPONDENTS INTERVIEWED

FILTERING			INTERVIEWS		9 Telephone	Depth
France	Netprotect	Mr.	Robert	Havas	x	x
Germany	Netprotect	Mr.	J	Ritzke	x	
United Kingdom	Euforbia	Mr.	M	Cady	x	x
Finland	Med-Certain	Mrs.	Vappu	Taipale	x	
France	3W3S	Mr.	R.	Foka	x	x
France	3W3S	Prof.	Bernard	Merialdo	x	
United Kingdom	ICRASAFE	Ms.	Clare	Gilbert	x	
United Kingdom	ICRASAFE	Mr.	Ola-Kristain	Hoff	x	
United Kingdom	ICRASAFE	Mr	Chris	Gretton	x	x

HOTLINE			INTERVIEWS	9		
United Kingdom	Inhope	Mrs	Ruth	Dixon	x	x
Ireland	Inhope	Mr	Cormac	Calanan	x	x
Netherlands	Inhope	Mr	Alex	De Joode	x	
Germany	Inhope	Mr	Thomas	Rickert	x	
Belgium	Securenet	Prof	Joseph	Dumortier	x	
Sweden	Face-it	Mr	Lars	Lööf	x	
Denmark	Red	Miss	Marianne	Pihl	x	x
Italy	Basic	Mrs	Francoise	Barner	x	
Iceland	EPCP-Internet	Mrs	Sveinbjörg	Pálsdóttir	x	

AWARENESS			INTERVIEWS	13		
Spain	Infonet	Mrs	Ana Luisa	Rotta	x	x
Italy	Infonet	Dr	Dario	Cipiolla	x	
Austria	Sui	Mr	Friedrich	Lennkh	x	
United Kingdom	Once	Miss	Rachel	O'Connell	x	x
Ireland	Once	Mr	John	Hurley	x	x
Belgium	Educau-Net	Mr	Patrick	Verniers	x	
Italy	Friendly Internet	Dr	Laura	Galli	x	
Italy	Friendly Internet	Prof	Franco	Favilli	x	
United Kingdom	CISA	Mrs	Ann	Davidson	x	
United Kingdom	Dot-Safe	Mr		Blamine	x	
United Kingdom	Dot-Safe	Mr	Tony	Parkin	x	
Greece	Sifkal	Dr	Veronica	Samara	x	
United Kingdom	Susi	Mr	Nick	Morgan	x	

STAKEHOLDERS						
Belgium	Ministry of Justice	Mr	Van	Vaerenbergh	x	
Belgium	Police (federal computer crime unit)	Mr.	Luc	Beirens		x
Belgium	Judge	Mr.	C.	DeValkeneer		x
Finland	Mannerheim League for Child Welfare	Ms.	Helena	Molander		x
France	Transfert	Mr	Christophe	Agnus	x	
France	Le Monde	Mr	Yann	Chapellon		x
Germany	Fireball	Mr	Thomas	Adler	x	
Germany	Step 21	Mr.	Philip	Graf Döhnhoff		x
Ireland	Dept of Justice, Equality, Law & Reform	Mr	John	Haskins	x	
Ireland	Child Psychologist	Ms.	Marie	Murray		x
Ireland	Film Censor	Ms.	Audrey	Conlon	x	
Norway	Statens Filmtilsyn i Norge (film censors)		Dag	Asbjørnesen	x	
Spain	COFACE	Mrs	Esther	Pinilla	x	
Spain	Ministerio de Ciencia y Technología	Mr	Fernando	Fazio		x
Spain	La Vanguardia	Mr	Fèlix	Badia	x	
Switzerland (Germany)	Sprecher der Aktion Kinder des Holocaust (AKdH)	Mr.	Samual	Althof	x	
United Kingdom	DTI	Mr	Tony	Eden-Brown		x
United Kingdom	Internet Magazine	Mr	Steve	Hill	x	
United Kingdom	Home Office	Mr.	Stephen	Ruddell	x	
United Kingdom	ISPA	Mr.	Nicholas	Lansman	x	

NON PARTICIPANTS				
Sweden	ECPAT Sweden	Helena	Karlen	x
Netherlands	Magenta	Suzette	Bronkhorst	x
Germany	Social-network	Rolf Negele and Peter Niehover		x
Netherlands	Jante Benton	Erica	Euving	x

APPENDIX 2 – SURVEY QUESTIONNAIRE (PARTICIPANT)

IAP: Participant Questionnaire

Ask to speak to named person from the list.

Good morning / afternoon. My name is ……from BDRC, an independent market research agency based in London. I am calling on behalf of the European Commission. We have been asked to assess the effectiveness of the Safer Internet Action Plan in which I believe you are participating. You may recall receiving an email from Richard Swetenham about this.

