



Australian Government  
Australian Communications  
and Media Authority

---

Australia's regulator for broadcasting, the internet, radiocommunications and telecommunications

[www.acma.gov.au](http://www.acma.gov.au)

---

# Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety

First annual report to the Minister for Broadband,  
Communications and the Digital Economy

February 2008

© Commonwealth of Australia 2007

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Manager, Communications and Publishing, Australian Communications and Media Authority, PO Box 13112 Law Courts, Melbourne Vic 8010.

ISBN 0642 78357 8

Published by the Australian Communications and Media Authority

Canberra Central Office  
Purple Building, Benjamin Offices  
Chan Street, Belconnen  
PO Box 78,  
Belconnen ACT 2616  
Tel: 02 6219 5555  
Fax: 02 6219 5200

Melbourne Central Office  
Level 44, Melbourne Central Tower  
360 Elizabeth Street, Melbourne  
PO Box 13112 Law Courts  
Melbourne Vic 8010  
Tel: 03 9963 6800  
Fax: 03 9963 6899  
TTY: 03 9963 6948

Sydney Central Office  
Level 15, Tower 1 Darling Park  
201 Sussex Street, Sydney  
PO Box Q500  
Queen Victoria Building NSW 1230  
Tel: 02 9334 7700, 1800 226 667  
Fax: 02 9334 7799

# Contents

<b>EXECUTIVE SUMMARY.....</b>	<b>1</b>
Methodology .....	3
Development of internet technologies and their use .....	3
Measures for promoting online safety .....	4
Deployment of online safety initiatives in the European Union .....	5
<b>CHAPTER 1: INTRODUCTION .....</b>	<b>7</b>
Terms of reference .....	7
Methodology and scope.....	7
Outline of report .....	9
<b>CHAPTER 2: DEVELOPMENT OF INTERNET TECHNOLOGIES AND THEIR USE .....</b>	<b>12</b>
Overview .....	12
Developments in internet content and communication .....	13
The early internet .....	14
Online communication.....	16
Online games .....	17
Spam .....	18
Illegal content .....	18
High bandwidth internet .....	19
Illegal contact.....	21
Social networking .....	21
Internet use by children and young people in Australia today .....	23
<b>CHAPTER 3: MEASURES FOR PROMOTING ONLINE SAFETY.....</b>	<b>26</b>
Overview .....	26
Addressing online risks .....	28
Filtering technologies .....	29

Development of filtering technologies .....	30
How filtering works .....	31
Strengths and limitations of filters .....	40
Future of filtering technologies .....	45
Content rating and labelling .....	45
Development of content labels .....	46
Labelling by content providers .....	47
Rating by content consumers .....	48
Computer security software .....	49
Parental engagement .....	50
Active engagement .....	50
Parental control software .....	51
Education and awareness .....	52
Evolution of online safety education .....	52
Functions of internet safety education .....	52
Targets of internet safety education .....	53
Future directions for online safety education .....	54
Legal frameworks .....	55
Illegal internet content .....	55
Child sexual exploitation .....	56
Online fraud .....	56
<b>CHAPTER 4: DEPLOYMENT OF ONLINE SAFETY INITIATIVES IN THE EUROPEAN UNION ....</b>	<b>57</b>
Overview .....	57
Introduction .....	59
European Union approach to online risk .....	59
Legal framework .....	60
Programs to address online risk .....	62
Research initiatives .....	64
Filtering initiatives .....	66
Hotlines .....	73
Helplines .....	76
Awareness initiatives .....	77
Evaluations .....	86
<b>CHAPTER 5: TRENDS AND OBSERVATIONS .....</b>	<b>89</b>
Online risks .....	89
Methods for reducing risks to users .....	89
<b>APPENDIX A: DIRECTION TO ACMA .....</b>	<b>93</b>
<b>APPENDIX B: AUSTRALIAN INITIATIVES IN ONLINE SAFETY .....</b>	<b>95</b>

Overview .....	95
Online content co-regulatory scheme .....	96
Hotline for potentially prohibited content .....	96
Criminal laws relating to the internet .....	97
Education and awareness initiatives .....	97
Other actions to promote online safety .....	98
<b>GLOSSARY .....</b>	<b>99</b>
<b>BIBLIOGRAPHY .....</b>	<b>106</b>
Legislation .....	111

# Table of figures

<b>Figure 2.1: Timeline of internet developments from 1968 to 2002 .....</b>	<b>14</b>
<b>Figure 2.2: Number of Australian internet users and availability of bandwidth, 1996 to 2005 .....</b>	<b>19</b>
<b>Figure 2.3: Use of internet technologies by age group, 2007 .....</b>	<b>24</b>
<b>Figure 2.4: Use of internet technologies by gender, 2007 .....</b>	<b>25</b>
<b>Figure 3.1: Index filtering process .....</b>	<b>31</b>
<b>Figure 3.2: Category list from one filter vendor.....</b>	<b>32</b>
<b>Figure 3.3: Analysis filtering process .....</b>	<b>34</b>
<b>Figure 3.4: Locations at which filters may be deployed .....</b>	<b>37</b>
<b>Figure 3.5: Third party filter process.....</b>	<b>40</b>
<b>Figure 3.6: Content rating and labelling .....</b>	<b>48</b>
<b>Figure 4.1: Planned expenditures under the SIAP and SIP programs, 1999 to 2008 ....</b>	<b>63</b>
<b>Figure 4.2: Operation of illegal content filter deployed by ISPs.....</b>	<b>70</b>
<b>Figure 5.1: Effectiveness of measures in addressing risks.....</b>	<b>90</b>
<b>Figure 5.2: Clusters of measures to promote online safety.....</b>	<b>92</b>

# Executive summary

This report has been prepared by the Australian Communications and Media Authority (ACMA) in response to a ministerial direction received in June 2007 to investigate developments in internet filtering technologies and other safety initiatives to protect consumers, including minors, who access content on the internet. ACMA will report annually on its findings in this regard for three years. This is the first of those reports.

*Further details of key trends and observations are at pages 89-92*

The report draws together key trends and makes a series of observations about online risks and methods for mitigating those risks. In particular, the report highlights that as users increasingly engage with interactive internet technologies, the online risks have shifted from content risks associated with the use of static content to include communication risks associated with interaction with other users.

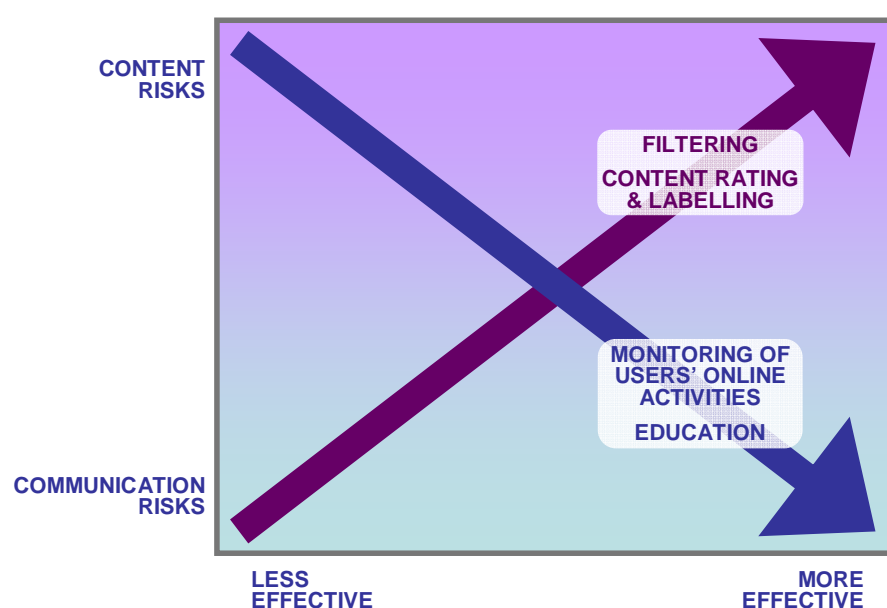
The report discusses how different online safety measures can play a part in mitigating one or more online risks. At this time, filtering technologies are regarded as suited to addressing particular static content risks. The report also discusses how the use of content rating and labelling can minimise risks associated with inappropriate static content and how internet hotlines provide a mechanism for users to report potentially illegal content to appropriate organisations for investigation. Legal frameworks also make the production and online publication of this content unlawful in some jurisdictions.

The report identifies how users can be empowered to manage the online risks they encounter. Parental monitoring of online activity can be effective in minimising both content and communication risks. Education initiatives can raise awareness of issues and provide information and support to develop protective skills and behaviours. These initiatives empower users to engage in online activities in a way that minimises exposure to the risks associated with their use of online services.

The report finds that while single measures can be effective in addressing some online risks, clusters of measures can supply a holistic approach. For example, security software plays an important role in managing risks associated with viruses and spam and, to a

degree, online fraud, while educational programs can also make users aware of how they can protect themselves against e-security risks, and in particular can alert users to particular risks—such as online fraud—for which technological measures are likely to play a smaller role than measures that encourage behavioural change.

When considering content and communication risks, the report highlights that clusters of measures can be more effective in minimising risks than single initiatives, as illustrated in the figure below. As a general rule, filtering and content rating and labelling schemes are aimed at addressing content risks, while monitoring of users' online activity and educational programs are mostly aimed at equipping users to identify and deal with communication risks.



The report observes that, given the complexity of online services, technologies and experiences, notably the newer risks associated with Web 2.0 applications, a constantly developing combination of measures that responds to changing risks is most likely to meet the challenges posed by new technologies and platforms.

To ensure awareness of the evolving nature of online risks remains current, ACMA intends in the second and third reports in this series to undertake a further survey of filtering developments in other countries and survey particular measures that address risks posed by children and young people's use of Web 2.0. ACMA also intends to explore how providers of social networking and other user-generated content services are implementing measures to minimise the risks of their sites.



## Methodology

*Further details of the report's methodology are at pages 7-9*

In undertaking its investigation of online safety initiatives deployed in other jurisdictions, ACMA drew on its experience in establishing and overseeing the current regulatory framework for online services which has been in effect since January 2000. ACMA also drew on published research and information from relevant overseas organisations, including filter vendors, online service providers and those with responsibilities for programs to mitigate online risks. This research was complemented by a study of programs deployed in the European Union (EU) to promote online safety.

## Development of internet technologies and their use

The report commences by establishing a contextual framework for the subsequent discussion of online safety in Chapter 2. It describes the emergence of internet technologies from the first use of the internet by the public, to the present. As access to higher bandwidth internet connections and new technologies has developed, internet users' interaction with internet technologies has changed. These developments mark a shift in how users engage with internet technologies—from consumption to interaction with content.

*Further information about online risks is at pages 14-23*

This change in use of internet technologies has resulted in a consequential shift in the risks to users from the internet environment. The report identifies and addresses three different types of risks to users—content, communication and e-security risks. *Content risks* include exposure to content that is illegal or inappropriate for audiences of particular ages. *Communication risks* arise from online interaction with other users and include cyber-bullying. *E-security risks* may arise when a home computer is compromised or personal information is released online and may result in identity theft.

*Further information about the use of internet technologies by Australians is at pages 23-25*

Chapter 2 also examines how Australians, particularly children and young people, currently engage with internet technologies. This research highlights that young Australians engage in a range of online activities and that, in the Web 2.0 era, their primary focus is not static content but use of interactive activities. Girls tend to spend more time communicating by instant messaging and social networking sites, while boys are more likely to spend time playing games online against other players.

## Measures for promoting online safety

Chapter 3 considers the range of measures available internationally to address online risks. These measures include filtering technologies, content rating and labelling schemes, security software, parental monitoring of children's internet experiences and education and awareness initiatives. Each of these measures has different strengths and limitations when targeting specific risks.

*Further information about filtering technologies is at pages 29-45*

Filtering technologies block access to internet content that is deemed to be inappropriate for a given user. Chapter 3 explains how filters work and the ways they can be deployed to address different filtering goals. Choice of filtering technique can affect accuracy outcomes, performance impacts and the means by which the filter may be circumvented.

This examination explains why currently available filter products can filter static web content, but have limited effect for increasingly popular communication tools such as chat and instant messaging services. Research reveals that filters are generally most effective when addressing static content of a sexual nature on commonly accessed websites expressed in English. Impact on network performance and the costs involved in providing filtering services continue to be matters affecting implementation.

*Further information about security software is at pages 49-50*

Chapter 3 examines how security software can be deployed to greatest effect to address online identity theft and other e-security risks. Security software can remove malicious software from home computers or block the receipt of malicious content.

*Further information about education and awareness initiatives is at pages 52-55*

The use of education and awareness initiatives is examined as a measure to address a range of online risks, particularly communication risks such as cyber-bullying. Raising awareness about online risks can be achieved through providing information, advice and support, and empowering users to use the internet safely and responsibly. Chapter 3 considers the targeting of education initiatives to key groups, including children of different age groups, parents, teachers and internet industry participants.

*Further information about parental engagement is at pages 50-51*

One focus of education campaigns is empowering parents to make informed choices about how to monitor their children's internet use. Educational activities can be complemented by measures such as parental control software and active engagement by parents with children's online activities and issues.

Underpinning many of these measures are legal frameworks that are being adapted to either expand the interpretation of existing legislation to the online environment, or establish new, internet-specific legislation. These laws often prohibit the use of internet

technologies to create or facilitate online risks, particularly the online sexual exploitation of children. For example, the United Kingdom (UK) introduced the *Privacy and Electronic Communications Regulations* in 2003, which prevents commercial entities from sending unsolicited electronic communication, and in Canada, the *Criminal Code* makes it illegal to use the internet to sexually solicit children.

## Deployment of online safety initiatives in the European Union

Chapter 4 focuses on the deployment of measures in the EU to promote safer use of the internet, and pays particular attention to programs implemented in the UK and Germany. The EU was selected for this survey because it was an early mover in the area of mitigating online risk, and member countries have adopted an array of measures to promote online safety. In addition, the region possesses a culture, legal system and historical approach to control of content that are not significantly different to those in Australia.

Two key EU initiatives are the INHOPE network of hotlines and the INSAFE suite of national safety nodes. All the EU initiatives including filtering and education programs are kept current by regular program evaluations and research into online risks.

The strategies employed by the EU are not dissimilar to those used in Australia, where there is an established hotline for reporting prohibited material and safety programs that emphasise technological and non-technological measures.

*Further information about the deployment of filtering initiatives is at pages 66-73*

The EU program drives and responds to the changing environment and initiatives in its member countries. Filtering has been deployed in the EU in a variety of locations, including in internet service provider (ISP) and mobile networks, and on home computers.

In the UK, BT developed the Cleanfeed ISP-level filter, which is deployed to block access to child pornography using an index provided by the internet hotline, Internet Watch Foundation. This system has now been deployed by many other ISPs internationally. A key feature of BT's Cleanfeed filter is the minimal impact it has on network performance, due to the limited scope and size of the index (not more than 1,500 websites).

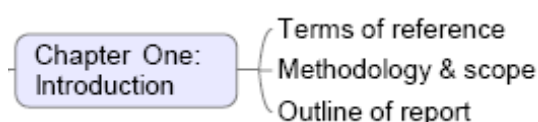
*Specific details of BT's Cleanfeed filter can be found at pages 69-70*

ACMA understands that BT's Cleanfeed filter has been deployed within the UK and by other ISPs internationally for the specific purpose of blocking a select group of web sites. While this system can be regarded as effective against web sites hosting child pornography, it is not technically designed to filter chat traffic and content that uses non-web protocols.

<i>Further information on search engine filtering is at page 71</i>	In Germany, search engine providers have agreed on a code of conduct under which they filter search results to prevent access to potentially illegal content. The EU has a three-year program to undertake a comparative survey of filters for home computers as a means of empowering users to manage online safety.
<i>Further information on INHOPE hotlines is at pages 74-76</i>	Founded by the EU, the INHOPE network of hotlines investigates complaints from the public about potentially illegal internet content, and fosters cooperation between members and key stakeholders, including law enforcement agencies, government and policy-makers. Further, INHOPE members maintain strong lines of communication with each other; for example, when content is hosted outside the country in which it is reported, it is referred to the INHOPE member hotline in the host country for action. Now found in 27 countries, INHOPE hotlines include the UK's Internet Watch Foundation, and Germany's ECO, FSM and Jugendschultz.net.
<i>Further information about the deployment of education initiatives is at pages 77-86</i>	<p>The EU's INSAFE program coordinates education and awareness activities through key organisations at the national level known as internet safety nodes. These include the Child Exploitation and Online Protection Centre in the UK and klicksafe.de in Germany.</p> <p>The education initiatives deployed in the EU target a range of online risks and diverse audiences, including parents, educators and young children. Deutschland sicher im Netz (Safer on the Net) focuses specifically on providing e-security information to internet users, encouraging parents, teachers and school children to learn about safer internet behaviour. Germany's 'Where's Klaus?' addresses a broad range of online safety issues, targeting a wide audience using an advertisement broadcast on television and the internet. In the UK, the Think U Know campaign seeks to address the risk of sexual contact by adults with children, with specifically-tailored materials to reach parents and children. This program has been embedded in the UK education curriculum and educators are provided with appropriate resources to teach children about online safety.</p>
<i>Further information about the EU's research programs is at pages 64-65</i>	Research into internet behaviour and associated safety issues is undertaken to inform policy development in the EU and its member countries. Programs such as EU Kids Online provide data that assist authorities to target new risks as they emerge and to determine where online safety messages are best targeted.

# Chapter 1: Introduction

In June 2007, ACMA was directed by the then Minister for Communications, Information Technology and the Arts to investigate developments in internet filtering technologies and other safety initiatives to protect consumers, including minors, who access content on the internet. ACMA was required to report its findings to the Minister by 31 December 2007, and in two subsequent reports to be delivered at the end of 2008 and 2009. This is the first of the three reports. The purpose of ACMA's investigation was to inform the government about developments in filtering technology and other safety initiatives, to help ensure that Australian families have access to the most effective technologies and other safety measures.



## Terms of reference

The *Protecting Australian Families Online Direction No. 2 of 2007* (Appendix A) was issued under section 171 of the *Broadcasting Services Act 1992*. The direction instructs ACMA to investigate developments in internet filtering technologies and other safety initiatives to protect consumers, including minors, who access content on the internet, having regard to:

- developments in internet filtering technologies deployable on internet service provider (ISP) servers, on home computers and on mobile phones;
- how filtering is currently deployed at each of these levels in other countries;
- legislative and administrative developments in other countries designed to promote safe and appropriate use of the internet by minors;
- contextual considerations that might impact on the relevance to Australia of the experience of other countries; and
- the challenges for internet content filtering and other internet safety initiatives posed by new technologies and platforms that permit high levels of user-generated content and social interaction.

## Methodology and scope

In investigating developments in internet content-filtering technologies and other safety initiatives to protect users who access content on the internet, ACMA has drawn on its own

experience and that of its predecessor, the Australian Broadcasting Authority, over the past decade in the establishment and oversight of the online services regulatory framework set out in the Broadcasting Services Act.

ACMA's functions under the Broadcasting Services Act include:

- encouraging development of codes of practice for the internet industry and registering, and monitoring compliance with such codes, the provisions of which are legally enforceable;
- administering a complaints hotline to investigate complaints about prohibited and potentially prohibited internet content;
- advising and assisting parents and responsible adults in supervising and controlling children's access to internet content;
- conducting or coordinating community education programs;
- researching issues related to internet content and internet carriage services;
- liaising with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the internet industry; and
- informing itself and advising the Minister about technological developments and service trends in the internet industry.

Particular information considered in the preparation of this report includes:

- literature reviews on matters related to filtering and online risk sourced from other organisations;
- quantitative research studies into user behaviour related to online risk undertaken by ACMA and other organisations;
- quantitative research on filter markets undertaken by other organisations;
- comparative test research on filters sourced from other organisations;
- previous research reports on filtering undertaken by Australian Government organisations; and
- a study of programs to mitigate online risk in countries that have adopted a range of programs in their approach to mitigating online risk, consistent with the requirement of the direction that ACMA have regard to
  - (i) how content filtering is deployed at various levels in other countries;
  - (ii) legislative and administrative developments in other countries designed to promote safe and appropriate use of the internet by minors; and
  - (iii) contextual considerations that might affect the relevance of these deployments and developments to Australia.

In line with its function set out in paragraph 94(e) of Schedule 5 to the Broadcasting Services Act, ACMA also liaised with regulatory and other relevant bodies overseas to gain information about technologies, deployments, legislative and administrative developments, and other safety initiatives, including with:

- leading filter vendors;

- bodies responsible for major government and non-government programs to mitigate online risk; and
- providers of online services.

This report is the first of three annual reports about international developments in internet filtering technologies and other online safety initiatives. It provides a context for all three reports by mapping the terrain from the emergence of the internet to the present. It describes this evolution both in terms of developments in internet content and use, and developments in filtering technologies and other online safety initiatives. The report provides examples illustrating how filtering and other online safety measures have been deployed overseas and foreshadows developments in online safety solutions and programs for exploration in the subsequent two reports.

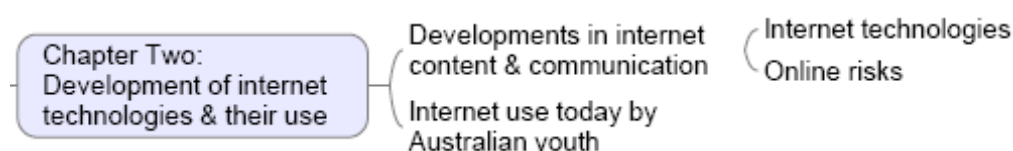
ACMA proposes to acquire and use new research for the second and third reports, and to draw on non-English sources, to provide a greater depth of evidence and widen the scope of sources of information. ACMA also proposes, in the second and third reports, to address the performance aspects of different filtering technologies in more detail, examine the development and implementation of filtering for mobile access to the internet, identify new methods of mitigating risk for users of social networking and user-generated content services, and further explore overseas initiatives.

## Outline of report

The remainder of this report is structured as follows.

*Chapter 2* describes the historical context in which the later examination of online safety measures and initiatives occurs. It describes the type of internet content that was available when the World Wide Web first emerged and how, at that time, the internet was used for communication through specific applications. Chapter 2 also describes how developments in internet technologies have changed the way users engage with the internet, and how this has changed the nature of online risks. The chapter notes that online risks manifest themselves in three forms: risks related to internet content, risks related to communication via the internet and risks related to security on the internet.

Following this general discussion of use of internet technologies and associated risks, Chapter 2 details how Australian users currently interact with internet technologies and describes services that are popular among different demographic groups. It shows that **Web 2.0**<sup>1</sup>—the growing collection of internet-based services that enable a high level of interaction between users and websites, and among internet users themselves—accounts for much of the time that Australian youth spend online.

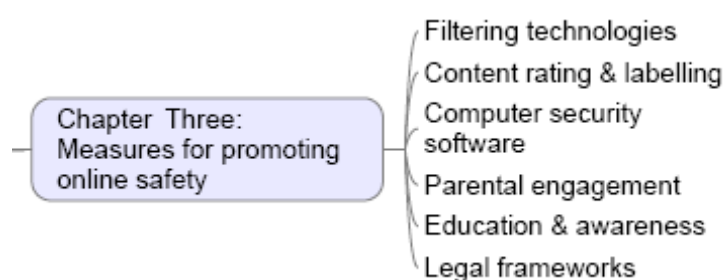


*Chapter 3* provides an overview of filtering technologies and other online safety measures. Different techniques for filtering and blocking content accessed on the internet are described,

<sup>1</sup> **Web 2.0** refers to the growing collection of internet-based services that enable a high level of interaction between users and websites, and among internet users themselves.

together with an explanation of how these technologies are deployable at different physical locations in a network. The strengths and limitations of filtering technologies deployed at different locations are also described, including the accuracy and performance implications of filtering techniques and means by which they can potentially be circumvented.

Also described in Chapter 3 are other measures to promote the safety of users who access content on the internet, including content rating and labelling schemes, parental engagement in children's online activities, computer security technologies and education and awareness programs. This survey of non-filtering online protection strategies concludes with a consideration of legal measures that specifically address online risks.

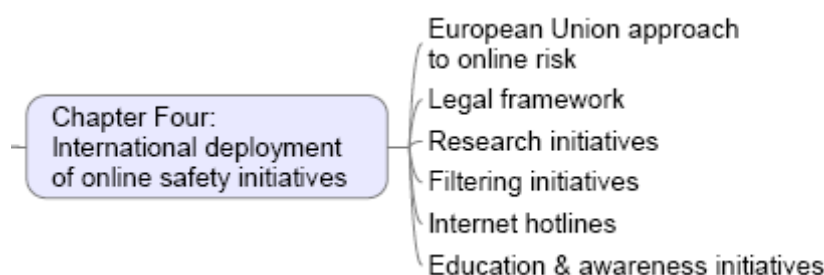


*Chapter 4* provides examples of how filtering technologies and other online safety measures have been deployed in the European Union (EU) to address online risks. The purpose of this chapter is to provide illustrations of how specific programs have been implemented to address specific online risks.

The EU was selected for this survey of deployment of online safety measures because it was an early mover in the area of mitigating online risk. Member countries have adopted an array of measures in an effort to promote online safety, and each possesses a culture, legal system and historical approach to control of content that are not significantly different to those of Australia.

While there are various approaches to online risk among the 27 member states, the EU has umbrella programs aimed at promoting responses to content, communication and e-security risks in each state. The overall objective of the programs is to encourage EU citizens to gain maximum benefit from access to the internet with minimal risk. EU programs described in Chapter 4 include those dealing with the establishment of internet hotlines, filtering schemes, education and awareness initiatives, research, measures targeted at mobile services, and the legal framework related to e-security.

Chapter 4 then proceeds to look more closely at the implementation of these and related programs in two EU member states, the United Kingdom (UK) and Germany.



Based on this 'snapshot' of internet technologies and use, the state of the art of various measures for promoting online safety and the selected examples of deployments of these



measures in other countries, *Chapter 5* presents trends and observations that reflect the findings of the earlier chapters. These commence with an assessment of the nature of the online risks for Australian children and young people today, followed by current developments and trends in the various filtering technologies, deployments of these technologies, and the extent to which they have kept pace with the nature and scale of online risks. This is complemented by a similar appraisal of developments in other online safety measures. The chapter concludes with observations about the respective roles of online safety measures in the new world of Web 2.0 applications.



#### *A note about glossary terms*

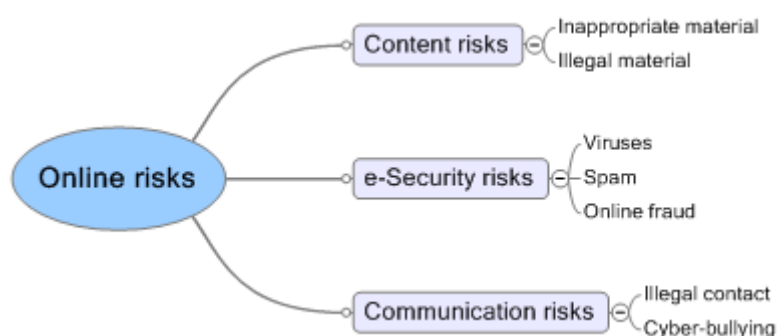
A glossary is provided, defining technical or subject-specific terminology used within the report. The first instance of each glossary term within the text is shown in **bold** to assist the reader. The glossary definition is also provided as a footnote.

## Chapter 2: Development of internet technologies and their use

### Overview

During the last 10 years the internet has emerged as a dominant communications medium. Through the World Wide Web (web), the internet has provided a platform for the publication of content on any topic and, increasingly, it has become easier for users to generate their own content. Early online communication technologies such as email, instant messaging and newsgroups have evolved to include web-based tools and user-friendly interfaces, enabling uptake by more internet users. Increasingly high bandwidth connections have facilitated the wide distribution of multimedia content such as audio and video files, and real-time communications. A range of web-based tools have emerged, such as social networking sites, weblogs and online games, which enable greater interactivity between internet users in online communities.

While users have benefited from these developments in interpersonal communication and information-sharing, their use is not without risks. These risks take various forms that are associated with how users interact with internet technologies and relate to content, communication and e-security matters.



- *Content risks* are associated with the consumption of content that has been published on the internet, and include exposure to content that is illegal and content that is considered to be inappropriate for children.
- *Communication risks* are associated with interpersonal communications on the internet and include contact with children by sexual predators and cyber-bullying.
- *E-security risks* are associated with a variety of internet activities, including the release of personal information to public forums, or simply connecting a home computer to the internet without adequate protection, and include viruses, online fraud and spam.

The global nature of the internet means that perceptions and attitudes to risk may differ from country to country because cultural differences inform what is considered inappropriate and illegal in terms of content and behaviour. Over the past decade, various measures have been developed in response to identified risks, such as an international network of ‘hotlines’ for the reporting of illegal material online. These hotlines issue take-down notices for locally hosted content and refer offshore material to enforcement agencies and other accredited hotlines for their action.

Legislative, educational and technological measures have also been developed in response to communication and e-security risks such as internet usage by adults with a sexual interest in children, or the misuse of personal information and electronic fraud.

Risks to users vary with the use of different internet technologies. Currently in Australia, children and young people use the internet for a variety of purposes, but increasingly engage in interactive online activities such as online games, instant messaging and social networking.

## Developments in internet content and communication

The internet comprises a worldwide network of interconnected computer networks that transmit data using the internet protocol (**IP**)<sup>2</sup>. These networks carry information and services comprising content and communication.

- *Content* includes text, images, audio and video.
- *Communication* refers to the ability to use the internet to communicate with other users using applications such as **email**<sup>3</sup> and instant messaging (**IM**)<sup>4</sup>.

Both content and communication applications may be accessed through either a fixed or portable device, including home computers and a proportion of mobile phones.

While the term is often used interchangeably with the internet, the web specifically refers to interlinked documents using hypertext transfer protocol (**HTTP**)<sup>5</sup> that contain text, images, video and other multimedia accessed using the internet.

Users, educators and governments recognise the benefits provided by the internet. The importance that parents place on the internet as a positive resource for children is highlighted by the higher proportion of home internet connections in households with children aged between six and 17 years old (94 per cent), compared with households without children (79 per cent)<sup>6</sup>. Concerns about young people’s access to content and communication in the online environment are considered in this context.

---

<sup>2</sup> **IP** is the language that computers use to communicate over the internet. A protocol is the pre-defined way that someone who wants to use a service talks with that service. The ‘someone’ could be a person but more often it is a computer program like a web browser.

<sup>3</sup> **Email** refers to a specific protocol that enables users to send text based messages, using a store and forward mechanism, through the internet to users at a specific destination.

<sup>4</sup> **IM** is near real time text-based or video communication between two or more users via the internet. IM applications commonly include contact lists that enable users to indicate their online presence.

<sup>5</sup> **HTTP** is the communications protocol that is used to publish and retrieve pages on the web.

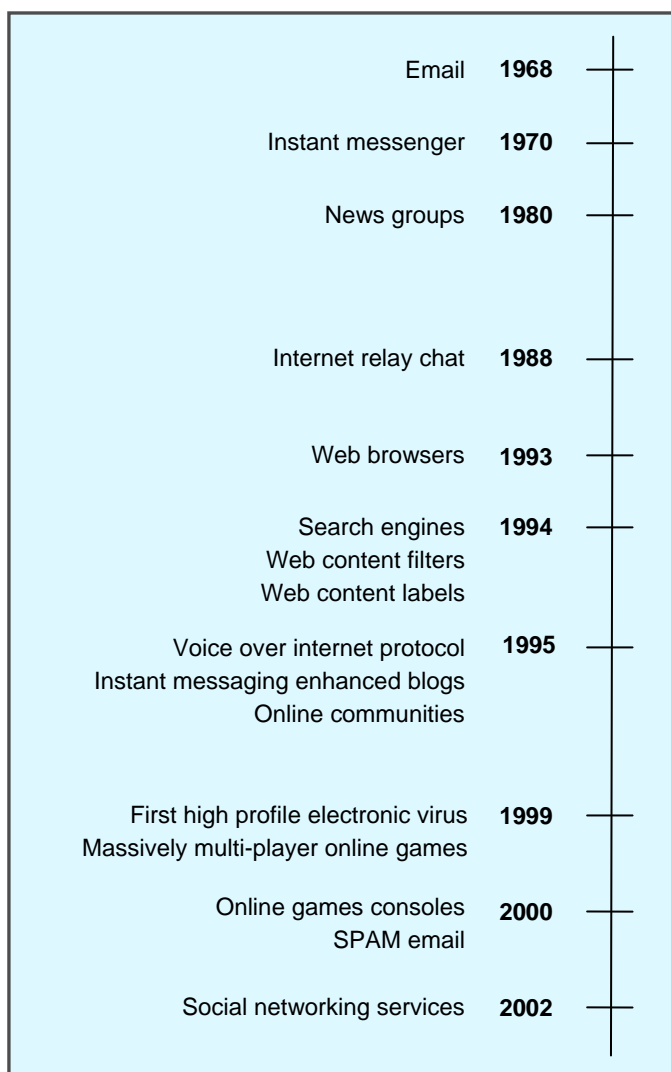
<sup>6</sup> Nielsen//NetRatings (2007), *Australian eGeneration Report, Fifth Edition*, Nielsen//NetRatings

## THE EARLY INTERNET

Since its inception, users have been able to use the internet to communicate and interact with other users, using email (first developed in 1968), IM applications (developed in the 1970s), **news groups** and **web forums**<sup>7</sup> (first developed in the 1980s) and internet relay chat (**IRC**)<sup>8</sup> (first developed in 1988).

Early take-up of internet technologies focused on the use of email for communications within and between enterprises. This was closely followed by consumption of content on the internet. The internet became widely available to a mass audience following the development of graphical web browsers in 1993. Initially, access to content was facilitated using directories and search engines. The first search engine that was able to search entire web pages, rather than web page titles, was developed in 1994<sup>9</sup>. At this time, internet technologies primarily provided access to static content that was organised topically and comprised text and images arranged on web pages. These contained hypertext links to other web pages, which provided users with easy access to ‘an almost unlimited and highly diverse (if sometimes unverified) library of information resources’<sup>10</sup> about a broad range of social and scholastic subjects.

**Figure 2.1: Timeline of internet developments from 1968 to 2002**



In 1995, the UK hotline known as the Internet Watch Foundation (IWF) and the children’s charity ChildNet International were formed. A catalyst for the formation of the IWF was the possibility in the UK that some ISPs might be prosecuted for hosting child pornography. The hotline was established following an agreement between the government, law enforcement agencies and the internet industry. In addition to the pro-social nature of the hotline, the removal of child pornography from UK servers following an IWF take-down notification

<sup>7</sup> **Newsgroups** provided an early facility for communication between multiple users. Users access content using specific software, called a news-reader. **Web forums** are similar to newsgroups, but users access content

was seen as likely to be taken in court as evidence that an ISP had made reasonable efforts to comply with legislative obligations.

ChildNet International<sup>11</sup>, a registered charity, was established with the objective of taking a balanced approach to internet usage by promoting the positive side of the medium as well as providing programs in response to its negative aspects and dangers for children.

Internet technologies were seen very early on to be potentially beneficial to young people's development, particularly when deployed in creative ways to address specific problems or create new opportunities. In 1997, Childnet International, in partnership with Cable & Wireless, developed the Cable & Wireless Childnet Awards and, later, the Childnet Academy awards<sup>12</sup> to celebrate the creativity of children, young people, schools and not-for-profit organisations that had developed innovative and outstanding websites. These awards attract entrants from a number of countries and seek to recognise 'new ideas and showcase how young people can use the internet positively and to help other young people around the world'<sup>13</sup>.

Winners of these awards have included:

- Fintan's Zone—Fintan Real, a 16 year old Australian boy, used the internet to help him overcome his physical limitations associated with muscular dystrophy. Real's award-winning website enabled him to communicate and share information that assisted him in completing homework and making friends across the world<sup>14</sup>.
- The kids channel—a resource to increase internet literacy for children and parents using quizzes, stories, and jokes. In 1999, judges commented that the project:

---

through a web browser. News groups and web forums enable open discussion between users on matters of common interest. Content is usually text based and is displayed in chronological order or organised topically.

<sup>8</sup> IRC has been available since 1988 and enables both communication between groups of users and private communication between two users. IRC is real time, text-based discussion, organised into topics of interest. Users of IRC must use a client to connect to the IRC network and receive traffic from other users. IRC is also commonly used to facilitate file sharing by enabling users to send files directly to other users.

<sup>9</sup> W3C (2007) 'A Little History of the World Wide Web', available at: [www.w3.org/History.html](http://www.w3.org/History.html), accessed 12 November 2007

<sup>10</sup> Thornburgh, D and Lin, H (Eds) (2002), *Youth, Pornography and the Internet*. National Academy Press, Washington

<sup>11</sup> Formed by a partnership between industry, government, education and law enforcement, Childnet aims to work in partnership with others around the world to 'help make the Internet a great and safe place for children'. In working towards this goal, Childnet seeks to assist young people to use the internet constructively, raise awareness among organisations, parents, teachers and carers about internet and mobile safety, and work to protect children from being exploited in online environments. The organisation also takes an active role in policy development, seeking to initiate and respond to policy changes that relate to online safety for children.

<sup>12</sup> The Cable & Wireless Childnet awards were open to young people, teachers and not-for-profit organisations that developed innovative web projects while the Childnet Academy awards are open only to young people under 18 years of age.

Childnet International (2003) 'Childnet Academy: About', available at: [www.childnetacademy.org/about/](http://www.childnetacademy.org/about/), accessed 12 November 2007

<sup>13</sup> Childnet International (2003) 'Childnet Academy: Cable & Wireless Childnet Academy Winners 2005', available at: [www.childnetacademy.org/winners/](http://www.childnetacademy.org/winners/), accessed 12 November 2007

<sup>14</sup> Childnet International (2003), 'Childnet Academy: Winners, Individual 1998', available at: [www.childnetacademy.org/winners/winners/ind98-01.aspx](http://www.childnetacademy.org/winners/winners/ind98-01.aspx), accessed 12 November 2007

... shows what one family can do on the [n]et. Getting families around a PC to surf together is hard enough. This family has gone one better, they have worked together and produced an engaging and participative resource for other families<sup>15</sup>.

Early internet technologies were taken up by business, governments and educational institutions for communication. The opportunity to use the internet to distribute content to an increasing audience was also embraced by the adult content industry. In response to this use of internet technologies, concerns associated with the increasing availability of web content in the early 1990s focused on managing access to adult content, particularly sexual content. Filters became commercially available in 1994 to block web content based on lists of inappropriate keywords and phrases<sup>16</sup> and the US Internet Content Rating Association (ICRA) developed a scheme to enable content producers to apply appropriate labels to web content. These content labels integrate with some web content-filtering software and web browsers to enable users to manage their access to specific categories of content<sup>17</sup>.

## ONLINE COMMUNICATION

During the mid 1990s, developments in internet technologies enhanced the sophistication of users' ability to communicate online, including:

- the development of voice over internet protocol (**VoIP**)<sup>18</sup>;
- enhancements to IM applications to enhance usability through a graphical user interface;
- use of the internet to post **blogs**<sup>19</sup>; and
- the development of the first online communities, such as **Geocities**<sup>20</sup>.

While the development of internet technologies in the mid 1990s focused on use of the internet for communication, concerns about the internet focused on access to 'indecent', 'offensive' and illegal material. These concerns were highlighted by the introduction of legislation such as the US *Communications Decency Act 1996*. While this Act was successfully challenged in the US Supreme Court by civil liberties groups, the development of this legislation highlights the nature of concerns at that time about access to material using internet technologies including web pages, news groups and chat services.

### Content risk: what is meant by inappropriate material?

Material that is considered to be inappropriate varies depending on the culture of the jurisdiction, the values of the guardian and the age of the child. Content that may be considered inappropriate includes: violence, nudity, coarse language, pro-anorexia or bulimia material, terrorism, race hate, advertising, gambling or social networking.

<sup>15</sup> Childnet International (2003), 'Childnet Academy: Winners, Individual 1999', available at: [www.childnetacademy.org/winners/winners/ind99-02.aspx](http://www.childnetacademy.org/winners/winners/ind99-02.aspx), accessed 12 November 2007

<sup>16</sup> Brennan Center for Justice (2006), *Internet Filters: a Public Policy Report*, The Brennan Centre for Justice at NYU School of Law, Free Expression Policy Project, p. 29, available at: [www.fepproject.org/policyreports/filters2.pdf](http://www.fepproject.org/policyreports/filters2.pdf), accessed 4 July 2007

<sup>17</sup> Family Online Safety Institute (2007), 'About ICRA', available at: [www.fosi.org/icra/](http://www.fosi.org/icra/) accessed 31 October 2007

<sup>18</sup> **VoIP** uses internet technology to transmit voice signals over the internet. Voice information is coded format and transmitted in packets of information in the form of data. The data packets are then sent across the internet and reassembled into sound at the other end for the receiver to hear.

<sup>19</sup> A **blog** or web log is an online log, similar to a public journal or diary.

<sup>20</sup> **Geocities** was an early web-hosting service that provides a forum for users to build their own websites.

Other developments in the use of the internet for communication in the mid-1990s resulted in the launch of web-based email programs, such as Hotmail. Prior to this development, email was accessed using specific applications loaded onto individual computers. The development of web-based email enabled users to access email from any web browser in any location.

In Australia, the passage of the *Broadcasting Services Amendment (Online Services) Act 1999* established Schedule 5 to the Broadcasting Services Act. It specified that access to particular categories of content be restricted and established a framework for addressing complaints about potentially prohibited internet content.

Electronic security emerged as a concern with the release of the Melissa **virus**<sup>21</sup> in 1999. This virus used email to send messages containing the virus to the contacts listed in a user's email address book. While the Melissa virus was not designed to destroy data, it disrupted the email systems of large organisations, reducing their communication ability.

#### **E-security risk: what are viruses?**

A virus is a computer program that affects a computer negatively by altering the way the computer works, without the user's knowledge or permission. These alterations can include capturing passwords, banking details or other personal information and sending it to a malicious party. Most viruses also contain a mechanism to distribute themselves further, be it automatically (a worm) or via human interaction (a Trojan horse). Modern malicious software is commonly referred to as 'malware' (a contraction of **MALicious softWARE**<sup>22</sup>).

Viruses have the capacity to destroy computer files and reformat computer hard drives. While less malicious viruses may not destroy data, they may consume storage space and degrade computer performance<sup>23</sup>.