Can I emphasise that we are evaluating the overall Program itself, and not any of the projects.

We are looking to talk to all project co-ordinators as well as a selection of other project partners.

Could I ask you some questions about the processes you went through to get involved in this and your opinion on the program itself ?

It will take about 20 minutes to complete the interview. Would it be possible to talk to you now or could I arrange a convenient time to call you back ?

PROJECT

ACTION LINE: (9)
- Hotlines 1
- Rating & Filtering 2
- Awareness 3

NAME

COMPANY

COUNTRY

TELEPHONE NUMBER

CALL BACK TIME

CALL BACK DATE

INTERVIEWER

DATE COMPLETED

1a First of all I would like you to think back to when you first got involved with the Safer Internet Action Plan. How did you first become aware of the plan ?

1b Has your organisation had any previous contact with the Commission?

(10)

Yes ..... 1 ASK Q1C
No ..... 2 GO TO Q2A

1c IF YES, in what way? What contact have you had ?

ASK ALL

2a. And what made you decide to get involved with the Safer Internet Action Plan?

2b. How important were each of the following in your decision to get involved ? first of all, a need for funding. Was that important ? Could you please give me a number between 1 and 5 where 1 is not at all important and 5 is very important.

Repeat for
A desire to be public spirited
We have commercial expectations from the product we are developing ?
A desire to find and work with international partners

	Not Important				Very Important	
need for funding	1	2	3	4	5	(11)
public spirited	1	2	3	4	5	(12)
commercial expectations	1	2	3	4	5	(13)
find / work with international partners	1	2	3	4	5	(14)

IF NEED FOR FUNDING CODED 3, 4 OR 5 ASK

2c Specifically, could you tell me in your own words, why did you needed funds?

2d If you had not been given funding, would you have gone ahead with the project anyway ?

(15)

Yes ..... 1 ASK Q2E
No ..... 2 GO TO Q3A

2e Why do you say that ?

ASK ALL

3a. Are you aware of any organisations who considered getting involved but did not ?

(16)

Yes	1	ASK Q3B
No	2	GO TO INSTRUCTION OVER Q4A

IF YES

3b Would you be able to tell me who that is ? EXPLAIN: As part of this research, we would also like to talk to people who decided against getting involved in the IAP to find out their reasons in more detail)

FILTERING & RATING & AWARENESS

4a. Were you involved in an information day ?

(17)

Yes	1	ASK Q4B
No	2	GO TO Q5A

IF YES

4b. How useful would you say that information day was ? Would you say….

(18)

Extremely useful	1
Very useful	2
Fairly useful	3
Not very useful	4
Not at all useful	5

4c Why do you say that ?

4d How did the information day help your project ?

4e And specifically, how useful were each of the following aspects of the day ? For each of the statements I am about to read out would you tell me how useful they were on a scale of 1 to 5 where 1 is not at all useful and 5 is very useful.

	Not At All Useful				Very Useful	
background information on the IAP	1	2	3	4	5	(19)
administrative information on the IAP	1	2	3	4	5	(20)
opportunity to talk to commission staff	1	2	3	4	5	(21)
opportunity to talk to other participants / develop partnerships	1	2	3	4	5	(22)
opportunity to hear about existing projects	1	2	3	4	5	(23)

4f What could be changed to make such information days even more useful to you ?

ASK ALL

5a. I would now like to think about the process of submitting a proposal to the Commission ? In your own words, how much support do you feel the Commission gave you in this. Would you say

	(24)	
Too much	1	ASK Q5B
About right	2	GO TO Q6
Not enough	3	ASK Q5B

IF 5a/1 or 3

5b Why do you say that ?

ASK ALL

6 What else do you think the Commission could have done ?

7 What could they have done differently ?

8 And how did the support you were given compare to any expectations you had before getting involved in the programme ? Were you…

	(25)
Given much more than you expected	1
Given a little more than you expected	2
About what you expected	3
A little less than you expected	4
Much less than you expected	5

9. How did you find the actual process of your application being assessed ?

10. What could have been done to improve this ?

11a. And since you have been given funding how do you feel about the support given to you ? Have you been given …

	(26)	
Much more than you anticipated	1	ASK Q11B
A little more than you anticipated	2	
About what you anticipated	3	GO TO Q11C
A little less than you anticipated	4	
Much less than you anticipated	5	

IF Q11A/1,2, ASK:

11b What support did you get that you thought was particularly useful? N.B MAKE SURE SUPPORT IS NOT INTERPRETED AS FUNDING

NOW GO TO Q12A

IF Q11A/4,5, ASK:
11c What additional support would you like to receive?

ASK ALL
12a Did you actually request any support ?