## **ONLINE GAMES**

As uptake of the internet increased in the late 1990s<sup>24</sup>, massively multi-player **online games**<sup>25</sup> (MMOGS), such as **EverQuest**<sup>26</sup>, were developed to enable interactive game play between users in different locations. Games such as this also enable social interaction as players form online communities around each game, and have been acknowledged as offering benefits including teaching young people problem-solving skills and how to work

---

<sup>21</sup> **Viruses** are a form of malware that infects other programs on an individual's computer. Viruses may contain a single message or image that is intended to consume memory and degrade computer performance or may be more malicious and destroy data or computer hard drives.

<sup>22</sup> **Malicious software**, or malware, includes viruses, worms, trojan horses, spyware and keystroke loggers. Many early forms of malware were written as pranks that were intended to disrupt organisations' functioning rather than cause serious damage. However, malware is now increasingly used for extortion through denial of service attacks and to perpetrate online fraud.

<sup>23</sup> Trend Micro (2007), 'Virus Primer', available at: <http://us.trendmicro.com/us/support/virus-primer/index.html>, accessed 28 November 2007

<sup>24</sup> Internet penetration using dial-up connections in the UK and US reached 92 and 81 per cent, respectively, by 2001.

OECD (2001), *Household access by type of service, 2001*, available at: [www.oecd.org/dataoecd/43/26/2766850.xls](http://www.oecd.org/dataoecd/43/26/2766850.xls), accessed 6 November 2007

<sup>25</sup> **Online games** (including console games) refer to games that use the internet to enable users to engage in collaborative play and communicate with other players.

<sup>26</sup> **EverQuest** is a fantasy role-playing game in which players create avatars that are used to explore a fantasy world and interact with other players.



collaboratively with others<sup>27</sup>. MMOGs enable communication both during and subsequent to game play, enabling users to choose to engage in social interaction unrelated to the game.

## SPAM

The widespread take-up of email, first by the business community and then by users generally, resulted in an increased incidence of **spam**<sup>28</sup> email in the late 1990s. Spam email was perceived to have potentially significant economic consequences resulting from the costs associated with productivity loss and bandwidth usage, and may also contain links to malware. In response to these concerns, governments legislated to prohibit the sending of email for marketing purposes. Anti-spam legislation includes the EU *Directive on Privacy and Electronic Communications*<sup>29</sup> in 2002, the UK *Privacy and Electronic Communications Regulations*<sup>30</sup> in 2003 and the *Spam Act 2003*<sup>31</sup> in Australia.

### E-security risk: what is spam?

Spam email is unsolicited electronic messages that contain advertising material. Spam email may result in increased costs to businesses, such as increased bandwidth costs, and productivity losses resulting from employees receiving, reading and deleting large numbers of unsolicited messages. Spam email may also contain malware, such as viruses, which can destroy data.

## ILLEGAL CONTENT

As the use of the internet expanded around the world, it was used increasingly to distribute content, including illegal content. As awareness of the use of the internet to distribute content such as child pornography increased in the late 1990s, hotlines were established to enable users to report illegal internet content to authorities. Countries setting up such hotlines included Australia, France, Germany, Ireland, the Netherlands, the UK and the US. In response to complaints about content, hotlines may issue take-down notices and refer investigations to law enforcement agencies. These networking arrangements were formalised with the establishment of INHOPE in 1999. INHOPE is an international association of hotlines that exchanges expertise and reports about illegal content to facilitate a coordinated approach to minimising illegal internet content<sup>32</sup>. INHOPE currently has 30 member hotlines from 28 countries in Europe, Asia and the US.

---

<sup>27</sup> Johnson, S. (2005), *Everything Bad is Good for You: how today's popular culture is actually making us smarter*, Riverhead

<sup>28</sup> **Spam** email is unsolicited electronic message that contains advertising material.

<sup>29</sup> *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, O.J. L201/37 31.07.2002, available at: [http://eur-lex.europa.eu/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf)

<sup>30</sup> *Privacy and Electronic Communications (EC Directive) Regulations 2003*, available at: [www.opsi.gov.uk/si/si2003/20032426.htm](http://www.opsi.gov.uk/si/si2003/20032426.htm)

<sup>31</sup> *Spam Act 2003*, available at: [www.austlii.edu.au/au/legis/cth/consol\\_act/sa200366/](http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/)

<sup>32</sup> INHOPE (2007), 'About INHOPE', available at <https://www.inhope.org/en/about/about.html>, accessed 31 October 2007



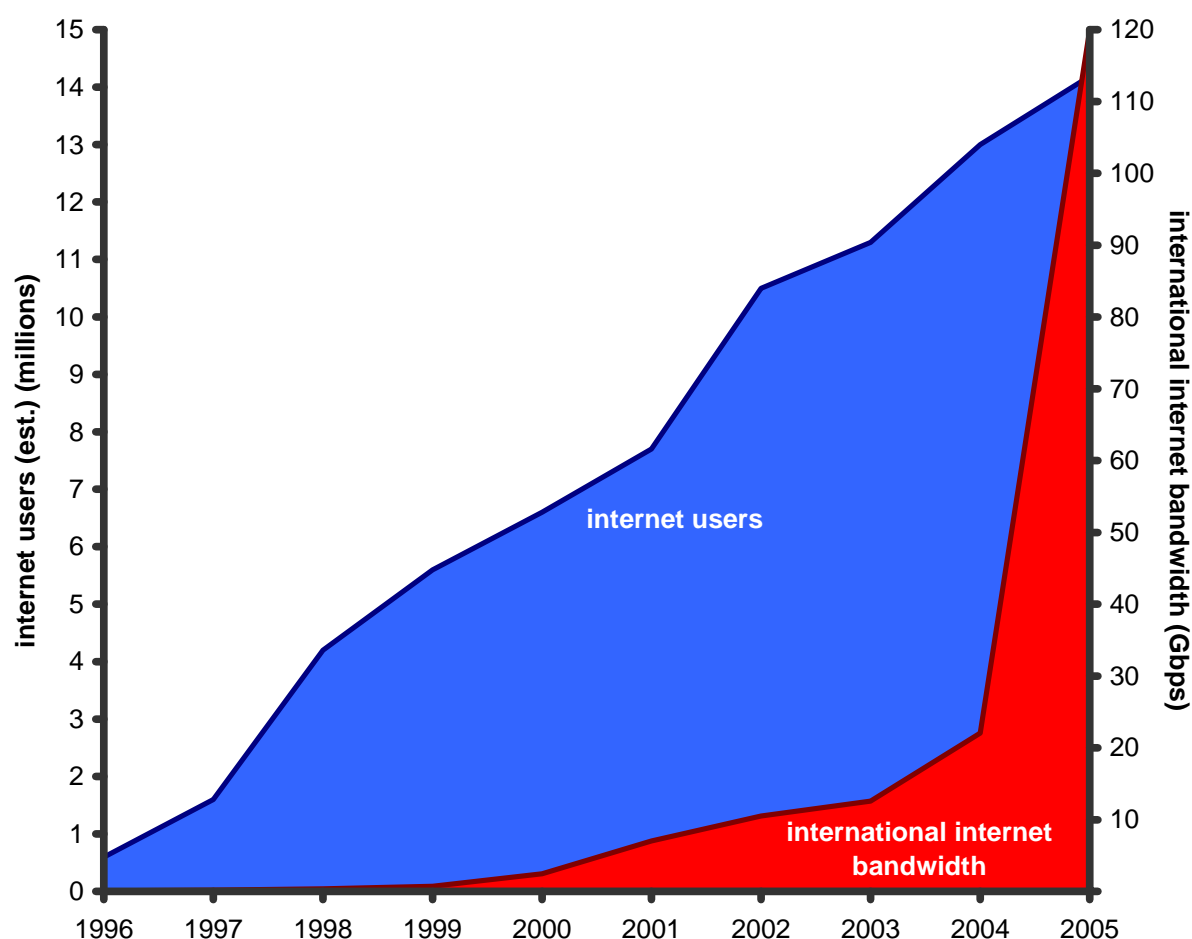
**Content risk: what is illegal material?**

Material that is considered illegal varies depending on the jurisdiction. It may include: sexualised images of children or minors, sexually explicit content, depictions of sexual violence or fetishes, violence, racism or political content. As the type of material that is considered illegal varies with different jurisdictions, it may be possible for users to access content hosted in another country that would be considered illegal in their own country.

**HIGH BANDWIDTH INTERNET**

From the early 2000s, users were increasingly able to access continuous, higher bandwidth internet connections to replace dial-up connections<sup>33</sup>. This facilitated widespread take-up of internet content such as audio, video and online games. In addition to the widespread availability of MMOGs, Sony and Microsoft released console gaming platforms in 2002 that enabled online play and voice or video communication between multiple users using high bandwidth internet connections.

**Figure 2.2: Number of Australian internet users and availability of bandwidth, 1996 to 2005**



Source: International Telecommunication Union, *Year Book of Statistics*, July 2007

<sup>33</sup> OECD (2007), 'OECD Broadband Statistics to December 2006', available at: [https://www.oecd.org/documentprint/0,3455,en\\_2649\\_201185\\_38446855\\_1\\_1\\_1\\_1,00.html](https://www.oecd.org/documentprint/0,3455,en_2649_201185_38446855_1_1_1_1,00.html) accessed 1 November 2007

The increased availability of high bandwidth also facilitated the take-up of other interactive technologies, enabling collaborative education and study, and creating opportunities for remote, near-instantaneous communication with peers, mentors and subject matter experts<sup>34</sup>. Interactive websites can be used for a wide range of educational purposes. Some examples from the Childnet Academy of award-winning educational websites are:

- [www.bonjour.org.uk](http://www.bonjour.org.uk)—a web resource developed to help students learn French in the UK. The website uses interactive games, quizzes, and exercises on various topics and is a resource used by schools world-wide. Subsequent to the success of the original online language resource, similar web sites have been developed to assist in the teaching of Italian, German and Spanish. In 2003 judges commented that the resources was:  
... [a] real labour of love from one individual teacher who has responded to a need to produce language resources in an accessible, fun and relevant way. It is excellent that the site is non-commercial and clearly teachers, parents and students are benefiting from one individual's dedication to help others learn French. The opportunities to replicate this model for other languages are enormous<sup>35</sup>.
- [lameladinewton.it](http://lameladinewton.it)—*La mela di Newton* won in 2004. The website examines themes of science, technology and multimedia, developed by an Italian 14 year old. This website is used frequently by Italian teachers and students who can access video clips, chat and forums<sup>36</sup>.

Winners of Childnet Academy awards in 2005 travelled to Jamaica to receive their awards and received a share of the Academy's web development fund to continue to enhance their projects.

In the early part of this decade, the widespread take-up of online communication applications such as email, **chat**<sup>37</sup> and IM increased as high bandwidth internet penetration became widely available. In addition, communication applications have become embedded in web pages, removing the need for specific software and further increasing their uptake. This began with web-based email programs and chat services. In addition to the use of specific communication applications, users also began to use static content such as blogs to communicate with other users and produce their own **user-generated content**<sup>38</sup> for consumption by others. The use of static content to communicate also marks a shift in the skills required to produce internet content. Previously, specific skills and software were required to develop web pages that were edited before being uploaded onto the internet.

---

<sup>34</sup> Thornburgh, D and Lin, H (Eds) (2002), *Youth, Pornography and the Internet*, National Academy Press, Washington

<sup>35</sup> Childnet International (2003), 'Childnet Academy: Winners, Individual 2003', available at: [www.childnetacademy.org/winners/winners/ind03-04.aspx](http://www.childnetacademy.org/winners/winners/ind03-04.aspx), accessed 12 November 2007

<sup>36</sup> Childnet International (2003), 'Childnet Academy: Winners, Individual 2004', available at: [www.childnetacademy.org/winners/winners/ind04-03.aspx](http://www.childnetacademy.org/winners/winners/ind04-03.aspx), accessed 12 November 2007

<sup>37</sup> **Chat** services take two primary forms—internet relay chat (IRC) (discussed above) and web-based chat services, which developed as use of the web proliferated. Initially, chat sites provided users with access to a number of chat 'rooms' organised topically. While these sites are still available, web-based chat functionality is increasingly added to individual sites to encourage discussion about the content of the site or a topic of interest.

<sup>38</sup> **User-generated content** generically refers to publicly available content that is generated by end-users on the internet.

## ILLEGAL CONTACT

While communication technologies, such as chat and IM, are frequently used to facilitate communication between individuals that are known to each other off-line, they can also be used to communicate with individuals who are only known in the online environment. The increasing use of these applications, particularly by young people, resulted in public concern about the potential use of these applications by adults with a sexual interest in children. Responses to this concern include legislative and educational measures, for example, amendments to the following were passed to specifically address illegal contact online:

- the Canadian *Criminal Code* in 2002<sup>39</sup>;
- the UK *Sexual Offences Act 2003*<sup>40</sup>;
- the Australian *Criminal Code Act 1995* in 2004<sup>41</sup>; and
- Title 18 of the *United States Code*<sup>42</sup> in 2005.

However, legislative measures are only able to respond to online risks after the fact. Education campaigns aimed at parents, children and service providers, to forewarn users of online risks and develop avoidance strategies, have also been developed. For example, the UK Home Office Task Force on Child Protection on the Internet developed the *Good practice guidance for the moderation of interactive services for children* in 2005. The guidance was produced in response to public concern about the safety of children using interactive communication services<sup>43</sup> and provides specific advice for service providers about how to effectively monitor online chat services, online games with chat or IM facilities and **message boards**<sup>44</sup> to maximise the safety of young people using the services.

### Communication risk: what is illegal contact?

Illegal contact is communication between adults and children with the specific purpose of forming close personal relationships that are subsequently used to arrange physical meetings for the purpose of sexual exploitation.

## SOCIAL NETWORKING

A recent development in the use of online technologies is the increased popularity of websites across jurisdictions that combine content and communication features, providing users with space for social interaction. These websites, including [MySpace](#), [Facebook](#), [YouTube](#), [Friendster](#), and [Bebo](#), provide facilities for users to create and share **profiles**<sup>45</sup> containing personal information or content. They enable users to post video clips or images

<sup>39</sup> *Criminal Code 1985*, available at: <http://laws.justice.gc.ca/en/C-46/>

<sup>40</sup> *Sexual Offences Act 2003*, available at: [www.opsi.gov.uk/ACTS/acts2003/20030042.htm](http://www.opsi.gov.uk/ACTS/acts2003/20030042.htm)

<sup>41</sup> *Crimes Legislation Amendment (Telecommunications Offences and Other Measures Bill (No.2) 2004*, available at: [www.frli.gov.au/comlaw/Legislation/Bills1.nsf/0/609515684FFB15C0CA256F72002610E7/\\$file/04149b.rtf](http://www.frli.gov.au/comlaw/Legislation/Bills1.nsf/0/609515684FFB15C0CA256F72002610E7/$file/04149b.rtf)

<sup>42</sup> *United States Code*, available at: [www.law.cornell.edu/uscode/](http://www.law.cornell.edu/uscode/)

<sup>43</sup> Home Office (2005) *Good Practice Guidance for Moderation of Interactive Services for Children*, available at: <http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation.pdf?view=Binary>, accessed 31 October 2007

<sup>44</sup> **Message boards** enable users to post messages online, accessed through a web browser. Content may be text-based or may include images, video or audio content.

<sup>45</sup> **Profiles** on web pages contain personal information about the user that is often shared with a network of other users that may or may not be known to the user in the physical world. Profile information is primarily used for to maintain and develop friendships.

and communicate with friends through blogs, message boards, email or IM applications. Users are also able to 'tag share' web pages using social bookmarking services such as [del.icio.us](http://del.icio.us) and [Digg](http://Digg).

Users are able to use their web browser to edit and save content online. Using these technologies, children and young people can express themselves and keep in touch with friends in an environment where their parents are not physically present. The use of the internet by young people for communication, via **social networking**<sup>46</sup> services and other user-generated content services, can have positive benefits for them, such as fostering a sense of independence and self-reliance. In addition, these websites enable users to engage and interact *en masse* with internet technologies to both produce and consume content. The benefits of sites such as [www.matmice.com](http://www.matmice.com) have been recognised by the Childnet Academy. Matmice.com was developed by children for children and won first prize in 2002. It provides space for children to create their own web pages and produce their own content. Judges commented that the website was:

... [a] technically superb site which allows young people to interact and create pages in a non-commercial environment. The webpager kit is so easy to use and translates across cultures and language, evident in that children from over 100 countries have now contributed<sup>47</sup>.

However, the increased uptake of these services and large number of users posting personal information online via blogs, message boards and IM on social networking and other user-generated content sites has also increased the potential for the misuse of such personal information. Information in profiles can be used by unintended audiences to commit identity theft. Specific personal details, such as full name, address and date of birth, are often contained in profiles and can be used to illegally produce identities for online fraud. These concerns have been addressed by the introduction of legislation to address electronic fraud such as the UK *Fraud Act 2006*, which makes it illegal to use false representation to gain personal information such as banking details from a user<sup>48</sup>.

#### **E-security risk: what is online fraud?**

Online fraud is the use of personal information to commit theft or fraud online. It may involve theft through the harvesting of personal information that has been posted by users on websites to create fake credit accounts, or the use of malware to access banking information or passwords.

Posting images online can increase risks to users because the images may inadvertently contain information that identifies the location of the user, such as a school name or a significant landmark, or provide information about the user's wellbeing. Possible ways in which personal information that is available online can be detrimental to individuals includes the use of such information for cyber-bullying.

---

<sup>46</sup> **Social networking** refers to using the internet to build and maintain relationships with other users. Most social networking websites contain features that include personal profile information, blogs, message boards, chat and email.

<sup>47</sup> Childnet international (2003), 'Childnet Academy: Winners, Individual 2002', available at: [www.childnetacademy.org/winners/winners/ind02-01.aspx](http://www.childnetacademy.org/winners/winners/ind02-01.aspx), accessed 12 November 2007

<sup>48</sup> Home Office (2006), *Home Office Circular 042 / 2006*, available at: [www.knowledgenetwork.gov.uk/HO/circular.nsf/WebPrintDoc/4597CD4C98B621418025724B004D9C6A?OpenDocument](http://www.knowledgenetwork.gov.uk/HO/circular.nsf/WebPrintDoc/4597CD4C98B621418025724B004D9C6A?OpenDocument), accessed 6 November 2007.

Developments to address emerging online risks include expanding the ICRA content labelling scheme to a broader range of digital content. The scheme was revised in 2005 to expand its reach to other types of digital content, in addition to that available from websites<sup>49</sup>.

#### Communication risk: what is cyber-bullying?

Cyber-bullying incorporates a range of offline behaviours including harassment, intimidation, stalking, threats and abuse. Cyber-bullying may take a range of other forms including **sharing information, communications or images**<sup>50</sup>, **personal intimidation**<sup>51</sup>, **impersonation**<sup>52</sup>, **exclusion**<sup>53</sup> and **'happy slapping'**<sup>54</sup>.

The UK Home Office Task Force on Child Protection on the Internet convened a project group in late 2006, currently nearing completion, to prepare good practice guidance for providers of social networking and other user-interactive services. The project was established to ensure that users of these services are informed about the risks associated with using these types of services.

The *Communications Legislation Amendment (Content Services) Act 2007* extended the Australian legislative framework established by Schedule 5 to the *Broadcasting Services Act 1992* to include mobile internet and live content services.

## Internet use by children and young people in Australia today

As can be seen from the previous section, risks online have evolved and been responded to as new content and communications technologies have emerged. This section will examine how young people in Australia currently use internet technologies. This information will highlight how current use of the internet by young people in Australia is similar to the use of the internet by young people in other countries and that young Australian users actively engage with services that permit high levels of user-generated content and interactivity.

Consumers use the internet to access a variety of services, including news and information, shopping, social networking and user-generated content sites. The rate of growth in the use of social networking services and user-generated content has recently increased markedly in

---

<sup>49</sup> Family Online Safety Institute (2007), 'About ICRA', available at: [www.fosi.org/icra/](http://www.fosi.org/icra/) accessed 31 October 2007

<sup>50</sup> **Sharing information, communications or images** is a form of cyber-bullying that involves publishing content that was intended to be private to a public space to embarrass or antagonise the victim.

<sup>51</sup> **Personal intimidation** is cyber-bullying that involves posting personally abusive and threatening comments on another user's website, profile, blog or email.

<sup>52</sup> **Impersonation** involves setting up fake web pages that are attributed to the victim of bullying to make manipulative or derogatory comments about other users. This may involve stealing passwords and using them to gain access to other users' websites to make comments about other users that are later attributed to the victim.

<sup>53</sup> **Exclusion** involves blocking a particular user, the victim, from a social group or deleting them from friendship lists to make the victim feel socially isolated.

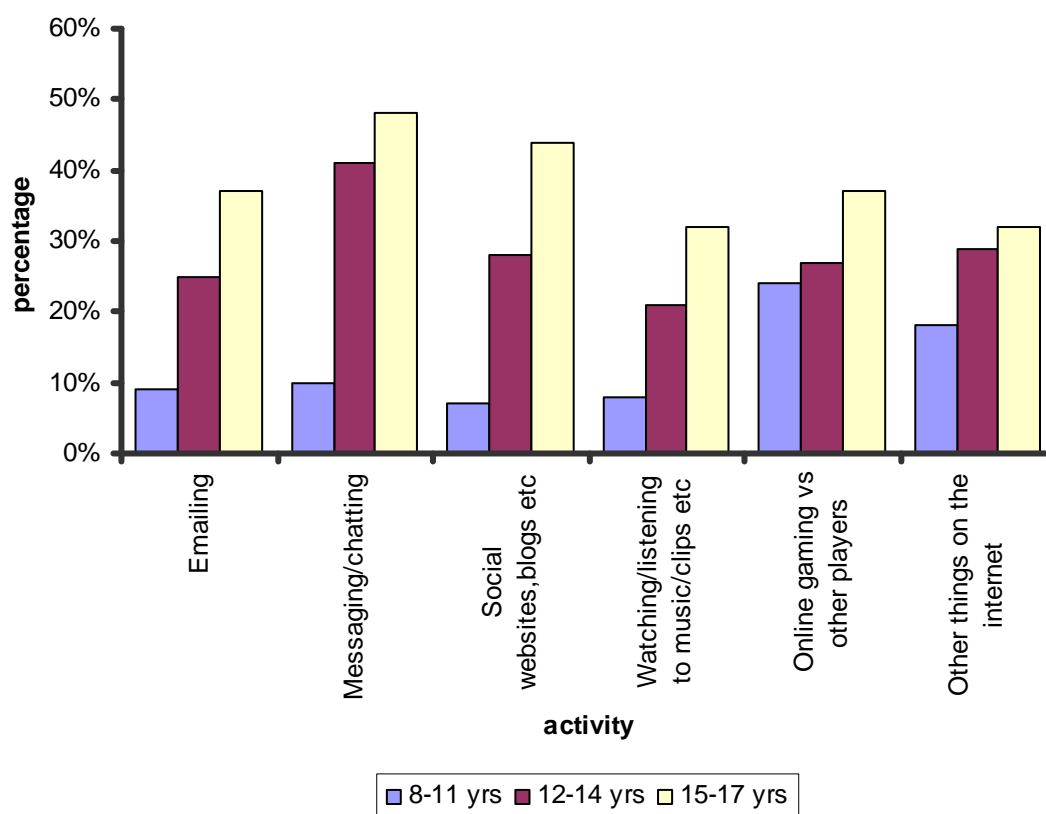
<sup>54</sup> **'Happy slapping'** involves posting images of bullying incidents online.

Australia and internationally. Analysts predict that, within a few years, 75 per cent of all broadband internet services will be used for user-generated content services<sup>55</sup>.

Of websites with a high proportion of the youth audience in Australia, 30 per cent focus on creating or editing user-generated content<sup>56</sup>. The most popular user-generated content sites in Australia include [myspace.com](http://myspace.com), [piczo.com](http://piczo.com), [clubpenguin.com](http://clubpenguin.com), [bebo.com](http://bebo.com), [facebook.com](http://facebook.com) and [blogger.com](http://blogger.com)<sup>57</sup>. Other internationally popular user-generated content sites are [youtube.com](http://youtube.com), [friendster.com](http://friendster.com), [orkut.com](http://orkut.com) and [linkedin.com](http://linkedin.com).

In 2007, ACMA undertook research into children's use of media in the home including use of televisions, mobile phones, games consoles, internet access and computers. The research found that children aged 8–17 years consume an average of two hours of television each day and spend an average of one and a quarter hours online each day<sup>58</sup>. Internet use increased as the age of children increased and the use of internet technologies such as IM, social networking sites and gaming online against other players peaked for children aged 15–17 years<sup>59</sup>.

**Figure 2.3: Use of internet technologies by age group, 2007**



Source: ACMA, *Media and Communications in Australian Families 2007*, December 2007

<sup>55</sup> Paul Budde Communication Pty Ltd (2007), *Australia – Digital Media – Video Comms, P2P, Instant messaging, Blogging, Social Network*, Paul Budde Communication Pty Ltd

<sup>56</sup> Nielsen//NetRatings (2007), *Australian eGeneration Report, Fifth Edition*, Nielsen//NetRatings

<sup>57</sup> Nielsen//NetRatings (2007), *Australian eGeneration Report, Fifth Edition*, Nielsen//NetRatings

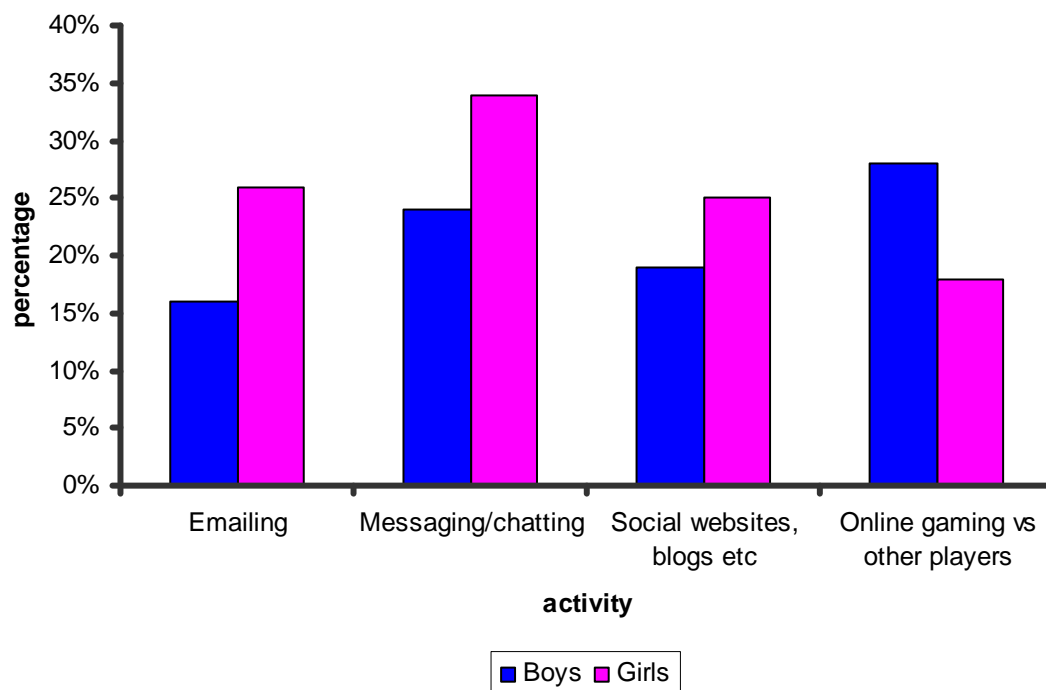
<sup>58</sup> Australian Communications and Media Authority (2007), *Media and Communications in Australian Families 2007*, ACMA, Canberra, pp. 2–8

<sup>59</sup> Australian Communications and Media Authority (2007), *Media and Communications in Australian Families 2007*, ACMA, Canberra, p. 81



In particular, the research revealed that while both boys and girls participated in a range of online activities, girls were more likely to spend a greater proportion of time communicating using IM and social networking sites, while boys were more likely to spend a greater proportion of time gaming online against other players<sup>60</sup>.

**Figure 2.4: Use of internet technologies by gender, 2007**



Source: ACMA, *Media and Communications in Australian Families 2007*, December 2007

ACMA's research also revealed that a significant minority of children (39 per cent) reported publishing their own material on the internet at the time of the study. This includes one or more of:

- a profile on a social networking site;
- their own website; and/or
- a stand-alone blog<sup>61</sup>.

The research also revealed that publishing material on the internet increased with age and young people aged 14–17 years were more likely to have their own material online—80 per cent of girls and 65 per cent of boys aged 14–17 years have some form of web authorship<sup>62</sup>.

In addition to these findings, research undertaken by Nielsen/Netratings found that use of email has decreased since 2005 from 71 per cent to 60 per cent. This decline in the use of email was attributed to an increase in the use of social networking services and, in particular, replacing email with communication through these websites<sup>63</sup>.

<sup>60</sup> Australian Communications and Media Authority (2007), *Media and Communications in Australian Families 2007*, ACMA, Canberra, p. 81

<sup>61</sup> Australian Communications and Media Authority (2007), *Media and Communications in Australian Families 2007*, ACMA, Canberra, p. 83

<sup>62</sup> Australian Communications and Media Authority (2007), *Media and Communications in Australian Families 2007*, ACMA, Canberra, p. 83

<sup>63</sup> Nielsen//NetRatings (2007), *Australian eGeneration Report, Fifth Edition*, Nielsen//NetRatings

## Chapter 3: Measures for promoting online safety

### Overview

The mid to late 1990s saw the emergence of measures by industry, government and internet users to mitigate online risks. These included educational initiatives, legislative actions and technological solutions, such as content filtering, content rating and labelling schemes, and security software. All are mechanisms that have endeavoured to keep pace with the evolving risks and challenges outlined in Chapter 2, including access to adult content, illegal contact, spam, viruses, online fraud, malware and identity theft.

Each of the measures considered in this chapter has different strengths and limitations, and may therefore be more useful when applied to some online risks rather than others. In this context, ACMA considers that online safety measures provide optimal outcomes when used in combination, as part of a strategic, coordinated, online safety framework.

Filters can be deployed at various locations in a network, including on computers connected to the internet, on separate devices located in a home network, in an enterprise network, in an ISP's facilities, in a third party's facilities, or in a search engine. They identify content to be blocked by two main techniques: reference to an index of addresses of internet content or by analysis of the content as it is retrieved from a remote host by the user. Once the content has been identified, there are several main techniques for preventing it from being accessed by users. The techniques used for identification and blocking of content can affect efficacy and performance.

The development of filters has been primarily driven by market demand in enterprises rather than by families, as well as developments in people's use of the internet and how online risks have manifested. Progress has been made in developing filtering solutions for static content. A recent study undertaken for the European Commission found that particular filter products available today perform well with commonly accessed English language websites that contain sexually explicit content, although over- or under-blocking occurred in about 25 per cent of test cases.

Filtering technologies are the subject of ongoing technical development to improve their ability to control the content and communications accessed by users. However, filters are yet to develop sufficiently to adequately address real time online communications, and concerns remain regarding performance impacts, particularly when the filter is deployed other than on a home computer, and circumvention methods. Nevertheless, filters can be quite effective when applied to achieve more narrowly defined goals, such as filtering previously identified potentially illegal content in ISPs' networks, or restricting access by young children to an approved 'whitelist' of safe web content.



Filters are most likely to affect network performance when large indexes are used and/or complex analysis of content is undertaken. While these performance impacts can be overcome, the cost of increasing capacity to neutralise impacts increases with the size of the network and computational requirements of the filter. Where a network filter is applied to a relatively small number of URLs, or a generous level of computational resources are dedicated to filtering—as is not uncommon for home computers—the impact on performance is likely to be minimal.

In addition to the practical concerns outlined above, content-filtering solutions have been controversial on philosophical and practical grounds. Content rating and labelling schemes complement filtering solutions by allowing labelling to be done either by content producers or by individuals and communities of interest. These schemes have been supported by the development of technical protocols. While going some way to addressing the philosophical concerns held by those critical of placing access control in the hands of government or industry, user-generated labelling and rating schemes have not been widely adopted to date.

Filtering solutions are often bundled with related protective measures for use on home computers. These are known as parental control software and provide monitoring tools, time management functions, application blocking and content filtering. Parental control software is also sometimes bundled with computer security software.

The most common methods of addressing risks associated with e-security have been software and hardware solutions that involve detection and blocking of spam, viruses and other malware, and attempts to gain unauthorised access to enterprise networks or home computers. These ‘active’ measures to guard against e-security risks are complemented by more ‘passive’ measures that take the form of behaviours among computer users aimed at reducing the likelihood of encountering these risks. These behaviours include securely managing passwords, being vigilant about unsolicited email, and keeping operating software up-to-date.

Other measures for mitigating online risks build on this notion of changing behaviour. Education and awareness initiatives have the capacity to address online safety issues, and to do so in a time frame that allows them to respond quickly to new risks associated with emerging internet technologies and services. If appropriate messages are suitably targeted and delivered, education initiatives have the capacity to not only raise awareness about online risks, but also to influence the way children behave online as a means of promoting their safety.

Most of the measures described here are supported by legal frameworks that make it unlawful to engage in behaviour that creates or facilitates certain online risks, notably child pornography, illegal contact and online fraud. A challenge for any legal framework that seeks to mitigate online risk arises from the global, cross-jurisdictional character of the internet. However, domestic legal action against unlawful behaviour originating overseas or international law enforcement action can be effective, particularly when the unlawful content against which legal action is taken involves a paid service. If there is a financial flow to a service provider as a result of unlawful or criminal activity online, it is increasingly likely that the flow can be blocked by law enforcement action. Alternatively, the threat to block the flow can be used to change the behaviour of the service provider in relation to the potentially illegal content. Changes in behaviour may also be brought about because an overseas service provider wishes to protect its reputation, either with regulators or its customers—some social networking sites have cooperated with national governments in removing potentially illegal material.

This chapter will examine measures that have been developed to address the online risks identified in Chapter 2. In particular, it will consider the applicability, strengths and limitations of:

- filtering technologies;
- content rating and labelling schemes;
- education programs;
- e-security technologies;
- monitoring of users' online activities; and
- legal frameworks, including the enforcement of the criminal law.

Examples of how these measures have been deployed in EU countries to address identified risks will be considered in Chapter 4.

## **Addressing online risks**

As discussed in Chapter 2, changes in internet technologies and their use over time have resulted in changes to the risks to families online. Likewise, as governments, industry, non-government organisations (NGOs) and families have become aware of and understand the changing risks, the measures deployed to protect families have changed and developed. This section will examine the different drivers that contribute to online safety measures, and the competing philosophies about the regulation of the internet to which they each adhere. It will also consider the way online safety measures have evolved over time to address changing risks to families.

Due to its origins and early developments in the US, particularly in institutions of higher learning, the internet was initially characterised as a space of free expression and information sharing. Before internet penetration into homes became common in the late 1990s, access was generally limited to adult staff and students of universities and employees of business enterprises. There was resistance by early users to the control of internet use. However, as families and children gained access to the internet in the home, it was recognised that, along with the many benefits of the internet, there were risks, particularly to children. This has fuelled the debate about regulating the internet as a medium.

In some cases, views on appropriate measures to address online risks have polarised. In 1996, the US *Communications Decency Act* prohibited, in effect, the transmission or publication online of 'obscene or indecent' content without appropriate restrictions to prevent access by children<sup>64</sup>. The legislation was intended, among other things, to protect children from material that was considered inappropriate for them to view. This legislation was subsequently challenged in the courts by civil liberties groups on the basis that it infringed constitutional protections for free speech<sup>65</sup>. The US Supreme Court upheld this view and ruled that the prohibitions relating to indecent material could not be enforced, in

---

<sup>64</sup> US Supreme Court (1997), 'Syllabus: *Reno, Attorney General of the United States, et al. v. American Civil Liberties Union et al.*,' available at [www.law.cornell.edu/supct/html/96-511.ZS.html](http://www.law.cornell.edu/supct/html/96-511.ZS.html), accessed 12 November 2007

<sup>65</sup> ACLU (2007), 'Internet Free Speech,' available at: [www.aclu.org/privacy/speech/index.html](http://www.aclu.org/privacy/speech/index.html), accessed 12 November 2007

part because less restrictive measures could be used to address the purpose of the legislation<sup>66</sup>.

In 2003, the Australia Institute<sup>67</sup> proposed mandatory ISP-filtering of internet access for all internet users to block access to content that would be classified as inappropriate for children. This proposal included an opt-out feature for adults, following age verification, to gain access to sexually explicit material<sup>68</sup>. This proposal was criticised by Electronic Frontiers Australia<sup>69</sup> who cited, among other reasons, that it would require the government to place responsibility for decisions about content with filter vendors<sup>70</sup>.

These and other debates led to a broad and diverse range of measures by governments, commercial interests and families to promote online safety. This chapter will discuss how these measures have developed, how they can be deployed to address online risks, and some of their strengths and limitations.

## Filtering technologies

This section will examine filtering technologies as a measure that may be used to address some of the online risks identified in Chapter 2. In particular, it will consider:

- factors that have driven the development of filters over time;
- how filters identify internet material that is not to be accessed by users;
- how filters prevent users from accessing identified material;
- where filters may be deployed in computer networks, and the implications of choosing to use one location rather than another; and
- the strengths and limitations of filters, including the means by which filters may be circumvented by users.

‘Internet content filtering’ refers to the use of computer hardware or software to screen content and control users’ access to that content. Most commonly, it is used to exclude from access content that is deemed to be objectionable or that falls into certain predetermined categories of content deemed to be inappropriate for a given user.

Filter technologies can include either or both of hardware and software elements to firstly identify content to be excluded and then block access to that content. They can be usefully

---

<sup>66</sup> Legal Information Institute (1997), ‘Syllabus: *Reno, Attorney General of the United States, et al. v. American Civil Liberties Union et al.*’, available at [www.law.cornell.edu/supct/html/96-511.ZS.html](http://www.law.cornell.edu/supct/html/96-511.ZS.html), accessed 12 November 2007

<sup>67</sup> The Australia Institute is a ‘public policy research centre funded by grants from philanthropic trusts, memberships and commissioned research’.  
The Australia Institute (2006), ‘About Us’ available at:  
[www.tai.org.au/index.php?option=com\\_content&task=view&id=25&Itemid=37](http://www.tai.org.au/index.php?option=com_content&task=view&id=25&Itemid=37), accessed 8 November 2007

<sup>68</sup> Flood, M., and Hamilton, C. (2003), *Regulating Youth Access to Pornography*, Discussion Paper Number 53, The Australia Institute, p. vi, available at: [www.tai.org.au/documents/dp\\_fulltext/DP53.pdf](http://www.tai.org.au/documents/dp_fulltext/DP53.pdf), accessed 8 November 2007

<sup>69</sup> Electronic Frontiers Australia is a ‘non-profit national organisation representing Internet users concerned with on-line freedoms and rights’.  
Electronic Frontiers Australia (2004), ‘About Us’ available at: [www.efa.org.au/AboutEFA/](http://www.efa.org.au/AboutEFA/), accessed 8 November 2007

<sup>70</sup> Electronic Frontiers Australia (2003), ‘Comments on Mandatory Filtering and Blocking by ISPs’, available at: [www.efa.org.au/Publish/ispblocking.html](http://www.efa.org.au/Publish/ispblocking.html), accessed 8 November 2007

deployed to address several of the risks identified in Chapter 2, particularly those related to inappropriate or illegal content. However, filters have a number of limitations that mean that they are unable to effectively address all online risks.

## **DEVELOPMENT OF FILTERING TECHNOLOGIES**

This section provides a historical overview of the development of filtering technologies. As outlined in Chapter 2, filtering technologies first emerged in the mid-1990s in response to concerns about children's access to internet material that their parents or carers felt was inappropriate for them to view.

In response to these concerns, technical solutions were developed as commercial filters that could be easily installed on home computers, enabling families to manage their children's access to internet content. The first content filters were reasonably rudimentary and were exclusively software for installation on personal computers that allowed parents or administrators to configure a list of websites they deemed unsuitable for access at home or work. The next generation of filters were able to perform rudimentary keyword analysis to block inappropriate web content, but not other kinds of internet services and materials.

As it became clear in the early 2000s that, alongside the many positive uses of the internet, paedophiles were using internet technologies to distribute child pornography, filters were deployed to block this and other illegal content, such as racist material. ISPs in several countries around the world have worked with governments, other industry participants and NGOs to develop lists of illegal content and to block internet users' access to that content.

Commercial filter vendors provide filtering technologies to various markets, including families, small, medium and large enterprises and ISPs. In particular, the enterprise sector is demanding filtering solutions to comply with privacy and other legislation, and to reduce the productivity and bandwidth losses associated with employees' personal use of the internet. Consumer demand for filter products for home use is growing, but remains a secondary driver<sup>71</sup> of the development of filters.

While filtering technologies have developed significantly in the past 10 years, the blocking of static web material containing sexually explicit content is still the function that filters perform most effectively. Filter vendors work to keep pace with emerging internet technologies and changing risk profiles—particularly the emergence of communication risks such as illegal sexual contact, online fraud and cyber-bullying—but it can take some time for vendors to develop effective solutions to emerging problems. At present, most filters deal with communication risks by completely blocking access, rather than filtering the content of applications that permit high levels of interactivity, such as social networking sites, IM and chat<sup>72</sup>.

---

<sup>71</sup> Frost & Sullivan (2006), *World Content Filtering Market*, #BAoD-74, Frost & Sullivan, London, pp. 2–4

<sup>72</sup> A 2006 study, commissioned by the European Commission, examined 30 filters available in Europe for families. Most of the studied filters offered blocking of chat or IM, rather than filtering, for example, Content Protect, Cyber Patrol, Norton Internet Security, Optenet Web Filter, Safe Eyes 2006 and Websense Enterprise. MacAfee Internet Security Suite and NetNanny did provide some filtering ability within chat or IM sessions, but their effectiveness was found to be limited.

Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, available at: [www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf](http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf)

## HOW FILTERING WORKS

This section describes techniques used to select content for exclusion, techniques for blocking access and the deployment of filters in different network locations.

### Identification techniques

Filter products perform two basic functions in order to limit users' access to content: they *identify* content that is to be excluded (or allowed); and then *block* (or allow) access to that material. Identification methods are common to most filter products, while blocking methods vary depending on the type of location where a filter is deployed, for example, a home computer, ISP server or mobile phone network.