(27)

Yes 1..... ASK Q12B
No 2..... GO TO Q12E

IF YES
12b What support did you request ?

12c Was this given ?

(28)

Yes 1..... GO TO Q12E
No 2..... ASK Q12D

IF NO
12d Why do you think that support was not given ?

ASK ALL
12e Did you receive any support from people involved in other projects ?

(29)

Yes 1..... ASK Q12F
No 2..... GO TO Q12G

IF YES
12f How useful was this ? Would you say…

(30)

Extremely useful 1
Very useful 2
Fairly useful.....3
Not very useful 4
Not at all useful.....5

ASK ALL
12g Was information provided to you in your own language ?

(31)

Yes, written.....1
Yes, spoken.....2
No, not own language.....3

13a I would now like to think about the IAP programme in general. What do you see as the aims of this programme ? PROBE: What do you think the commission would like to get out of it ?

13b. The aims of the Safer Internet Action Plan are to combat harmful and illegal content on the internet. Overall how successful do you think the IAP will be in meeting these aims ? Would you say……

	(32)
Extremely successful	1
Very successful	2
Fairly successful	3
Not very successful	4
Not at all successful	5

13c Why do you say that?

14a In your opinion are there any differences in the handling of illegal and harmful content on the internet ?

	(33)	
Yes	1	ASK Q14B
No	2	GO TO Q15A

IF YES

14b What are the differences in the ways illegal and harmful content should be handled ?

ASK ALL

15a I am now going to read out a list of different areas of concern on the internet. First of all, could I ask you to tell me whether you feel the IAP currently covers each of these ? READ OUT, CODE ALL THAT APPLY

15b And should the IAP cover each of these ? READ OUT, CODE ALL THAT APPLY

15c And which does your specific project cover ? READ OUT, CODE ALL THAT APPLY

	15a (34	15b (36)	15c (38)
Child pornography	1	1	1
Violence	2	2	2
Medical information	3	3	3
Drugs / alcohol / tobacco	4	4	4
Dissemination of racist and Xenophobic ideas	5	5	5
Satanic / cult ideas	6	6	6
Adult Pornography	7	7	7
Advertising in general	8	8	8
Hate speech / intolerance	9	9	9

	(35	(37)	(39)
Chat rooms	1	1	1
Any others (specify)	2	2	2
None of these	3	3	3

16a. Thinking again about the Internet Action Plan, if you were responsible for the Internet Action Plan, how would you have done things differently ? First of all, when the project was initially set up ?

16b And what would you do differently now ?

17a. As you know, the programme covers Hotlines, Rating and Filtering and Awareness. Are there any other areas which you think should be included ?

(40)

Yes..... 1 ASK Q17B
No..... 2 GO TO Q17D
Don't Know..... 3

IF YES

17b What other areas are these ?

17c Why should they be included?

ASK ALL

17d Should all three Action Lines have been included ?

(41)

Yes..... 1 GO TO Q18
No..... 2 ASK Q17d

IF NO

17e Which should **not** have been included ?

(42)

Hotlines..... 1
Rating & Filtering..... 2
Awareness..... 3

17f Why do you say that ?

ASK ALL

18 And to what extent do you feel the Commission should be involved in this area overall ?

CLASSIFICATION

Finally, I have a few questions I would like to ask about your project.

C1a How many countries does your project cover ?

(43)

All of EU	1	
If less, write in number	2	…….

IF C1a/2

C1b Which countries are those ?

(44)

Belguim 1
Denmark 2
France 3
Germany 4
Greece.....5
Ireland (Rep) 6
Italy.....7
Luxembourg 8
Netherlands.....9

(45)

Portugal 1
Spain.....2
United Kingdom.....3

ASK ALL

C2 And from which countries are your partners drawn ?

(46)

Belgium 1
Denmark 2
France 3
Germany 4
Greece.....5
Ireland (Rep) 6
Italy.....7
Luxembourg 8
Netherlands.....9

(47)

Portugal 1
Spain.....2
United Kingdom.....3

C3 What types of organisations are represented amongst your partners ?

(48)

Private Commercial Organisation 1
Public Commercial Organisation 2
Governmental organisation 3
School or University..... 4
Charitable organisation / not for profit..... 5

C4 And specifically, what type of organisation do you represent ?

(49)

Private Commercial Organisation 1
Public Commercial Organisation 2
Governmental organisation 3
School or University..... 4
Charitable organisation / not for profit..... 5

C5. How long has your organisation been in operation ?

(50)

Up to 2 years 1
2 – 5 years 2
Over 5 years 3

COMMERCIAL ORGANISATION (C4/1,2)

C6. And what was your approximate turnover in the last financial year ?
Write in:

ASK ALL

C7. How many people work for your organisation ?

(51)

Less than 10..... 1
11 – 25..... 2
26 – 50..... 3
51 – 75..... 4
76 – 100..... 5
101 – 200..... 6
201 – 500..... 7
501 - 1000..... 8
1001 + ... 9

READ OUT
We will be wanting to interview some participants in more depth. Would you be willing to take part in a further interview on a face to face basis ?

Yes..... 1
No..... 2

CHECK BACK: IDEALLY NEED 10 RESPONDENTS FROM:

ACTION LINES	
HOTLINES	3
RATING & FILTERING	4
AWARENESS	3

Q13b

EXTREMELY/ VERY	7
NOT VERY / AT ALL	3

IF ELIGIBLE & WILLING RECRUIT TO DEPTH:

DATE:
TIME:
LOCATION:
CONFIRMATION SENT:

APPENDIX 3 – SURVEY QUESTIONNAIRE (STAKEHOLDER)

IAP: Stakeholder Questionnaire

Ask to speak to named person from the list.

Good morning/afternoon. My name is ….. from BDRC, an independent market research agency based in London. I am calling on behalf of the European Commission. We have been asked to assess the effectiveness of the Safer Internet Action Plan which is looking into illegal and harmful content with emphasis on the protection of minors. As part of this we are looking to talk to a limited number of interested parties including charitable organisations, journalists and politicians, whose names have been suggested to us by our evaluators.

Could I ask you some questions about your opinion on the program?

This is confidential market research. Your responses will be put together with those from all other respondents and not relayed back in a way which could be attributable to you. It will take 15 – 20 minutes to complete the interview. Would it be possible to talk to you now or could I arrange a convenient time to call you back?

PROJECT (if appropriate): _____

NAME: _____

COMPANY/Organisation/Activity (if journalist): _____

COUNTRY: _____

TELEPHONE NUMBER: _____

CALL BACK TIME: _____

CALL BACK DATE: _____

INTERVIEWER: _____

DATE COMPLETED: _____

1a First of all, could I ask how much you are aware of the **Safer Internet Action Plan** from the European Commission?

(10)

Fully Aware	1	
Have a basic idea	2	CONTINUE
Not aware before receiving email	3	
Not aware at all	4	CLOSE

1b If yes, how did you first become aware of the Internet Action Plan?

1c And when was this?

1d Could you tell me what you see as the aims of the Internet Action Plan?

2a In your opinion are there any differences in the handling of illegal and harmful content on the internet?

(11)

Yes	1	ASK 2b
No	2	GO TO 3a

IF YES

2b What are the differences in the ways illegal and harmful content should be handled?

2c. In your opinion, who should be handling illegal and harmful content ?

2d. Why do you say that ?

ASK ALL

3a I am now going to read out a list of different areas of concern on the internet. First of all, if you are sufficiently aware of the IAP, could I ask you to tell me whether you feel the IAP currently covers each of these? **READ OUT, CODE ALL THAT APPLY**

3b And should the IAP cover each of these? **READ OUT, CODE ALL THAT APPLY**

	3a			**3b**
	(12)	(14)	(16)	(18)
	Yes	No	DK	
Child pornography	1	1	1	1
Violence	2	2	2	2
Medical information	3	3	3	3
Drugs/alcohol/tobacco	4	4	4	4
Dissemination of racist and Xenophobic ideas	5	5	5	5
Satanic/cult ideas	6	6	6	6
Adult pornography	7	7	7	7
Advertising in general	8	8	8	8
Hate speech/intolerance	9	9	9	9
E-commerce	0	0	0	0
	(13)	(15)	(17)	(19)
Chat rooms	1	1	1	1
Any others (SPECIFY) _____	2			2
None of these	3	3	3	3

4a The IAP is made up of a number of Action Lines (Hotlines, Rating & Filtering, and Awareness). I would now like to look more closely at each of these Action Lines. First of all Hotlines. These are designed to give people a network of support and specifically a contact number in each member county allowing reporting of illegal and harmful sites. Were you aware of this aspect?

(20)

Yes..... 1

No..... 2

4b Currently hotlines are being set up independently in a number of European countries and are overseen by InHope. From the information you have just been given and any prior knowledge you may have, could you tell me what you think of these hotlines part of the Action Plan? **PROBE**: Is it a good idea or a bad idea?

4c What areas should the hotlines cover ?

4d Should they involve private companies, public companies or both ?

(21)

.....Private 1

..... Public 2

..... Both 3

4e Who should be responsible for ensuring they are working efficiently ?

4f How could the hotlines be improved?

PROBE: What do you think the hotlines should include ?