There are two basic methods for identifying content to be filtered:

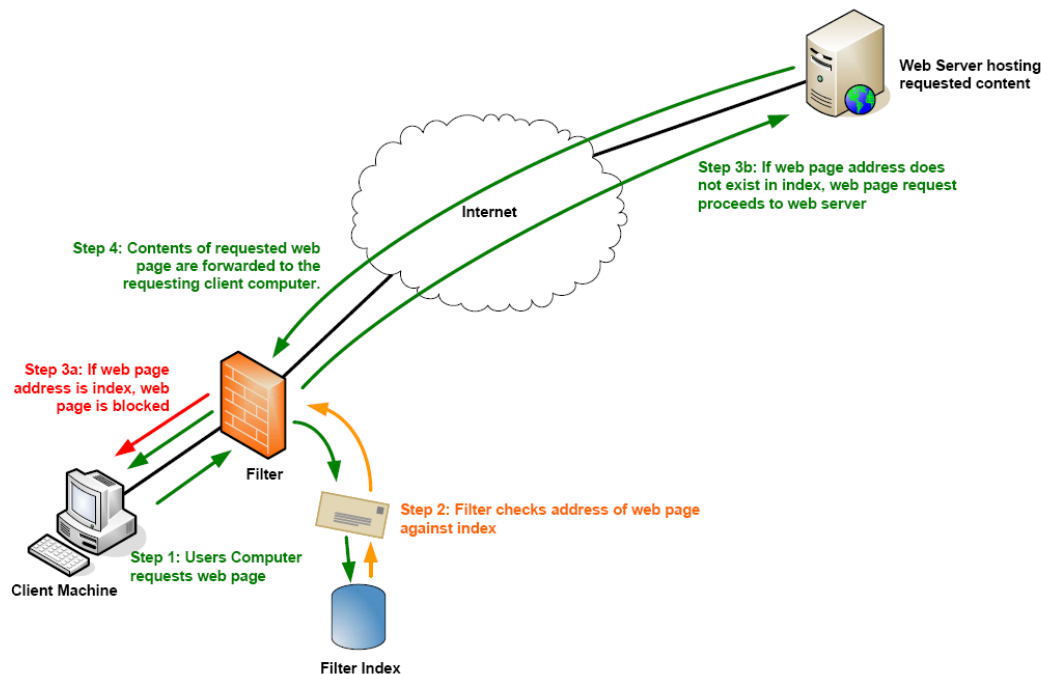
- *index filtering*—material is included in a list of either 'good' or 'bad' content; or
- *analysis filtering*—on an examination of the content, it is found to meet a set of criteria intended to determine its acceptability.

These identification techniques are discussed further below.

#### Index-based filtering

Index-based filtering is the process of permitting or blocking access to web pages on the basis of their inclusion on an index (or list) of web resources (see Figure 3.1). Such filtering can be based on a 'whitelist' or blacklist. Indexes may be developed manually, by human searches and analysis of content, or automatically, by analysis-based filtering, as discussed below.

**Figure 3.1: Index filtering process**



#### Whitelist indexes

Whitelist based index filtering permits access only to web resources that appear on a pre-approved list. Whitelists are usually used only as the basis of filter settings for young children, as they prevent access to the vast majority of internet content and applications.

## Blacklist indexes

Blacklist based index filtering permits access to all web resources, except those previously identified by the compiler of the blacklist as undesirable for a given user.

## Category indexes

Most commercial filter vendors classify content according to a wide range of subject categories that may correspond to types of content that parents (or employers, in the case of enterprise filters) wish to block, such as violence, sexual material, social networking sites, gambling or racist material. See an example of one vendor's category list below at Figure 3.2.

On the basis of these category lists filter administrators—which, in the case of filters used in the home, are generally parents—can choose which categories of content are appropriate or inappropriate for an individual user. Those web resources on the filter's index that are classified as falling into selected categories would, for the purposes of that user, constitute a whitelist or a blacklist of content to be allowed or blocked by the filter. In addition, some products allow categories to be blocked on the basis of additional criteria, such as the time of day or total browse-time duration.

**Figure 3.2: Category list from one filter vendor**

Custom Select your own set of categories to block.		
Commonly Blocked Categories		[ Block All ]   [ Unblock All ]
<input type="checkbox"/> <a href="#">Abortion</a>	<input type="checkbox"/> <a href="#">Intimate Apparel/Swimsuit</a>	<input type="checkbox"/> <a href="#">Proxy Avoidance</a>
<input type="checkbox"/> <a href="#">Adult/Mature Content</a>	<input type="checkbox"/> <a href="#">Nudity</a>	<input type="checkbox"/> <a href="#">Sex Education</a>
<input type="checkbox"/> <a href="#">Alternative Spirituality/Occult</a>	<input type="checkbox"/> <a href="#">Open Image/Media Search</a>	<input type="checkbox"/> <a href="#">Sexuality/Alternative Lifestyles</a>
<input type="checkbox"/> <a href="#">Gambling</a>	<input type="checkbox"/> <a href="#">Peer-to-Peer (P2P)</a>	<input type="checkbox"/> <a href="#">Social Networking</a>
<input type="checkbox"/> <a href="#">Hacking</a>	<input type="checkbox"/> <a href="#">Personals/Dating</a>	<input type="checkbox"/> <a href="#">Spyware Effects/Privacy Concerns</a>
<input type="checkbox"/> <a href="#">Illegal Drugs</a>	<input type="checkbox"/> <a href="#">Phishing</a>	<input type="checkbox"/> <a href="#">Spyware/Malware Sources</a>
<input type="checkbox"/> <a href="#">Illegal/Questionable</a>	<input type="checkbox"/> <a href="#">Pornography</a>	<input type="checkbox"/> <a href="#">Violence/Hate/Racism</a>
Other Categories		[ Block All ]   [ Unblock All ]
<input type="checkbox"/> <a href="#">Alcohol/Tobacco</a>	<input type="checkbox"/> <a href="#">Government/Legal</a>	<input type="checkbox"/> <a href="#">Remote Access Tools</a>
<input type="checkbox"/> <a href="#">Arts/Entertainment</a>	<input type="checkbox"/> <a href="#">Health</a>	<input type="checkbox"/> <a href="#">Restaurants/Dining/Food</a>
<input type="checkbox"/> <a href="#">Auctions</a>	<input type="checkbox"/> <a href="#">Humor/Jokes</a>	<input type="checkbox"/> <a href="#">Search Engines/Portals</a>
<input type="checkbox"/> <a href="#">Blogs/Newsgroups</a>	<input type="checkbox"/> <a href="#">Job Search/Careers</a>	<input type="checkbox"/> <a href="#">Shopping</a>
<input type="checkbox"/> <a href="#">Brokerage/Trading</a>	<input type="checkbox"/> <a href="#">Military</a>	<input type="checkbox"/> <a href="#">Society/Lifestyle</a>
<input type="checkbox"/> <a href="#">Business/Economy</a>	<input type="checkbox"/> <a href="#">News/Media</a>	<input type="checkbox"/> <a href="#">Software Downloads</a>
<input type="checkbox"/> <a href="#">Chat/Instant Messaging</a>	<input type="checkbox"/> <a href="#">Online Games</a>	<input type="checkbox"/> <a href="#">Sports/Recreation/Hobbies</a>
<input type="checkbox"/> <a href="#">Computers/Internet</a>	<input type="checkbox"/> <a href="#">Online Storage</a>	<input type="checkbox"/> <a href="#">Streaming Media/MP3</a>
<input type="checkbox"/> <a href="#">Cultural/Charitable Organizations</a>	<input type="checkbox"/> <a href="#">Pay to Surf</a>	<input type="checkbox"/> <a href="#">Travel</a>
<input type="checkbox"/> <a href="#">Education</a>	<input type="checkbox"/> <a href="#">Political/Activist Groups</a>	<input type="checkbox"/> <a href="#">Vehicles</a>
<input type="checkbox"/> <a href="#">Email</a>	<input type="checkbox"/> <a href="#">Real Estate</a>	<input type="checkbox"/> <a href="#">Weapons</a>
<input type="checkbox"/> <a href="#">Financial Services</a>	<input type="checkbox"/> <a href="#">Reference</a>	<input type="checkbox"/> <a href="#">Web Advertisements</a>
<input type="checkbox"/> <a href="#">For Kids</a>	<input type="checkbox"/> <a href="#">Religion</a>	<input type="checkbox"/> <a href="#">Web Hosting</a>



Depending on the vendor, the web resources on these lists can number in the hundreds of millions, with some vendors claiming to have assessed as much as 98 per cent of commonly accessed websites. Methods of list compilation vary between vendors, with some using advanced software analysis techniques to scan the web for inappropriate or illegal material, and others relying in all instances on human assessors. Given the dynamic nature of much internet content, lists must be constantly reviewed and updated. Each vendor's list compilation methodology is commercially sensitive information, but most vendors appear to use a combination of artificial intelligence (using techniques described in 'analysis-based filtering' below) and human assessment.

Filters designed for specific purposes may draw on a more limited index. For example, a blacklist may be comprised of material that is found to be illegal in a given jurisdiction, such as the list compiled by the UK's Internet Watch Foundation, which is used by ISPs to block access by UK users to child pornography.

Indexes of web content may be based on the **IP address**<sup>73</sup> or **URL**<sup>74</sup> of the identified material. The choice about which kind of address is used in an index may significantly affect the scope of material that is included in any blocking action. This is discussed in more detail in this chapter under *Blocking techniques*.

### **Analysis-based filtering**

Analysis-based filtering refers to the dynamic classification of content using computer software and has emerged in response to the shortcomings of index-based filtering—that is, that the latter is only applicable to web pages that have previously been assessed.

There are several different methods of analysis employed to undertake such filtering, including<sup>75</sup>:

- *Key word filtering* looks for words that might indicate that the site is of a problematic nature. Words may be located in the URL, title or text of a website, or in the text of a communication, such as an email or chat session. This may involve the classification as inappropriate of an entire site or communication that contains an identified word or it may involve complex analyses of word usage to determine whether the word is acceptable in its context. In its most rudimentary form, this filtering may only work in a single language, and it can lead to 'over-blocking'<sup>76</sup>. Over-blocking refers to the unintentional blocking of acceptable content as a result of the filtering techniques employed, and is discussed under *Limitations of filtering* in this chapter.
- *Profile filtering* attempts to categorise the requested content by comparing its characteristics (such as format, word usage or technical features) to other known problematic content. It is possible to analyse the content of a web page to assess the

<sup>73</sup> An internet protocol address (**IP address**) is essentially a network address. It is a unique identifier that electronic devices such as computers, routers and printers use to identify and communicate with each other on a computer network that uses the internet protocol. The internet is one such network.

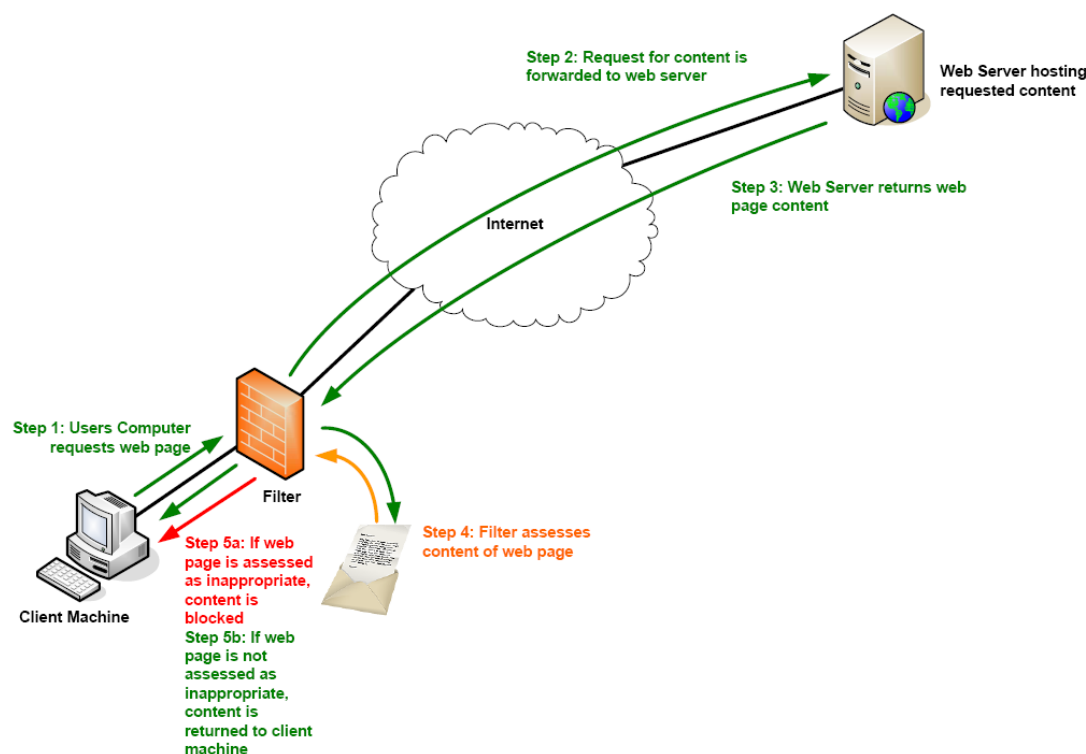
<sup>74</sup> A uniform resource locator (**URL**) is a string of characters used to identify or name a resource on the internet. It provides users seeking access to a resource (such as a website, or a picture or other element within a website) with a means to locate it.

<sup>75</sup> Ovum (2003), *Internet content filtering. A report to DCITA*, pp. 16–18, available at: [http://www.dbcde.gov.au/data/assets/file/10915/Ovum\\_Report\\_-\\_Internet\\_content\\_filtering.rtf](http://www.dbcde.gov.au/data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf), accessed 15 October 2007

<sup>76</sup> Over-blocking caused by rudimentary keyword analysis has, in the past, included the blocking of sites discussing breast cancer, and of the home pages of high profile people with the first name of 'Dick'. It is also widely presumed that 'Beaver College' in the US changed its name to stop the repeated blocking of its website by key word filters.

probability that it is a commercial sex site, for example, on the basis of the proportion of the page devoted to images or other characteristics. This is computationally intensive, and may therefore be more commonly used in offline analysis of resources for the purpose of list compilation than the real time analysis of material as it is requested by users.

**Figure 3.3: Analysis filtering process**



- *Image analysis filtering* involves the examination of images for large amounts of skin tone to determine whether the image contains nudity. This filtering is computationally intensive and is unable to make fine distinctions between acceptable and unacceptable kinds of nudity or near-nudity (consider, for example, an image of a child's swimming lesson). This technique is only applicable to identifying sexual content, rather than other kinds of content such as racist or violent content.
- *File type filtering* blocks certain file or media types, such as movie or photo files, usually on the basis of the file extension. It is commonly used by enterprises concerned about email attachments carrying malicious payloads, or using excessive bandwidth.
- *Link filtering* analyses the links included in a web page to try and determine the nature of the requested page. It works on the assumption that, if a web page links to another known to contain inappropriate content such as sexual content, it is likely to also contain inappropriate material. This method is likely to be of most use for filter vendors in identifying web pages that may warrant further scrutiny using other methods.
- *Reputation filtering* assesses the source of a communication on the basis of historical and current information about malicious behaviours and considers the likelihood that content coming from that source is harmful or inappropriate. This method is most commonly used in filtering email from spammers, but is increasingly being applied to web content to address e-security threats and online fraud.



Many filter manufacturers attempt to maximise the benefits and minimise the limitations of both index-based and analysis-based identification techniques by using both in their products. Index-based filtering is more commonly used as the primary means by which content is filtered, due to the speed with which such identification can be completed. Analysis-based filtering, being generally much more computationally intensive but able to immediately address new content, is more often used offline by filter vendors to develop indexes of inappropriate material. In some cases, analysis-based filtering is an optional feature that users can choose to activate or deactivate.

## Blocking techniques

Having identified content that is to be excluded from a user, a filter must then block access to that content. The blocking technique employed to prevent users from accessing content will depend to some extent on the identification technique used. For example, where index filtering is used to identify content to be blocked, requests for content are not delivered to the webserver hosting the content, whereas analysis filtering requires delivery of content in order to conduct analysis.

This section will examine the different techniques used to block access to content, including packet filtering, domain name server (DNS) tampering, caching web proxies and port blocking.

### Packet filtering

Packet filtering is a blocking technique available at the network level whereby a router or other device determines whether to allow or deny the passage of a request for content by examining the **headers**<sup>77</sup> of the **packets**<sup>78</sup> as they pass through. Packet filtering examines the destination IP address in the header and determines whether that IP address is to be blocked according to an index. Where an IP address is to be blocked, the router will not forward the request for data to the content host, and therefore no connection will be made with the host computer. This means that, not only will the web content at that IP address be blocked, but so will all other internet applications, including chat and email<sup>79</sup>.

Blocking on the basis of IP address is typically very fast and involves minimal performance impact, but can result in over-blocking of content that has not been assessed, and may be innocuous, if more than one website uses the same IP address. Where one of those sites is included in a blacklist, this method will prevent access to all of them. Further, it may be that only one page of a website contains inappropriate material but a result of blocking by IP address is that the entire site will be blocked.

### DNS tampering

DNS tampering involves changing the information that the **DNS server**<sup>80</sup> used by a particular user's computer returns after receiving a query regarding a blocked domain so that

---

<sup>77</sup> **Header** refers to the information contained at the beginning of a packet, which contains information about the handling of the packet. Analogous to an envelope around a letter, header information includes, among other things, the destination and source IP addresses.

<sup>78</sup> A **packet** is a formatted block of data that can be transmitted over a network. It includes both header information and the content to be delivered.

<sup>79</sup> Dornseif, M. (2003), 'Government Mandated Blocking of Foreign Web Content', in: von Knop, J., Haverkamp, W. and Jessen, E. (Editors), *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitsstagung über Kommunikationsnetze*, Düsseldorf, pp. 2–3, available at: <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>, accessed 10 October 2007

<sup>80</sup> The domain name system is the system that translates internet domain names such as 'acma.gov.au' into IP addresses. A **DNS server** is a server that performs this kind of translation. ISPs generally have DNS servers.

users attempting to request blocked websites will not be directed to the correct IP address. Like IP address blocking, this method can cause over-blocking because it affects all contents in the sub-domains under the blocked top level domain. In the case of some large domains, such as Geocities<sup>81</sup>, blocking one domain would result in the consequential blocking of millions of web pages that have not been assessed<sup>82</sup>.

### **Caching web proxies**

Proxies are often used in networks to acquire web content from a host computer on behalf of a user and deliver it to the user's web browser. Caching web proxies provide increased web browsing speeds and reduce bandwidth usage by holding copies of frequently requested material so that a request does not need to be made to the content host every time a user in the network wants to view the content<sup>83</sup>.

Caching web proxies can precisely block the content that is deemed to be inappropriate, usually on the basis of URL. They may also modify the communications between user and content host, usually to block requests for content hosted at a URL on a blacklist, but potentially making changes to returned content to filter out inappropriate sections<sup>84</sup>. However, this function requires significant computational power and has the potential to degrade network performance (discussed in *Performance impacts* in this chapter).

### **Port blocking**

Some filters block particular ports through which data is transferred. Different classes of programs or services on a computer use different ports to send and receive data. For example, some email programs use port 110, while web traffic is received through port 80 by default. By blocking the ports that various programs use to access the internet, filters aim to prevent use of those programs to access content on the internet.

### **Blocking modes for analysis filtering**

Where analysis filtering is used, requested information is retrieved, analysed and, where it is found to be inappropriate for the user, discarded rather than delivered to the user. There are two modes by which this analysis and blocking may be conducted:

- *Pass-by filtering* allows a requested page to load, and marks it for later analysis. The page will later be added to the vendor's index of classified material and therefore blocked, where appropriate, for users of the filter software. This means there is no delay to the user in accessing requested material, but that inappropriate content will be viewed by a user at least once.
- *Pass-through filtering* is often referred to as 'proxying'. Delivery of a requested website is not permitted until analysis of its content is complete, introducing a certain amount of

---

<sup>81</sup> Geocities is a web hosting service that enables users to create their own websites with the address format [www.geocities.com/mypage](http://www.geocities.com/mypage).