5a I would now like to consider Rating and Filtering. This is the part of the Action Plan which aims to use leading edge technology to prevent specified words and potentially images from being downloaded to a PC. and which may also involve self-rating or automatic filtering of words and images on webpages. Were you aware of this aspect of the IAP?

(22)

Yes..... 1

No..... 2

5b In your opinion, do you feel there is a need for this sort of programme?

(23)

Yes..... 1

No..... 2

5c Why do you say that?

5d Thinking just about Rating now, this might ask website owners to rate their site according to a pre-defined check list. How successfully do you think this will be?

(24)

Extremely successful..... 1

Very successful 2

Fairly successful..... 3

Not very successful 4

Not at all successful..... 5

5e Why do you say that?

5f How could this be improved?

PROBE: What do you think this should involve ?

5g Alternatively, Filtering devices are being developed which react to certain words or images and divert the browser or your PC to another site. How successful do you think this will be?

(25)

Extremely successful..... 1

Very successful 2

Fairly successful..... 3

Not very successful 4

Not at all successful..... 5

5h Why do you say that?

5i How could this be improved? PROBE: What do you think this should involve?

5j Both of these require software to be installed on the PC, probably performed by a parent. What impact do you think this will have on the success or otherwise of this Action Line?

5k What should be done to promote filtering and rating ?

6a The final area is awareness. This involves activities to promote awareness of the positive aspects of the internet as well as the dangers. Were you aware of this aspect?

(26)

Yes..... 1

No..... 2

6b What do you think of this part of the Action Line?

6c Do you think that actions to promote awareness should have any specific emphasis?

(27)

Yes..... 1

No..... 2

IF YES

What emphasis should this have ? PROBE: What do you think is important ?

6d How could it be improved? PROBE: What else should it involve ?

7a Having now discussed the three main areas of the Action Plan, do you feel that there are any other areas that should be included?

(28)

Yes..... 1 ASK 7b

No..... 2 GO TO 7d

IF YES

7b What other areas are these?

7c Why should they be included?

ASK ALL

7d Should all three Action Lines have been included?

(29)

Yes..... 1 ASK 8

No..... 2 GO TO 7e

IF NO

7e Which should **not** have been included?

(30)

Hotlines 1

Rating & Filtering 2

Awareness 3

7f (If not already covered), why specifically should that action line have been excluded from the Action Plan?

8a The aims of the Safer Internet Action Plan are to combat harmful and illegal content on the internet. Overall, how successful do you think the IAP will be in meeting these aims? Would you say …

(31)

Extremely successful..... 1

Very successful 2

Fairly successful..... 3

Not very successful 4

Not at all successful..... 5

8b Why do you say that?

ASK ALL

9a And to what extent do you feel the Commission should be involved in this area overall?

9b Who else do you think should be involved ?

9b Do you have any other comments about the Safer Internet Action Plan?

CLASSIFICATION

I have a final few questions. I would like to ask you about your involvement in this area of harmful and illegal internet content.

C1 What is your interest in this area? Is it …

(32)

Purely professional 1

Personal 2

Other 3

C2 To what extent is harmful and illegal content on the internet of concern to you? Is it ..

(33)

A very strong concern 1

Of some concern 2

Of little or no concern 3

C3 Why is that? As individual? As professional?

C4 Were you/your organisation involved in any way in the set up of the IAP?

(34)

Yes ..... 1 go to C5

No ..... 2 go to C6

IF NO

C5a Where there any particular reasons you were not involved ?

C5b Do you feel you should have been?

(35)

Yes..... 1

No..... 2

C5c What would you have changed about the IAP if you had been involved at the outset ?

IF YES AT QC4

C6a In what capacity were you involved?

C6b Do you feel your opinions were taken into account?

(36)

Yes, fully..... 1

Yes, to some extent 2

No..... 3

C6c What, if anything, would you have done differently?

ASK ALL

C7 And specifically, what type of organisation do you represent?

(37)

Private Commercial Organisation 1

Public Commercial Organisation 2

Government organisation 3

School or University..... 4

Charitable organisation/not for profit..... 5

Newspaper / Publication..... 6

C8 How long has your organisation been in operation?

(38)

Up to 2 years 1

2 – 5 years 2

6 – 10 years 3

11 – 20 years 4

21 – 40 years 5

Over 40 years 6

COMMERCIAL ORGANISATION (C7/1,2)

C9 And what was your approximate turnover in the last financial year?

Write in:

ASK ALL

C10 How many people work for your organisation?