<sup>82</sup> Clayton, R. (2005), 'Failures in a Hybrid Content Blocking System' available at [www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf](http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf), accessed 8 August 2007

<sup>83</sup> Dornseif, M. (2003), 'Government Mandated Blocking of Foreign Web Content', in: von Knop, J., Haverkamp, W. and Jessen, E. (Editors), *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze*, Düsseldorf, p. 11, available at: <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>, accessed 10 October 2007

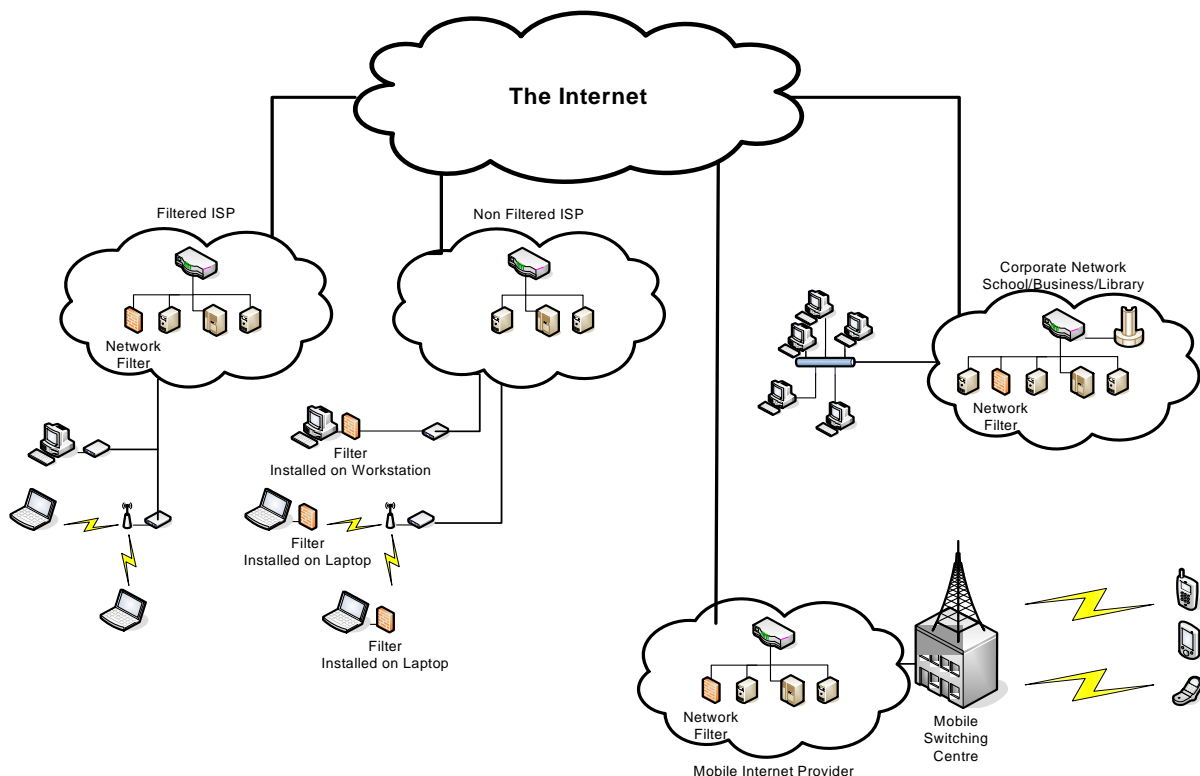
<sup>84</sup> Dornseif, M. (2003) 'Government Mandated Blocking of Foreign Web Content', in: von Knop, J., Haverkamp, W. and Jessen, E. (Editors), *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze*, Düsseldorf, pp. 13–14, available at: <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>, accessed 10 October 2007

delay<sup>85</sup> that depends on the processing power of the hardware on which the filter software is installed.

### Deployment of filters

There are several options for the deployment of filtering software or devices. Filter software may be installed on a device that is used to access the internet, such as a personal computer, or it may be deployed at a remote location, such as the network servers of an enterprise, an ISP, a mobile service provider or a third party. Likewise, hardware filters may be attached to a home computer, or be a component of an enterprise network environment. The decision about where to deploy filtering technologies will, to some extent, dictate the methods that may be used, their strengths and limitations, and the means by which they may be circumvented.

**Figure 3.4: Locations at which filters may be deployed**



Despite this, while the filter methods used by each filter vendor are commercially sensitive information that is usually closely held, it is apparent that increasingly, filter products deployed in different locations share many common features. Filter vendors often provide similar solutions for parental controls over home computers, employer administration of networked computers and ISP administrator management of subscribers' services. In many cases, filter vendors use the same filter software functions and indexes behind all of these filter products. In all cases, an administrator (or parent) can manage the internet experience of users. Products designed for enterprises and ISPs enable an administrator to control the web access of a larger number of users. In addition, ISP products may have additional administrator functions for individual customers.

<sup>85</sup> Ovum (2003), *Internet content filtering. A report to DCITA*, p. 17, available at: [http://www.dbcde.gov.au/\\_data/assets/file/10915/Ovum\\_Report\\_-\\_Internet\\_content\\_filtering.rtf](http://www.dbcde.gov.au/_data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf), accessed 15 October 2007

The following sections describe the implementation of filtering technologies at different network locations including home computers, mobile phones, ISP servers, within enterprises and search engines.

#### **Home computer and end-user filters**

Filters designed for home computers are installed directly on the home computer (or computers) and may be configured to provide differing levels of filtering for different users. Home computer filters are increasingly packaged along with other features as ‘parental control software’ (discussed under *Parental engagement* in this chapter) and computer security software (discussed under *Security software* in this chapter). However, the scope of home computer filters can vary, from a simple ‘add-on’ to a web browser that limits the websites to which a user may have access, to a comprehensive suite of parental controls, including blocking access to specific content and application, monitoring, reporting and time management functions.

Although hybrid models<sup>86</sup> of home computer filtering exist, most home filtering software operates almost exclusively on the home computer, with no remote computer involvement. Alternatively, some filter products involve a hardware element, as well as software.

Although more common in an enterprise environment, a possible new trend is to provide filtering software on a device that plugs into a home network of several computers and provides a filter between the home computer and the modem<sup>87</sup>.

#### **Mobile phone filters**

An emerging filter product is a filter for mobile devices (including mobile telephones), which are increasingly used to explore the internet and download music, games and videos. Mobile phones have limitations that make the deployment of filters on mobile devices challenging. These generally include a lack of:

- computational and battery power to run filtering software;
- storage capacity to hold indexes of content; and
- security controls to ensure that users cannot disable the filter.

Dedicated filter software for mobile devices is still under development. However, as mobile devices become more powerful and are released with more storage capacity, it is becoming more feasible to operate filters on them<sup>88</sup>.

ACMA is aware of several mobile filter products currently under development. Some of these systems perform filtering functions predominantly in the mobile network, while others operate largely on the handset. Some are hybrid models, splitting the processing functions between the network and the handset. These products are yet to be commercially offered to consumers in Australia, although they are used within internal enterprise networks of mobile carriers.

#### **ISP (including mobile ISP) filters**

Filtering solutions can be implemented at the ISP level, whereby filter software is installed on a server within the ISP’s network and the filtering occurs upstream of the user. Such

---

<sup>86</sup> Hybrid models include some functions on a remote device as described under **ISP (including mobile ISP) filters**, as well as software installed on the user’s computer.

<sup>87</sup> See, for example, D-Link Secure Spot, at [www.dlink.com/products/securespot/](http://www.dlink.com/products/securespot/).

<sup>88</sup> OECD (2007), *Mobile Commerce*, Directorate for Science, Technology and Industry, Committee on Consumer Policy, Organisation for Economic Co-operation and Development, available at: [www.oecd.org/dataoecd/22/52/38077227.pdf](http://www.oecd.org/dataoecd/22/52/38077227.pdf)

filtering may be considered more secure than home computer filtering because the user does not have physical access to the system on which the filtering occurs. However, depending on the filter product and the way the ISP chooses to deploy it—for example, whether ISP staff or users have direct access to filter controls—parents may have less decision-making control over the kinds of content that are blocked than they would with a parental control package installed on the home computer.

Historically, server level filtering has been considered only feasible using index filtering because internet servers were not capable of undertaking the additional computational load required for dynamic analysis of content for many concurrent users. However, as computing power within networks increases, some ISPs are beginning to deploy filtering solutions that include some analysis-based components. This is discussed under *Performance impacts* in this chapter.

Some mobile service providers in other countries that provide internet access to their customers have also deployed filter products at ISP level on their mobile platforms, filtering internet content before it reaches users' mobile phone handsets. This solution is generally marketed to parents as a service option for their children's accounts.

Depending on the filter solution deployed by the ISP, there may be a hybrid element to the filter that requires the installation of a small piece of software on the user's home computer in order to make use of the filter in the network.

### **Enterprise solutions**

Smaller enterprises, including small businesses, schools and libraries, may use either network solutions or software that is designed to be installed directly on the computers used to access the internet, while larger enterprises typically use network solutions. Software solutions installed on the user's device operate in a similar way to home computer filters, while network solutions are comparable to ISP filtering.

Enterprise network filter products may be applied to any network, including small to large businesses, schools, or libraries. Often deployed as a solution comprising both hardware and software, a filtering device is attached to the enterprise's network—typically on a server. Use of dedicated hardware in the filter product is intended to address the intensive computational requirements associated with complex filtering software.

Some filter vendors provide the same solution for enterprise and ISP customers. In its 2006 study of ISP-level filtering, RMIT Test Lab used enterprise filter products in the absence of the availability in the Australian market of offerings tailored specifically for ISPs<sup>89</sup>.

### **Third party filters**

Filtering and blocking can also occur on a server or router hosted by a third party. This solution requires the third party server to be in the path for either web requests initiated by a user, or delivery of content in response to a request. This routing of traffic can be achieved in various ways, such as by configuring the user's web browser, or the local ISP's network routing policies.

Third party filtering is sometimes used by enterprises to enable filtering of internet traffic for their employees, where those employees travel away from the office, and it may also be used

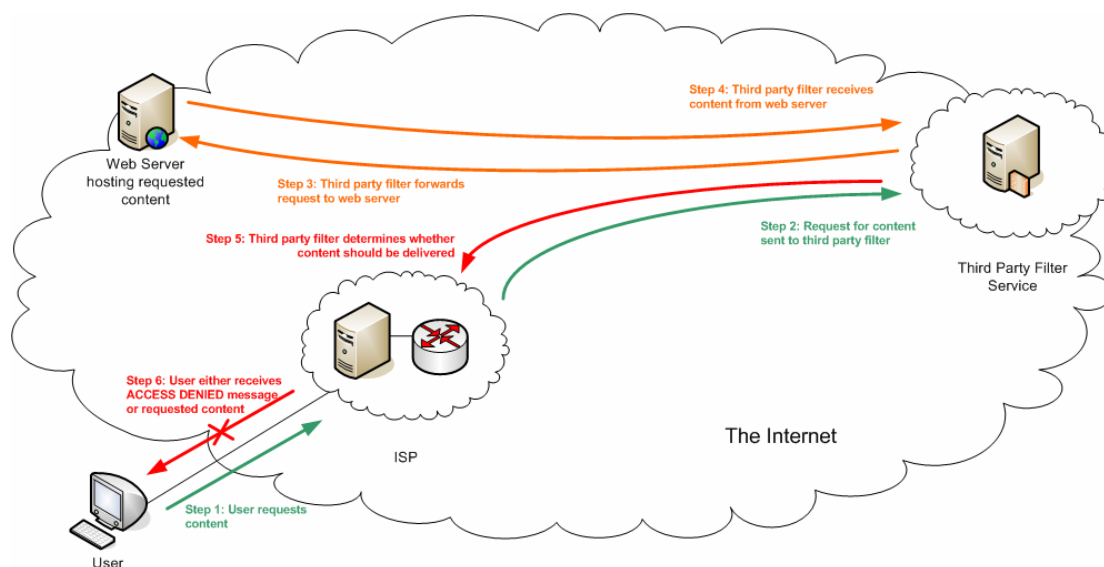
---

<sup>89</sup> RMIT Test Lab (2006), *A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience*, prepared for NetAlert, available at: [www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf](http://www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf), accessed 10 July 2007



by an ISP that wishes to outsource content filtering for its customers. While this solution has the benefit of potentially being available anywhere in the world, it is more commonplace for the third party's servers to be located in relatively close proximity to the customer to avoid degradation of performance.

**Figure 3.5: Third party filter process**



### Search engine filters

Most major search engines offer filtered search capabilities that enable customers to manage their own access to content. They are designed to remove content illegal in a given jurisdiction or content deemed to be inappropriate for children from search results, although search engine providers emphasise that no filter is 100 per cent effective<sup>90</sup>. Some search engines permit users to set filtering preferences within their main search site, with options of filtering only images and other media, or filtering all web search results<sup>91</sup>. Other search engines provide a separate search page designed specifically for children<sup>92</sup>.

Filter vendors often incorporate these safe searches into their products. Many parental control suites provide parents with the ability to mandate the use of safe searching, so that children cannot turn it off while the filter is operating.

## STRENGTHS AND LIMITATIONS OF FILTERS

Filters are capable of addressing several of the content risks outlined in Chapter 2. This section will discuss the strengths and limitations of filters in relation to performance impacts, accuracy and circumvention.

Filters can be effective in controlling users' access to inappropriate content. However, there are several limitations that are generally associated with the use of filters.

- *Performance impacts* – filters may slow access to the internet.
- *Inaccuracy* – filters may block innocuous content (over-block) or not block undesirable content (under-block).

<sup>90</sup> See Google's safe search at: [www.google.com/safesearch\\_help.html](http://www.google.com/safesearch_help.html)

<sup>91</sup> See Yahoo's safe search at: <http://au.search.yahoo.com/web/advanced>

<sup>92</sup> See MSN kidsafe search at: <http://encarta.msn.com/>

- *Circumvention* – a user may circumvent a filter in order to access the internet without restriction.
- *Interference* – filters may impede the operation other software such as security software.

#### **Children and internet content**

Filters may be particularly advantageous in controlling the internet access of very young children who lack the skills or understanding to make decisions about the kinds of content that may be appropriate for them. The use of whitelists that provides a completely safe internet experience for young children may be appropriate in such a context. Similarly, the use of filtering software to help protect older children from unintended exposure to undesirable material may be useful if these children are insufficiently mature or unequipped to make decisions about the content they should view.

A recent study commissioned by the European Commission considered the effectiveness of 30 filtering products designed for families, including those installed on a home computer, those installed in an ISP's network, and solutions that employed a mix of both methods. The study found that filter products currently available to parents perform well in filtering content from commonly accessed websites, containing sexually explicit material, and expressed in a common language, such as English<sup>93</sup>.

However, the products tested made a wrong filtering decision in more than 25 per cent of test cases, which resulted in over-blocking and under-blocking. This and other recent studies have also found that filters are generally more successful with blocking access to content hosted on popular (more frequently accessed) sites than those that are less frequently accessed<sup>94</sup>.

#### **Access to illegal content**

Filters can also be effective as part of a solution to address the problem of access to child pornography and ISP filtering is increasingly deployed to this end in countries such as Canada, Denmark and the UK. Examples of filtering solutions to address this problem are examined in Chapter 4.

However, it is worth noting that these measures are effective only after the fact and do not prevent the creation of illegal material nor, in the case of child pornography, the sexual exploitation of children. Neither do they remove illegal content from its location on the internet, nor prosecute the creators nor intentional consumers of this material.

Other measures may be deployed to complement filters in addressing the risks associated with illegal content. In particular, international efforts to enforce criminal laws prohibiting the distribution of child pornography, and the actions of internet content hotlines to receive reports of and issue take-down notices for illegal content hosted within their jurisdiction have been effective, as discussed in Chapter 4.

#### **Performance impacts**

A significant factor affecting the implementation, and sometimes the efficacy, of filtering solutions is the performance of the filtering solution as deployed in a particular location—

---

<sup>93</sup> Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, available at: [www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf](http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf)

<sup>94</sup> Brennan Center for Justice (2006), *Internet Filters: a Public Policy Report*, The Brennan Centre for Justice at NYU School of Law, Free Expression Policy Project, pp. 60–61, available at: [www.fepproject.org/policyreports/filters2.pdf](http://www.fepproject.org/policyreports/filters2.pdf), accessed 4 July 2007

home computer, ISP, mobile network or third party facility—and as configured to address a particular category of content—illegal content or user-selected category of content.

All filtering solutions consume processing resources on the computer or other hardware on which they are installed. The additional processing resources demanded by a filtering solution may have negligible impact on the network hardware, as long as the filtering/blocking task remains similar in magnitude and function to the task for which the hardware was designed. For example, where a router is designed to route packets to various destinations, the addition of a filtering solution that re-routes or terminates packets that are destined for (or sourced from) an address that is listed on a filter index may not impose significant additional load.

As a general rule, solutions that have been deployed in other countries to filter and block illegal content using index filtering cause no more than a small reduction in the performance of the network in which they are installed. This is because the magnitude of the task (blocking content associated with up to a few thousand URLs) does not significantly increase the demand on the processing resources of the hardware on which the solution is installed.

However, filtering and blocking solutions that must manage and process much larger indexes, or undertake complex analysis of content, or both, inevitably create a more significant drain on processing resources, and can cause a corresponding reduction in the performance of the hardware or the particular network.

This performance impact can nevertheless be relatively small for filtering and blocking solutions installed on personal computers, as the processing overhead for these solutions is generally comparable with other processing tasks on the computer and is relatively small in comparison with the overall processing power of the computer. As part of its ongoing work regarding online safety (discussed in Chapter 4), the European Commission's recently commissioned research regarding the effectiveness of filters in the home environment noted in relation to their testing of filtering and blocking solutions installed on personal computers, '[o]n recent systems, the performance impact was found [to be] negligible. On older systems, the resource requirement could have a more significant impact'<sup>95</sup>.

For ISPs that implement filtering and blocking solutions, the size of the task is closely related to the number of subscribers whose internet access is filtered. Without substantially augmenting the processing capability of its existing hardware, an appreciable reduction in network performance is inevitable. In a 2005 test of commercial filtering and blocking solutions available to ISPs, RMIT Test Lab found '[a] significant reduction in network performance when accessing the Internet through a content filter', with '[t]he level of performance degradation... [ranging] from 18% through to 78%'<sup>96</sup>.

Whether on a personal computer or ISP hardware, this performance impact can be minimised by upgrading or augmenting hardware to increase processing power. In the case of personal computers, the cost of upgrading processing power may be modest (although significant in

---

<sup>95</sup> Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, p 31, available at: [www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf](http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf)

<sup>96</sup> RMIT Test Lab (2006), *A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience*, prepared for NetAlert, p. 4, available at: [www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf](http://www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf), accessed 10 July 2007



terms of some household incomes). However, for ISPs, the cost of such upgrading or augmenting the expensive hardware that they typically deploy may be substantial, particularly for smaller providers.

#### **Over-blocking and under-blocking**

As discussed under *Blocking techniques* in this chapter, the technique used to block internet content can significantly impact the extent to which filters over-block. However, the sophistication of software that makes decisions about the appropriateness of material for a given user (analysis-based filtering), or the classification of material for inclusion in an index (index-based filtering), can also have consequences for the accuracy of filters.

If content decisions are solely made using computer software, they are limited to those relatively rudimentary distinctions that computers can make. While filter vendors focus on developing software that can assess the context in which content is situated to decide how content should be classified, this is not always sophisticated. Research has found that while analysis-based filtering can be effective in a textual and profile analysis of sexually explicit content, it is less effective with other categories of content that may also be prohibited or inappropriate for children<sup>97</sup>. Humans, in contrast, are able to make bring a more complex range of factors into consideration when assessing distinctions between inappropriate and appropriate content.

Given the limitations of artificial intelligence, analysis-based filtering involves a compromise between the twin goals of:

- a) thorough blocking of inappropriate content; and
- b) the minimisation of inadvertent blocking of innocuous content—over-blocking.

According to an academic in the field of statistics, who gave testimony in a court case in the US brought by the American Civil Liberties Union against legislation regulating access to internet content, filter testing has demonstrated that the filters that most effectively block inappropriate content also incorrectly block the highest levels of innocuous content. Conversely, filters with low levels of over-blocking tend not to be as effective in blocking inappropriate content<sup>98</sup>.

#### **Circumvention of filtering and/or blocking technologies**

The ease with which filters may be circumvented will depend on the technical knowledge of the user and possible methods of circumvention will vary according to the location in which the filter has been deployed. For example, methods for circumventing parental control software installed on a home computer may be different to those used to circumvent a filter located on an ISP server. The extent to which circumvention methods work in any filtered environment will depend on, among other factors, the nature of the filter deployed and the way in which it has been installed.

---

<sup>97</sup> Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, p 5, available at: [www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf](http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf)

<sup>98</sup> Stark, P.B. (2006), 'Expert report of Philip B. Stark, PhD, 8 May 2006' given in *ACLU v Gonzales* Civ. Action No. 98-5591 (E.D. Pa.), available at: <http://seth.com/infothought/blog/archives/copa-censorware-stark-report.pdf>, accessed 29 September 2007

Filter vendors are aware of all these methods of circumvention. As circumvention methods change or their application expands, filter vendors update their indexes or analysis techniques to mitigate attempts to circumvent their protections.

Some circumvention methods are specifically designed to circumvent filters installed on a user's computer, by gaining control of the computer and disabling or otherwise avoiding the filter software. For example:

- *Administrator passwords*—where filter software is installed on a computer, rather than a remote server, a user may circumvent the filter by gaining control of the filter software. This can be achieved by logging in as the administrator of the computer, instead of a user, which generally requires a user to know the username and password of the computer (and/or filter) administrator.
- *Boot disks*—where filter software is installed on a computer, rather than on a remote server, it may be possible to completely bypass the software with the use of a 'boot disk'. A user could boot the computer from a CD or removable storage device that contained an operating system and internet browsing software. The operating system and filter software installed on the computer's hard drive would not be loaded, and access to the internet would be unrestricted.

Some circumvention methods work on index-based, rather than analysis-based, filtering techniques, usually by hiding the source IP address or URL of the requested content. For example:

- *Anonymisers* are a form of proxy server that bypass index filtering techniques and serve as the content gateway for user requests. Users on a filtered network can configure their browsers to route web traffic through a proxy server to access any site, rather than accessing those sites directly. The filter software will see only the URL or IP address of the anonymiser not of the requested website and will therefore not act to block the content unless anonymisers are also blocked.
- *Translation software* sites are used to translate textual web content from one language to another. Typically, a user enters the URL of the website to be translated and the translation software presents the translated information within its own page. This function may be used in a similar way to anonymisers, to hide the source URL of a website from a filter, which only sees the URL of the translation site.
- *Search engine caching*—some search engines provide access to archived copies of websites, known as 'cached' versions. Like proxies and translators, some search engine providers permit access to cached content, and display it within their own pages. This may similarly hide the source of blocked material from an index filter.
- *Mirrors* are duplicate websites, commonly established to reduce the traffic load on servers hosting frequently accessed websites. A user seeking to access blocked content may access the mirror of a blocked site, which would circumvent index filters if the particular content on the mirror site is not listed on an index in addition to the primary site<sup>99</sup>.

---

<sup>99</sup> Dornseif, M. (2003), 'Government Mandated Blocking of Foreign Web Content', in: von Knop, J., Haverkamp, W. and Jessen, E. (Editors), *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze*, Düsseldorf, p. 14, available at: <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>, accessed 10 October 2007

- *Additional domain names*—content hosts may evade blocking by using multiple URLs pointing to the same IP address at which content is hosted. While this would not affect blocking techniques based on IP address, it would circumvent blocking based on URL or domain name if the alternative address for particular content is not listed on a filter index<sup>100</sup>.

## FUTURE OF FILTERING TECHNOLOGIES

Analysis filtering can address frequently changing content, such as the contents of news websites, but currently available filter products do not generally filter near real time content or interpersonal communications services and applications such as online gaming, IM and chat. Products that address these applications usually block access to them altogether, rather than filtering the material that is produced and consumed within them.

Where filtering of dynamic content is currently offered, it remains rudimentary. For example, the recent study of the effectiveness of filters designed for use by families commissioned by the European Commission found that at least one filter that attempted to remove profanities from IM communications could only remove a word once in each sentence—the first occurrence of the word would be removed, while subsequent occurrences would not<sup>101</sup>. Filter vendors are currently undertaking research and development to address dynamically generated content, and it is anticipated that more developed solutions will emerge in the next few years.

## Content rating and labelling

This section will examine content rating and labelling as a measure that may be used to address the range of online risks identified in Chapter 2. In particular, it will consider:

- how content rating and labelling schemes have developed;
- how labelling works; and
- the extent to which labelling has and may be deployed.

Content rating and labelling schemes aim to provide users with information about content in order for them to make informed choices about the materials they wish to view or interact with. The Australian National Classification Scheme<sup>102</sup>, includes a rating and labelling scheme to advise the Australian public about films, computer games and publications. When applied to the internet, labelling schemes are generally designed to work in conjunction with filtering software or web browsers. Content labels come in two forms: the labelling that content producers place on their own content; and the ratings of web content made by other individuals or communities of interest.

---

<sup>100</sup> Dornseif, M. (2003) 'Government Mandated Blocking of Foreign Web Content', in: von Knop, J., Haverkamp, W. and Jessen, E. (Editors) *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze*, Düsseldorf, p. 14, available at: <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>, accessed 10 October 2007

<sup>101</sup> Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, p. 24, available at: [www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf](http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf)

<sup>102</sup> See: <http://www.classification.gov.au>.

## DEVELOPMENT OF CONTENT LABELS

In response to concerns about children accessing inappropriate material on the internet in the mid 1990s, there were calls to restrict access to various kinds of web content, particularly adult content. However, some groups felt that intrusions into the internet experiences of private individuals were both inappropriate and unnecessary, and began to develop technical solutions to place access control in the hands of users, rather than a central authority such as an employer or government<sup>103</sup>.

The philosophy underlying labelling schemes was articulated by interested NGOs such as the Bertelsmann Foundation. The Bertelsmann Foundation considered that, rather than deploying a single filter, with a single set of value judgments about the desirability of particular web content, energy should be devoted to the development of 'a filter architecture designed to include various adaptable elements'<sup>104</sup>. For example, ICRA developed a content labelling scheme that was later adopted by the Family Online Safety Institute (FOSI)<sup>105</sup> in the US. This approach relies on 'both self-classification by content providers and active decision-making on the part of parents and guardians'<sup>106</sup>.

From 1995, interested industry participants and NGOs worked to develop standard labelling specifications through W3C, the key body responsible for developing standardisation in web technologies<sup>107</sup>. This led to the development of the Platform for Internet Content Selection, which enabled web developers to associate **metadata**<sup>108</sup> with their web content. That metadata could then be read by web browsers and filter software in order to filter the web content that is made available to users.

In the late 1990s, ICRA developed a labelling classification system to enable web content creators to label their own sites. The ICRA labels cover a range of subject topics that may be of concern to parents, including violence, sexual themes, nudity, profanity or the presence of user-generated content<sup>109</sup>.

FOSI and other interested parties continued to work through W3C, leading, in the early 2000s, to develop a standardised labelling system, the Resource Description Framework, which enhances the kinds of metadata that web content providers can apply to their content,

---

<sup>103</sup> Resnick, P. (1999), 'PICS, Censorship, & Intellectual Freedom FAQ,' available at: [www.w3.org/PICS/PICS-FAQ-980126.html](http://www.w3.org/PICS/PICS-FAQ-980126.html), accessed 8 November 2007

<sup>104</sup> Waltermann, J. and Machill, M. (Eds.), (2000) *Protecting our Children on the Internet: Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, Gutersloh, 2000, p. 14, available at: [www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst\\_engl/474.pdf](http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst_engl/474.pdf), accessed 7 November 2007

<sup>105</sup> FOSI, as the US successor organisation to ICRA, is an international, non-profit organisation that promotes self-regulation by internet content creators as a means to increase online safety.

<sup>106</sup> Waltermann, J. and Machill, M. (Eds.), (2000) *Protecting our Children on the Internet: Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, Gutersloh, 2000, p. 14, available at: [www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst\\_engl/474.pdf](http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst_engl/474.pdf), accessed 7 November 2007

<sup>107</sup> Waltermann, J. and Machill, M. (Eds.), (2000) *Protecting our Children on the Internet: Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, Gutersloh, 2000, p. 14, available at: [www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst\\_engl/474.pdf](http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst_engl/474.pdf), accessed 7 November 2007

<sup>108</sup> **Metadata** is information delivered with content, which is about the content being delivered. Metadata is available to the client application, e.g. the web browser reading html, and forms part of web page code, but is not displayed to the user.

<sup>109</sup> Family Online Safety Institute (FOSI) (2007), 'About ICRA,' available at: [www.fosi.org/icra/](http://www.fosi.org/icra/), accessed 29 October 2007

including applications from library catalogues, syndication services and personal collections of content and events<sup>110</sup>.

This work is ongoing<sup>111</sup>. One emerging development is the Protocol for Web Description Resources, which is intended to allow retrieval of content descriptions without retrieval of the content they describe<sup>112</sup>. This could significantly increase the ability of third parties to rate or label the web content of others.

Despite the development of standardised labelling and rating specifications, there is not yet widespread or standard use of labelling and rating schemes in Australia as a means to promote online safety, except as incorporated into commercial filter software.

## **LABELLING BY CONTENT PROVIDERS**

Website developers can label the content on their sites according to agreed assessment criteria and can include these labels in the metadata on their sites. However, there is no requirement to participate in rating schemes, and often little incentive for content producers to label their sites. Consequently, the use of content labels is not widespread.

Parents and other internet users can use filtering software or web browsers to filter content according to the ICRA labels on each site. Filter vendors commonly use ICRA labels as another method for assessing content in their filtering products and FOSI offers an *ICRAPlus* filter that performs this function<sup>113</sup>.

The *ICRAPlus* filter, which is available to be downloaded onto home computers free of charge:

- reads ICRA labels;
- allows the installation of additional modules that use other technologies to filter web content, including commercial filters; and
- supports additional sets of filtering rules or block/allow lists provided by third parties<sup>114</sup>.

FOSI also provides an 'ICRAchecked' service, which, for a fee, confirms the labels provided by content producers to provide assurance about the trustworthiness of the label<sup>115</sup>.

The Association of Sites Advocating Child Protection has similarly developed a 'Restricted to Adults' label<sup>116</sup> for use by the providers of adult internet content. ACMA understands that, unlike producers of content that has a less specific audience, many providers of legal sexual content online use this labelling in a deliberate effort to minimise access to their content by persons who are not adults.

---

<sup>110</sup> Herman, I. (2004), 'Resource Description Framework (RDF),' available at: [www.w3.org/RDF/](http://www.w3.org/RDF/), accessed 8 November 2007

<sup>111</sup> W3C (2005), 'W3C Content Labels,' available at: [www.w3.org/2005/Incubator/wcl/XGR-report/](http://www.w3.org/2005/Incubator/wcl/XGR-report/), accessed 29 October 2007

<sup>112</sup> Herman, I. (2007), 'Semantic Web Activity Statement,' available at: [www.w3.org/2001/sw/Activity](http://www.w3.org/2001/sw/Activity), accessed 8 November 2007

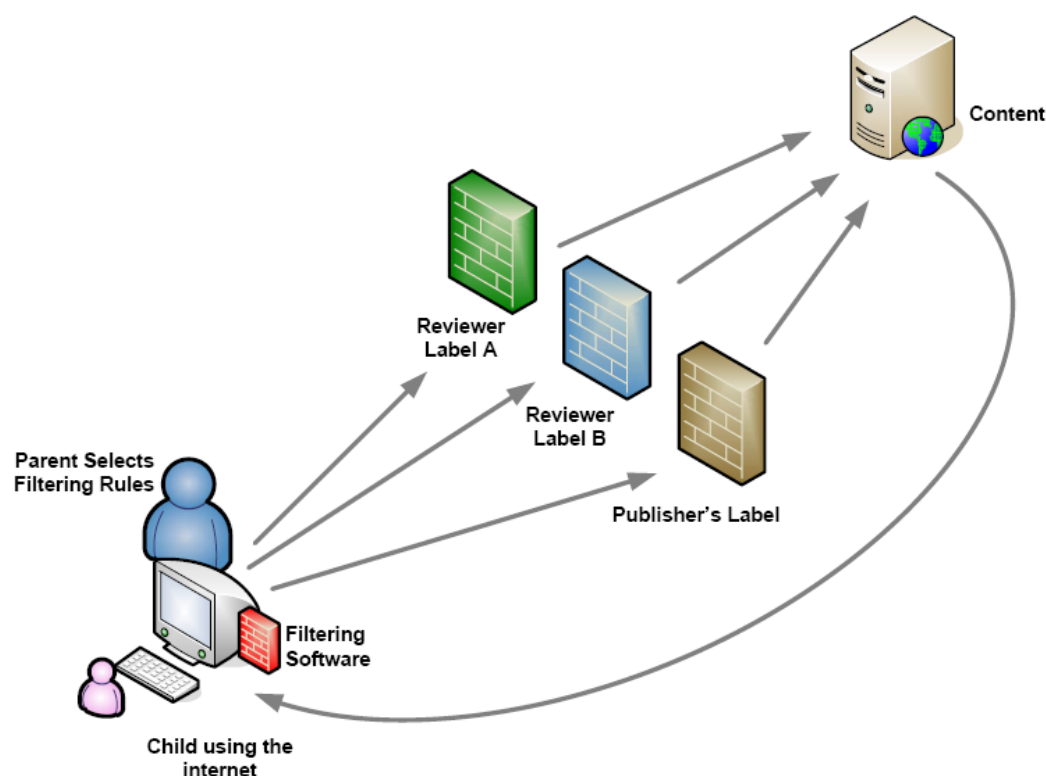
<sup>113</sup> Family Online Safety Institute (2007), 'About ICRA,' available at: [www.fosi.org/icra/](http://www.fosi.org/icra/), accessed 29 October 2007

<sup>114</sup> Family Online Safety Institute (2007), 'ICRAPlus,' available at: [www.icra.org/icraplus/](http://www.icra.org/icraplus/), accessed 12 November 2007

<sup>115</sup> Family Online Safety Institute (2007), 'ICRAchecked,' available at: <http://checked.icra.org/>, accessed 12 November 2007

<sup>116</sup> See [www.asacp.org/page.php?content=RTA](http://www.asacp.org/page.php?content=RTA) for more information about content labelling for adult websites.

Figure 3.6: Content rating and labelling<sup>117</sup>



## RATING BY CONTENT CONSUMERS

The Bertelsmann Foundation advocated users classifying internet content for their own and other's use. They suggested, for example, that socially relevant groups, such as churches or trade unions could provide labels for content to inform the internet use among people with shared values<sup>118</sup>. In this way, parents and guardians could select appropriate labelling schemes to filter content for their children, according to their own beliefs and ethics.

This approach has not emerged as a strong trend in internet usage. Although programs like [Glubble](http://www.glubble.com/)<sup>119</sup>, an add-on to the Firefox web browser, do permit parents to build and share blacklists and whitelists to be used to filter internet content for their children, use of rating schemes for web content is not common.

However, FOSI remains supportive of a move toward user ratings. Over the past couple of years, an increasingly popular online tool is tagging or rating systems. Services such as [del.icio.us](http://del.icio.us/)<sup>120</sup>, a 'social bookmarking' application, allow users to tag web content using labels

<sup>117</sup> Figure 3.5 is based on a diagram in the article: Resnick, P. (1999), 'PICS, Censorship, & Intellectual Freedom FAQ,' available at: [www.w3.org/PICS/PICS-FAQ-980126.html](http://www.w3.org/PICS/PICS-FAQ-980126.html), accessed 8 November 2007

<sup>118</sup> Waltermann, J. and Machill, M. (Eds.), (2000) *Protecting our Children on the Internet: Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, Gutersloh, p. 14, available at: [www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst\\_engl/474.pdf](http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst_engl/474.pdf), accessed 7 November 2007

<sup>119</sup> See: <http://www.glubble.com/index.php>.

<sup>120</sup> See: <http://del.icio.us/>



that have meaning for them, and to share their lists of tagged content with other users. FOSI sees this as evidence that rating systems designed to promote online safety are feasible<sup>121</sup>.

In a similar way, community ratings on social networking sites such as YouTube allow users to identify inappropriate content, so that where content breaches the site's terms of use the site providers can remove it. In this way, the community of users acts to ensure that the content hosted on the site meets agreed standards, and users can then choose whether to access a site on the basis of its terms of use or community guidelines<sup>122</sup>.

## Computer security software

This section will examine computer security technologies as a measure that may be used to address the range of online risks identified in Chapter 2. In particular, it will consider:

- factors that have driven the development of security software over time; and
- factors that affect the usefulness of security software.

Security software is designed to address many of the e-security risks outlined in Chapter 2, such as online fraud, malware and identity theft. Computer security software emerged in the late 1990s to address increasing risks associated with online viruses. The development of security software was driven by large businesses seeking to limit productivity loss associated with increasing levels of spam email.

As other e-security risks have emerged, software has been developed to address these concerns. Therefore, as e-security risks evolved to target data rather than productivity, security software increasingly focused on protecting businesses from data loss. A secondary driver is the rising use of online transactions by consumers, increasing their focus on installing appropriate security software on home computers<sup>123</sup>.

Security software includes:

- *Antivirus software*, which detects and removes viruses from the computer on which it is installed. Antivirus software products may now be installed directly onto home computers, may be run remotely via a vendor's web service, or may be used in both locations simultaneously. Further, most recent antivirus software addresses not only viruses, but worms, Trojans and other forms of malware<sup>124</sup>.
- *Firewalls*, which are used to prevent computers connected to the internet from receiving or sending data to other computers on the internet, based on a set of security policies. Firewall policies allow or deny connections based on the source, the destination, the protocol in use, or in some cases the contents of the communication (in much the same way as a content filter). They are commonly deployed to prevent hacking of corporate networks or to prevent malicious attacks on particular computers.
- *Spam filters*, which use content filtering, sometimes including sophisticated analysis filtering to determine whether a given email has the characteristics of a spam email, and discard emails that are most likely to be spam.

---

<sup>121</sup> Family Online Safety Institute (2007), 'Everyone has an opinion on the web,' available at: [www.fosi.org/archive/everyonehasanopinion/](http://www.fosi.org/archive/everyonehasanopinion/), accessed 7 November 2007

<sup>122</sup> YouTube (2007), 'YouTube Community Guidelines,' available at: [http://uk.youtube.com/t/community\\_guidelines](http://uk.youtube.com/t/community_guidelines), accessed 28 November 2007

<sup>123</sup> Frost & Sullivan (2007), *Asia Pacific Secure Content Management Market 2005*, Frost & Sullivan, London

<sup>124</sup> Howstuffworks Inc (2007), 'Antivirus Software Buying Guide,' *How Stuff Works* website, available at <http://products.howstuffworks.com/antivirus-software-buying-guide.htm>, accessed 23 October 2007

The extent to which security software is effective in preventing e-security threats depends, to some extent, on the responsiveness of the software vendor in quickly providing updates to address new threats and the other security measures taken by the user of the computer, such as:

- keeping software patched with the latest security updates;
- deleting suspect emails that are not removed by a spam filter, and not following links in, or opening attachments to, emails from an unknown source;
- avoiding files and applications on suspect websites;
- using long passwords that are difficult to predict for any application that provides access to personal information; and
- using a limited permission account for browsing the web<sup>125</sup>.

Security software is generally developed in response to identified e-security risks. Although the lag between the identification of e-security threats and software updates is relatively short—a matter of days or even hours—this unprotected period following the emergence of new threats, coupled with the increasing difficulty for users in identifying issues that may result in a security breach, mean that more robust approaches to mitigating e-security risks generally involve a combination of measures.

## **Parental engagement**

This section will examine parental engagements in children's internet experiences as a measure that may be used to address the range of online risks identified in Chapter 2. In particular, it will consider:

- how expectations of parental engagement have changed over time; and
- how software may be used to augment physical monitoring.

As identified in Chapter 2, the risks to young people online have changed as technologies have developed. Where parents were concerned about young people's access to inappropriate content in the early 1990s, parents are now also concerned by the risks presented by increasing interactivity and use of the internet to communicate with other users.

To be aware of risks to children online and how to combat them, parents need to be aware of how their children are engaging with and using internet technologies. Parents and carers must balance these risks with their own views about the benefits of internet access in order to determine the most appropriate approach for managing material available to their children on the internet.

## **ACTIVE ENGAGEMENT**

Key actions parents can take to engage with their children's online activities include:

- *Talking with children* about their online experiences, particularly when they feel uncomfortable about content they have encountered or if they are worried about their communications with strangers or friends online;

---

<sup>125</sup> For more information on keeping computers safe, see the ACMA website at:  
[www.acma.gov.au/WEB/STANDARD/pc=PC\\_310085](http://www.acma.gov.au/WEB/STANDARD/pc=PC_310085)



- *Being physically present* while children access the internet in order to actively monitor their level of comfort with the content or communications with which they are engaging;
- *Using monitoring software* to supplement physical monitoring if there is any reason for concern;
- *Becoming informed about online risks* and how to address them, and implementing strategies that are most appropriate to the particular family environment; and
- *Educating children* about how to use the internet safely.

## PARENTAL CONTROL SOFTWARE

More comprehensive filter software products designed to be deployed on home computers are generally referred to as ‘parental control software’. Although these products vary greatly in their approach and scope, they typically offer not only content filtering, but also monitoring tools, time management functions and application blocking, discussed below. Parental control software may also be packaged with security software to provide an integrated approach to home computer protection.

### **Monitoring**

Monitoring tools in parental control software provide parents with an overview of their children’s online activity. Product offerings vary, but can include the ability to log users’ keystrokes, record IM conversations or take screen shots of users’ activity. Monitoring reports generally list website visits and users’ attempts to access blocked material, and may include time spent online, programs accessed and the publication of personal information.

An emerging trend in monitoring software is the inclusion of remote monitoring tools, such as the ability for parents to receive an email or mobile phone text message when a child attempts to access blocked material. Some products enable parents to extend their children’s permissions remotely, for example, to allow access to an inappropriately blocked site.

While monitoring software assists parents in understanding how their children use internet technologies, most software is unable to alert parents to risks in real time.

### **Application management**

Some parental control suites are designed to not only limit access to content on the internet, but also software applications used to access specific services, such as email, IM and peer-to-peer (P2P)<sup>126</sup> programs. In addition, some packages will allow parents to limit access to software on the computer, such as accounting or other programs of no interest to children, or games that are considered inappropriate for a younger user. In some cases, these controls can be configured to permit access to particular programs only at specified times.

Application blocking is a method commonly used in parental control software to address communication risks associated with IM and chat. An emerging feature is the ability to permit use of email or IM programs, but limit communication to a pre-approved contact list.

### **Time management**

Many parental control suites allow parents to specify time limits for internet activity, by either a limit on the number of hours allowed online each day or week, or permitting access

---

<sup>126</sup> P2P is a computer communications model in which ‘peer’ computer systems are connected to each other via the internet. Primarily used to share files, P2P systems enable file sharing directly between computers on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as an end user.

only according to a timetable. Some packages apply these time limits to all computer activity. An emerging trend in functionality is the ability for parents to permit extensions of time remotely.

## **Education and awareness**

This section will examine education and awareness programs as a measure that may be used to address the range of online risks identified in Chapter 2. In particular, it will consider:

- what education programs can achieve;
- the appropriate targets of education programs; and
- challenges for the design and implementation of education programs in the future.