(39)

Less than 10..... 1

11 – 25..... 2

26 – 50..... 3

51 – 75..... 4

76 – 100..... 5

101 – 200..... 6

201 – 500..... 7

501 – 1000..... 8

1001 +..... 9

APPENDIX 4 - INTERMEDIATE EVALUATION STEERING COMMITTEE

➢ Ruth Dixon	IWF
➢ Rudi Roth	Secretary-General, EuroISPA (association of European Internet Service Providers)
➢ Friedemann Schindler	jugendschutz.net
➢ Bernard Spitz	Conseil D'Etat
➢ Timo Takkula	European Commission

APPENDIX 5 – TERMS OF REFERENCE FOR THE INTERMEDIATE EVALUATION

Scope of evaluation

The evaluation should cover the implementation of the Internet Action Plan for the two-year period from the adoption of the Decision in January 1999 until January 2001. It should take into account any evaluation of the measures taken to protect minors and human dignity foreseen by the recommendation adopted by the Council[44] on this issue.

The specific issues to be evaluated are the following:

- relevance of the Action's objectives, priorities and means of implementation;
- the effectiveness and impact of the Action;
- its efficiency and cost-effectiveness;
- its utility and sustainability;
- causal links from resources used through to activities and presumed impacts (the intervention logic);
- lessons to be learnt in terms of legal base, resources and delivery mechanisms for possible future interventions of similar type.

Main evaluation questions

The main evaluation questions have been grouped under six headings:

i) Relevance

ii) Effectiveness

iii) Efficiency

iv) Utility and sustainability

v) Intervention logic

vi) Lessons learnt

The detailed questions have been arranged hierarchically.

It is expected that the selected contractor will use their knowledge and experience, in discussion with the Steering Group to refine these questions and propose further questions. The Commission services will set clear priorities.

i) Relevance

- To what extent are the Action's objectives, priorities and means of implementation still pertinent with respect to:
  - the continued development of the Internet and the Internet industry;
  - the evolving expectations of users?

[44] Adopted on 24 September 1998: OJ L 270, 7 October 1998, p. 48

ii) Effectiveness

- Is the Action achieving its objectives?

  It is anticipated that some research, both documentary and on the basis of interviews with relevant players, will be required under the auspices of the Steering Group in order to clarify the correct interpretation of official goals. Some typical official statements and related evaluation questions are:

– To what extent have the Action's activities started to achieve the objective of "... promoting safer use of the Internet ..."? [article 2 of Decision]

– To what extent have the Action's activities started to achieve the objective of "...encouraging, at European level, an environment favourable to the development of the Internet industry."? [article 2 of Decision]?

– To what extent have the Action's action lines started to achieve the objectives specified in the preamble to Annex I of the Decision, namely to:

  - "incite the actors (industry, users) to develop and implement adequate systems of self-regulation";
  - "pump-prime developments by supporting demonstrations and stimulating application of technical solutions";
  - "alert and inform parents and teachers, in particular through their relevant associations";
  - "foster cooperation and exchange of experiences and best practices at European and international levels";
  - "promote coordination across Europe and between the actors concerned";
  - "ensure compatibility between the approach taken in Europe and elsewhere".

- To what extent has the financial support given to beneficiaries of the Action merely substituted for investments that would have been made anyway?
- How likely is it that the inferred effects of the Action would have occurred even if the Action itself had not been launched?
- To what extent has the Action been able to engage all EU member-states, and in particular the peripheral countries?
- To what extent has the Action been able to engage third countries, and in particular candidates for accession to the EU?
- To what extent has the Internet Action Plan contributed to the achievement of the goals set out in the "Council Recommendation on the Protection of Minors and Human Dignity in Audiovisual and Information Services"[45]?

[45] http://europa.eu.int/comm/dg10/avpolicy/new_srv/recom-intro_en.html - Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity. For background, see http://europa.eu.int/comm/dg10/avpolicy/new_srv/pmhd_en.htm

iii) Efficiency

- To what extent has the legal base (the Decision) proved to be clear, consistent and unambiguous in its stipulations and requirements?
- Is the annual budget of the Action commensurate with its objectives?
- To what extent has the shared-cost funding model proved to be an appropriate means of implementing the action lines?
- How economically have the various inputs to the Action (budget and staff resources) been converted into outputs (projects, support actions, activities and other actions) and results (services and applications)?
- How efficiently did the Action's delivery mechanisms (projects, support actions, activities and other actions) target the intended beneficiaries (the Internet industry and users)?
- How does the Action compare with any similar interventions executed under Community auspices, or undertaken by national or regional governments (including those outside the EU)?

iv) Utility and sustainability

- To what extent could the positive changes or trends induced by the Action be expected to last if it were to be terminated?
- Would another kind of action or policy instrument have been more useful?
- To what extent has the principle of subsidiarity been respected? In other words, what evidence is there that the Action could not have been carried out as effectively by national or regional interventions?

v) Intervention logic

The contractor selected will be expected to reconstruct the original intervention logic of the Action. The contractor should then evaluate the validity of the apparent causal assumptions involved, relating in particular to:

- ❑ how the Action is expected to produce its intended effects;
- ❑ the Action's relationship to other, related policy interventions and relevant external factors.

vi) Lessons learnt

- Considering the operation and first results of the Action, what lessons could be drawn in terms of legal base, resources and delivery mechanisms for possible future interventions of a similar type?
- Looking ahead to the final evaluation of the Action, what quantitative indicators would it be sensible to establish related to success criteria such as state of progress of projects, attainment of project objectives, attainment of Action-level objectives, etc?

APPENDIX 6 – LIST OF IAP DOCUMENTS CONSULTED

Action Plan on Promoting Safe Use of the Internet - Basic Documents

1. European Commission, Bruxelles 16/10/96 COM (96) 487
   Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions

   Illegal and harmful content on the Internet

2. Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services

3. European Commission – Legal Advisory Board
   Response to the Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services

4. **COM (97) 582**

   Commission proposal for an Action Plan on promoting safe use of the Internet

5. **Decision N° 276/1999/EC** of European Parliament and of the Council of 25 January 1999 adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks

6. **4-year Programme 1999 – 2002**

7. **O.J.L 270/48 du 7.10.98 (98/560/EC)**
   Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity

8. Council Conclusions of 27 September 1999 **(1999/C 283/02)** on the role of self-regulation in the light of the development of new media services

9. Council Conclusions of 17 December 1999 **(2000/C 8/06)** on the protection of minors in light of the development of digital audio-visual services

1999

Internet Action Plan on Promoting Safe Use of the Internet

1. IAPPC 1st meeting 04/02/99 – Revised Draft Agenda IAPPC 1/99 EN Rev 1
2. Final Draft 4-year Work Programme 1999 – 2002 IAPPC 2/99 EN Rev 1
   A Multi-annual Community Action Plan on Promoting Safer Use of the Internet by combating illegal and harmful content on global services
3. Open Call for proposals for setting up a European network of hotlines IAPPC 3/99 EN
4. Call for proposals to demonstrate content filtering and rating systems and to prepare awareness actions: 1. The application of filtering and rating systems for Internet content 2. To promote awareness of safe use of the Internet IAPPC 4/99
5. Call for Tenders – Mutual benefit support actions IAPPC 5/99
6. *Draft* Call for Expressions of Interest "Preparatory action for a European Network of hotelines" IAPPC 6/99
7. Call for Tenders – Assistance to self-regulatory bodies in developing and implementing codes of conduct IAPPC 7/99 Rev 1
8. Rules of Procedure of the Programme Committee for the Action Plan on promoting safer use of the Internet IAPPC 8/99 EN
9. IAPPC 2nd Meeting 19/04/99 – Draft Agenda IAPPC 9/99 EN
10. Draft Minutes Internet Action Plan 04/02/1999 IAPPC 10/99 EN
11. Note for the Members of IAPPC – Results of written procedure – opinion on Work programme and the criteria and the contents of two calls for proposals IAPPC 11/99
12. Draft Minutes IAPPC 19/04/1999 IAPPC 12/99
13. Evaluation Report July 1999 – Calls for proposals for setting up a European network of hotlines and for projects to demonstrate content filtering and rating systems and to prepare awareness actions IAPPC 13/99
14. IAPPC 3rd Meeting 02/09/1999 – Draft Agenda IAPPC 14/99 EN_Rev 1
15. Note to the IAPPC – Selection of projects following two calls for proposals

IAPPC 15/99 EN

16. EU Preparatory Actions for Safe Use of the Internet IAPPC 16/99
17. Director's Report to the IAPPC IAPPC 17/99
18. Draft Minutes IAPPC 02/09/1999 IAPPC 18/99 EN
19. IAPPC 4th Meeting 06/10/1999 – Draft Agenda IAPPC 19/99 EN
20. Director's Report to the IAPPC 06/10/1999 IAPPC 20/99 Rev 1
21. Results of questions to proposers and face-to-face meetings, Brussels 21 – 22 September 1999 IAPPC 21/99
22. Draft Minutes IAPPC 06/10/1999 IAPPC 22/99 EN

Appendices:

- Four Year Budget Table
- Conferences "Initiatives related to Internet Self-Regulation"
- Slides "Internet Action Plan promoting Safer Use, combating illegal and harmful content"
- Context and background – Europe 16 October 1996 – 12 February 1999

2000

Internet Action Plan on Promoting Safe Use of the Internet

IAPPC 5th meeting 28/01/2000 – Revised Draft Agenda IAPPC 1/00
Proposition of the CE "Call for proposals for awareness actions" IAPPC 2/00
Director's Report – Commission Decision on Selection of Projects, 22/12/1999
IAPPC 3/00
IAP – Measures to be taken for intermediate evaluation IAPPC 4/00
Draft Minutes IAPPC 28/01/00 IAPPC 5/00
Evaluation Report July 2000: Call for Proposals to promote awareness of safe use of the Internet IAPPC 6/00
Evaluation Report (second evaluation) July 2000 – Call for Proposals for setting up a European network of Hotlines IAPPC 7/00
IAPPC 6th Meeting 13/09/2000 – Draft Agenda IAPPC 8/00
Short List - Awareness IAPPC 9/00
Short List - Hotlines IAPPC 10/00
Technical Background Document "2001 call for proposals for projects to demonstrate filtering software and services" IAPPC 11/00
Director's Report to the IAPPC 13/09/2000 IAPPC 12/00
Draft Minutes IAPPC 13/09/2000 IAPPC 13/00
Draft – Technical Background Document "Call for Proposals for projects to prepare awareness actions" Doc B1/00
Steering Group for intermediate evaluation of IAP Doc B2/00
Note for the IAPPC: Date of next meeting/update on implementation of the Action Plan Doc B3/00

2000 Call for Proposals

1. Official Journal
2. Technical Background Document
3. Guide to Proposers
4. Proposal Forms
5. Additional Notes for **Hotline** Proposers
6. Model Contract

Safe Internet Action Plan

Project Descriptions

1. 3W3S
2. BASIC
3. CISA
4. DOTSAFE
5. EDUCAUNET
6. EPCP
7. EUFORBIA
8. FACE-IT
9. FRIENDLY INTERNET
10. ICRASAFE
11. INFONET
12. INHOPE
13. MED-CERTAIN
14. NETPROTECT
15. ONCE
16. RED
17. SECURENET
18. SIFKAL
19. SUI
20. SUSI

Database Statistics and Listings November 2000

Awareness Day, Luxembourg, 25 January 2001, Presentations

APPENDIX 7 – EVALUATOR CVS

Philip Todd - Research Director, BDRC

Philip is responsible for all IT, telecommunications and internet research within BDRC. He began his career in Software Engineering at GEC before moving to BIS as a research consultant for 5 years. He then held a short secondment to British Aerospace before moving to Research Solutions Consultancy for 3 years, where he was Research Manager and Associate Director, prior to joining BDRC in August 1996.

With over 12 years in IT market research and consultancy, Philip has worked with major manufacturers and service providers in UK and Europe. In the Telecommunications market, he has specifically worked with PTTs as well as mobile and cable companies. He has experience of researching qualitative customer issues as well as market analysis, market modelling, and has developed price elasticity methodologies to assist with product and service development and planning .

Philip is specifically responsible for developing internet and new media research within BDRC, in the fields of e-commerce, website evaluations, and electronic brand analysis.

Philip holds a joint honours degree in Psychology and English (London University) and a Masters Degree in Computer Sciences from the University of Hertfordshire.

Lisa Garthside - Associate Director BDRC

Since joining BDRC in May 1996, Lisa has worked on a wide range of projects in the financial sector, and specifically in insurance, for Norwich Union Direct, Folgate Insurance, Generali and Eagle Star amongst others. She has extensive experience in both consumer and business qualitative and quantitative research. Before joining BDRC, Lisa spent two and a half years at Eagle Star, managing research projects for the commercial division.

Lisa commenced her market research career at Bulmershe Research, a subsidiary of NOP, in July 1990, concentrating on customer satisfaction and ad-hoc telephone research for automotive, utilities and financial organisations as well as qualitative work.

A Business Studies graduate, Lisa holds the Diploma of both the Market Research Society and the Chartered Institute of Marketing.

Peter Sommer - Research Fellow at the London School of Economics

Peter Sommer is a Research Fellow at the London School of Economics where his interest is "the legal reliability of information systems", a subject which includes e-commerce protocols, computer forensics and many other aspects of computer-derived evidence.

He has helped to develop the Secure Information Systems Masters course and its distance learning variants. His first expert witness assignment was in 1985 and his casework has included the Datastream Cowboy / Rome Labs hack, the Demon v Godfrey Internet libel and Operation Cathedral/W0nderland Club paedophile conspiracy and the Curador e-commerce sites attack. He has addressed law enforcement meetinga all over the world on computer evidence and was part of the UK delegation to the G8 High Tech Crime Workshop in Berlin in October 2000. He acts as an advisor and surveyor for leading insurers of complex computer systems.

Since December 1998 he has been Specialist Advisor for E-Commerce to the Commons Trade & Industry Select Committee and supports their scrutiny of government policy and legislation. He also lead the LSE Internet consumer-behaviour research on behalf of the Financial Services Authority.