As technical solutions such as filters do not address the full range of online risks, other measures such as education programs are required to create an integrated and comprehensive approach to online safety. In addition, although filters are an effective means of addressing content risks, they are generally subject to a number of limitations, discussed above.

Therefore education is a necessary adjunct to filtering to teach children how to deal with the inappropriate content they may encounter.

## **EVOLUTION OF ONLINE SAFETY EDUCATION**

Online safety education emerged in the mid 1990s amid concerns about children's access to adult content on the internet. Education was seen as an alternative, or a supplement, to concurrent initiatives to deploy filtering technologies. Those people and groups who were less comfortable with regulating or restricting access to content on the internet were particularly supportive of education and awareness activities.

As concerns increased in the early part of this decade regarding communication risks such as illegal sexual contact, online fraud and cyber-bullying, education rose in prominence as a ready solution to mitigating this new risk. Given that there is commonly a lag between the identification of online risks and the development and deployment of technological solutions, education is sometimes viewed as particularly helpful to address emerging risks.

## **FUNCTIONS OF INTERNET SAFETY EDUCATION**

Internet safety education initiatives can perform one or more of three distinct functions:

1. *Raise awareness of online safety issues*—this can involve informing parents about the range of risks online for families, including content, communications and e-security risks, particularly where they do not adequately understand the technologies involved. Raising awareness is also relevant for children, who tend to underestimate online risks<sup>127</sup> and educators, who can introduce internet safety messages to their students.
2. *Provide information, advice and support*—this includes activities that inform people about measures that can be taken to mitigate online risk such as the use of filters, where to find advice, and how to access support. These activities empower users to identify and implement protective measures and deal with issues as they arise.

---

<sup>127</sup> European Commission, Directorate-General Information Society and Media (2007) *Safer Internet for Children: Qualitative Study in 29 European Countries*, p 8, available at: [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm#overall\\_report](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm#overall_report) accessed 13 September 2007.

3. *Develop and embed skills and protective behaviours*—this includes empowering users to engage with the internet responsibly to minimise the potential impact of content, communications and e-security risks. Research suggests that while children might be well versed in internet safety messages they do not always practise them<sup>128</sup>. While all users are susceptible to online risks to some degree, children are particularly vulnerable to communications risks because their technological capability is generally not matched by maturity or the ability to understand the consequences of their actions<sup>129</sup>. In conducting education programs, online safety educators generally seek to embed skills and protective behaviours in users.

## TARGETS OF INTERNET SAFETY EDUCATION

Online safety education may be targeted at one or more identified groups in order to address online risks identified in Chapter 2. These different groups have different learning characteristics and needs.

### Children

Children construct knowledge on internet safety using a combination of informal advice and expert guidance. Parents and older siblings or peers may be a preferred source of advice for children, while schools are a suitable place for formal learning about online safety issues. The internet itself is a channel for information as are mass media campaigns—those on television are particularly well received. In addition, some children like to exchange experiences and share solutions online<sup>130</sup>.

#### *Developing strategies to embed protective behaviours*

To be most effective, it is beneficial for knowledge about online safety to translate into practical skills and to be applied as behaviours. Educational strategies that provide problem-solving of realistic online safety issues present children with opportunities for exploring potential online dangers and practising protective behaviours. Both scenario-based learning and case studies can be used to instruct in online safety issues, and can demonstrate to children how to work through a problem using appropriate online safety strategies.

Children use internet technologies and engage with each other, generating their own online cultures. Programs that embed responsible internet usage by children can draw on understandings of these cultures to deliver messages to children using the services that they use. In this way, online safety educators can deliver safety messages in children's own vernacular and encourage peers to communicate openly about appropriate online behaviour. This approach may have more credibility with teenagers than off-line approaches.

### Schools

Internet safety education programs may be introduced to school students on an ad hoc basis or as an embedded part of the education curriculum. Age-appropriate learning activities may

---

<sup>128</sup> European Commission, Directorate-General Information Society and Media (2007) *Safer Internet for Children: Qualitative Study in 29 European Countries*, p 9, available at: [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm#overall\\_report](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm#overall_report) accessed 13 September 2007.

<sup>129</sup> CEOP (2007) *Strategic Overview: Making every child matter...everywhere*, p 13, available at: <http://www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf>, accessed 9 October 2007.

<sup>130</sup> European Commission Directorate – General Information Society and Media (2007), *Safer Internet for Children: Qualitative study for 29 Countries*, p. 59, available at: [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm#overall\\_report](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm#overall_report), accessed 13 September 2007

demonstrate to young children and older students the advantages of the internet while training them to be wary of internet safety concerns. The provision of professional development support, in addition to lesson preparation materials for teachers, can encourage the introduction of internet safety programs into schools.

School-based internet education programs can also involve participation of expert speakers (such as police or specialist internet trainers), who can address students, teachers and parents on online safety issues.

## **Adults**

Public education programs can raise awareness of internet safety issues, offer advice on where to get help in the event of trouble, and provide tools for adults to implement internet safety in the home. The majority of these campaigns are centred on educating parents and carers on how to help their children stay safe while online, and are complemented by matched age-appropriate materials for young people.

Education campaigns targeted at parents are commonly designed to meet two primary objectives:

- informing parents/carers who are proactively seeking information to assist their child to use the internet safely—resources falling into this category may include guidelines, technology solutions and advice on engaging with children over their internet activity; and
- assisting parents/carers who are motivated by immediate concerns in relation to their child's safety—information provided for these parents ranges from print information to contact numbers for help lines and law enforcement agencies.

Campaigns may also target adults to raise awareness about general online safety issues such as online fraud, harassment and e-security.

## **Industry participants**

Industry-focused education campaigns are designed to enhance awareness of concerns in relation to internet safety among organisations such as ISPs, web hosting providers, content providers and phone companies. Such campaigns may take the form of advisory groups and conferences, and often promote a collaborative approach with involvement from government, law enforcement and education sectors. These programs can be used to inform a range of measures in internet safety such as information for users on technological solutions (password protection, parental permissions), end-user guidelines (age restrictions, 'netiquette') and sanctions (barring of offenders, reporting abuse).

## **FUTURE DIRECTIONS FOR ONLINE SAFETY EDUCATION**

As new technologies are developed and the internet environment becomes increasingly integrated into users' lifestyles, online safety education initiatives will need to evolve in order to remain effective. While it is not possible to be specific on the direction technological developments will take, recent trends in internet education suggest that the following will remain important to the effective delivery of online safety messages:

- ensuring education campaigns complement other measures aimed at mitigating online risks;
- ensuring that messages reflect technological developments and their use—for example, to reflect the increasing use of interactive and social networking sites; and

- extending online safety education campaigns to new audiences such as very young children and the elderly, as they become more active in the online environment.

## Legal frameworks

This section will examine legislation and other legal frameworks as a measure that may be used to address the range of online risks identified in Chapter 2. In particular, it will consider:

- the development of internet-specific legislation;
- the application of existing legislation to online safety issues; and
- the enforcement of the criminal law.

A variety of laws exist in most countries relating to risks associated with the use of the internet. Laws vary significantly by country, and cover a range of activities. In many cases, laws relating to offline activities have been amended or extended to cover online activities including fraud, harassment and the publication, distribution or consumption of illegal content, with particular emphasis on child pornography. However, the legal framework has evolved to accommodate technological developments and the changing ways users engage with the online environment.

While early responses to illegal online activity were made using existing legal frameworks, recognition that the internet presented specific risks or allowed specific solutions to addressing those risks, has seen the expansion or establishment of laws to specifically apply to online behaviour in several countries, such as Australia and Germany. For a variety of political or cultural reasons, some countries, including the UK, have chosen not to introduce internet specific legislation or have chosen other measures, such as education, to combat some online risks.

## ILLEGAL INTERNET CONTENT

Legislation prohibiting content may operate in a number of ways. It may prohibit the production and distribution of illegal online content, either for commercial producers or for any member of the public. Alternatively, the possession or viewing of illegal online material may be a crime. Legal liability for illegal online content on the internet may rest with various parties in different jurisdictions. However, it is most common for content producers to be held responsible for illegal online content, with content hosts sometimes being held responsible for illegal content, and consumers of illegal internet content being held accountable infrequently.

Decisions about whether content is illegal may be made by a range of different bodies, including internet industry participants, government agencies or the courts.

### ***Child pornography***

Laws prohibiting the publication of child pornography online are common to many countries, although the specific provisions, such as the age of a child, may vary. However, there are some countries where, for cultural or political reasons, there has been no commitment to implementing a legal framework to protect children.

### ***Other illegal content***

Legislation regarding the publication or consumption of internet content varies significantly by country, and often reflects the historical legacy of censorship and protections for free speech in each nation. For example, in Australia, the existing legal framework for

classification of material for publication or broadcast was applied in 1999, with appropriate adjustments, to content distributed over the internet.

Topics that may be subject to prohibition in other countries include racist materials or content that instructs in or incites the commission of crimes. The approach taken in some EU countries means that content that is racist, associated with extreme political views, or holocaust denial is subject to particular restrictions. Some governments or restrictive political cultures may also prohibit the online expression of certain political or religious views. Conversely, in the US there are legal tensions between a general reluctance, based on constitutional safeguards, to prohibit or restrict any material and a desire to protect children from obscene material.

## **CHILD SEXUAL EXPLOITATION**

Enforcement of criminal laws relating to the sexual exploitation of children, including the procurement of children using internet technologies, is widely regarded as a part of any comprehensive online safety strategy. It is a widespread, international concern and many countries devote significant police resources to the investigation of child pornography and the prosecution of paedophiles.

## **ONLINE FRAUD**

Many jurisdictions have enacted legislation relating to online fraud activities and rules designed to protect consumers online. Police activity to detect, investigate and prosecute online fraud, along with police–industry partnerships to develop preventative strategies and educational messages, are crucial to addressing the growing risks of online fraud and other e-security concerns.

Among the legal measures to address online fraud are regulations addressing the proliferation of spam, which includes malicious emails and phishing, in which Australia is, in many ways, a world leader. In other jurisdictions, such as the Netherlands, which has also introduced legislation prohibiting the transmission of spam emails and has followed this through with a strong enforcement focus, efforts are under way to legislate against malicious or nuisance communications, both within existing anti-fraud and business legal frameworks, and through the establishment of laws that deal specifically with online behaviour.

# Chapter 4: Deployment of online safety initiatives in the European Union

## Overview

In preparing this report, ACMA is required to consider developments in filtering technologies and other online safety measures, having regard to how those measures are deployed in other countries, and any contextual considerations that might impact on the relevance of those deployments to Australia. ACMA has surveyed online safety initiatives in a range of countries, including the USA, with its focus on education programs, and Canada and New Zealand, which use a combination of measures to mitigate risks among users. However, the European Union (EU) is the focus for this report's examination of measures deployed internationally to address online risks because:

- the EU or individual EU member states have been early movers in the area of mitigating online risk, and stand as an example of one way to develop online safety measures in response to changing online risks;
- the EU is nearly unique in the world in having developed and articulated a series of programs aimed at addressing the full range of identifiable online risks in a comprehensive and integrated manner;
- the EU and its member states possess a culture, legal system and historical approach to management of content which is not significantly different to Australia; and
- the EU's programs, and programs in individual EU member states, have been a major stimulus of online safety activity internationally, providing a norm in respect of both the development of technological and educational safety solutions and the measurement of their desirability and effectiveness.

Since 1999, the EU has provided a regional policy and implementation framework for online safety, funding programs and initiatives to the value of €83.3 million, rather than, in general, making legislation to bind member states to specific actions. It has made a series of decisions relating to online safety, which establish funding, research and coordination of programs to facilitate national deployment of specific online safety projects and initiatives. This promotes consistency in addressing online risks, while allowing for tailored implementation of online safety measures in EU member states.

Individual initiatives in countries such as the UK and Germany foreshadowed and influenced particular aspects of the EU's approach. In turn, it has stimulated activity internationally with its influence felt beyond member countries, providing a focus for the development of technological and educational safety solutions and measurements of their desirability and effectiveness.

The *Safer Internet Action Plan* (SIAP), which was extended and later replaced by *Safer Internet Plus* (SIP), is the EU program designed to promote online safety. The program uses a number of approaches to address online risks: by tackling the proliferation of ‘harmful’ or illegal content; encouraging the development of technical measures such as filtering and content labelling; and raising awareness about risks and available measures to address them.

Several emphases are apparent in the SIAP and SIP programs. The EU places importance on stimulating commercially viable initiatives, coordinating networks, and encouraging industry responsibility and NGO programs to address online safety risks. SIP has a strong focus on collaboration to achieve shared goals, and encourages its networks to share their experiences, research and initiatives to better inform online safety measures across the region. The EU also invests in research through its funding of projects to investigate the effectiveness of filtering technologies and patterns of internet usage of European children. This focus supplements all online safety measures as it provides an evidence basis for action and supports innovation in developing new and appropriate approaches.

The INHOPE network was established in 1999 to further facilitate the effectiveness of work done by individual hotlines to reduce the spread of child pornography and other potentially illegal content. While INHOPE coordinates and facilitates EU member states’ national efforts to receive and act on complaints about potentially illegal content, its membership extends beyond Europe to include hotlines in Asian countries, Australia, Canada and the US.

The INSAFE network of awareness nodes was also established under SIAP, with the aim of providing consistent online safety messages to children, parents and teachers. Nodes have been established in 23 countries, including the Child Exploitation and Online Protection Centre in the UK and Klicksafe.de in Germany. The ability to undertake activities in close cooperation with all concerned parties at local, national and regional levels is an important factor in the allocation of node status. A European coordination node ensures the exchange of best practices.

In its early online safety initiatives, the EU considered education programs to be a necessary complement to its other online safety measures, but over time has invested proportionately more funding in awareness activities, to encourage member states to place a higher priority on awareness measures and increase the targeting of programs to identified groups including teachers, parents and children of different ages. Education and awareness programs in member states provide education about online risks using a variety of methods including television advertisements, schools programs, web portals and helplines.

The EU encourages the take-up of technological measures to enable users to manage the amount of unwanted and inappropriate content and spam they receive. It has initiated research into filtering and content labelling technologies, and its approach to these research projects has evolved over time. Early projects had a strong emphasis on stimulating research and the commercial development of filtering and content labelling technologies tailored to meet the needs of European citizens. Later studies have focused on assessing the strengths and limitations of commercially available filter products to inform parents about their choices with respect to filtering, and how best to use commercial offerings.

E-security risks have also been addressed in EU member states by various measures including a spam hotline, education programs and industry codes of practice. This is evidence of the EU’s general approach to online safety, which is to provide multiple measures to address the range of identified risks.



## **Introduction**

The earlier chapters of this report describe how concerns around the risks associated with individuals' use of the internet began to emerge in the early 1990s. These concerns were initially confined to risks associated with access to inappropriate and illegal content, but subsequently extended to e-security risks and risks associated with communication via the internet.

In the mid 1990s, as both risks and concerns around whether and how to mitigate them developed, the first measures for promoting online safety emerged. The impetus for the introduction of a number of these measures, notably in European countries, stemmed from concerns regarding the liability of ISPs, including the personal liability of the chief executive officer and other individual employees of ISPs, especially in regard to illegal material. The internet industry was also becoming sensitive to the potential for damage to its reputation.

An example of this development relates to illegal internet content: in August 1995, an article published in a Dutch computer magazine on child pornography on the internet prompted a public discussion about the responsibility of internet providers in relation to this material and the possibilities for self-regulation. The conclusion was reached at the political level that there was a need for an industry response to the problem. A working group was subsequently formed of the Dutch internet providers association, law enforcement agencies and internet users, which established Meldpunt, the first internet hotline against child pornography in Europe. The following year, the Internet Watch Foundation was established as the UK hotline in response to similar stimuli.

This chapter explores how filtering technologies and other online safety measures have been promoted under EU programs and have been deployed in specific EU countries to address the range of online risks.

Early initiatives such as the establishment of the Dutch and UK internet hotlines against child pornography were an important influence on the programs developed by the EU, starting in 1999. These programs emphasised collaboration between relevant stakeholders to understand and appropriately address online risks. This chapter consequently describes the evolution of the EU's programs in line with the evolution of online risks, from these early influences to the current focuses of attention in a Web 2.0 environment, as well as describing the components of the programs, the supporting legal framework, and illustrative examples of their deployment.

## **European Union approach to online risk**

The EU's distinctive approach to addressing online risks is rooted both in the fundamental objectives and principles on which the Union is based, and in its institutional and legal framework.

One of these fundamental objectives is the achievement of a single market applying across all of the EU's member states<sup>131</sup>. This objective involves the progressive removal of constraints on the free movement of goods, persons, services and capital between the member states to promote economic and social progress, and a high level of employment,

---

<sup>131</sup> *Treaty on European Union*, art. 2, ¶ 1, [2002 consolidated version], O.J. C325/33 24.12.2002, available at: [http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E\\_EN.pdf](http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E_EN.pdf)

and to achieve balanced and sustainable development. In respect of use of online services by EU citizens, this entails ensuring that they are able to gain maximum benefit from access to these services to facilitate economic and social progress, but without this benefit and progress being hindered by undue levels of risks, especially those affecting children.

Of the principles that guide the activities of the EU, one of the most central is subsidiarity<sup>132</sup>. Subsidiarity implies that decisions are not taken at the European level unless this approach is more effective than action taken at a national, regional or local level. This principle can be seen driving the EU's approach to online risk, whereby broad objectives for online safety programs are set at the European level, but member states or local administrations are given considerable scope to decide on the particular strategy for a program in their own jurisdiction.

The EU seeks to achieve its objectives and give effect to its principles through both formal and informal measures. The former includes laws binding EU member states, created by the legislative institutions of the EU, with the purpose of aligning national legislation across the Union while leaving the member states choice as to the form and method of realising the objectives of the European law. At a less formal level, the EU legal framework enables its institutions to make recommendations to member states or to other EU institutions suggesting particular lines of action regarding EU policy objectives without imposing any legal obligation. These EU recommendations possess persuasive power, but may also signal future formal measures or funding of programs. The EU also makes funds available for pan-European projects or to stimulate efforts at a national, regional or local level in furtherance of Europe-wide policy objectives.

## **Legal framework**

The EU has more often taken the approach of adopting informal measures to address issues of online safety. In 1998, the Council of the EU adopted the first Recommendation on the Protection of Minors and Human Dignity in Audiovisual and Information Services<sup>133</sup>, which encouraged member states to:

- establish national frameworks for self-regulation of online service providers;
- fight against illegal online content by handling complaints and forwarding information about the content to relevant national authorities, and by cooperating with complaint-handling structures in other countries; and
- enhance awareness among parents and teachers of the potential of online services and ways they can be made safe for children.

The recommendation also urged European industry to:

- participate in the coordination of European and international efforts to protect children;
- develop codes of practice for the protection of children in respect of online services; and

---

<sup>132</sup> *Treaty on European Union*, art. 5 and protocol, [2002 consolidated version], O.J. C325/33 24.12.2002, available at: [http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E\\_EN.pdf](http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E_EN.pdf)

<sup>133</sup> *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 (98/560/EC)*, O.J. L270/48 7.10.98, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/1998/l\\_270/l\\_27019981007en00480055.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/1998/l_270/l_27019981007en00480055.pdf)

- develop new means of protecting children.

This first recommendation was followed in early 1999 by the launch of the first four-year (later extended to six-year) funding program for internet safety initiatives, the *Safer Internet Action Plan* (SIAP), discussed separately.

In December 2006, two years after the launch of a second four-year funding program, the *Safer Internet Plus* (SIP) program, the European Parliament and the Council of the EU adopted a second Recommendation on the Protection of Minors and Human Dignity in Audiovisual and Information Services<sup>134</sup>. This new recommendation continued the earlier encouragements to member states to establish structures for reporting of illegal activities on the internet and to improve the level of awareness among parents and teachers of ways of making online services safe for children.

In addition, the second recommendation urged the online services industry, for the first time in such specific terms, to examine the possibility of creating filters to ‘prevent information offending against human dignity’ being transmitted via the internet. The recommendation also recorded the intention of the European Commission to introduce a pan-European freephone number to provide European internet users with information on issues related to protection of minors and human dignity, and to support the formation of pan-European networks of self-regulatory bodies aimed at enhancing the effectiveness of self-regulatory codes of conduct.

While this approach of encouraging action by member states and by industry has applied in the area of online content risks, the EU has adopted a more formal approach in the area of e-security risks. In 2002, as part of the introduction of a new European framework for regulation of electronic communications, the EU adopted the Privacy and Electronic Communications Directive<sup>135</sup> requiring member states to introduce national legislation that prohibits the sending of unsolicited communications, principally spam, without the consent of the addressee.

The directive requires that individuals must be asked to opt in for communications when personal data is first provided to an organisation—such as when opening an account—and given the choice of opting out with all subsequent communications. The directive also requires that access to or storing information on a user’s communications device, such as a home computer or mobile phone, is only allowed if the user is given clear information about the purpose of this action and is offered the opportunity to refuse it. This rule applies to **spyware**<sup>136</sup>, **Trojan horses**<sup>137</sup> and **cookies**<sup>138</sup>.

---

<sup>134</sup> *Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry* (2006/952/EC), O.J. L378/72 27.12.2006, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l\\_378/l\\_37820061227en00720077.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_378/l_37820061227en00720077.pdf)

<sup>135</sup> *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, O.J. L201/37 31.07.2002, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l\\_201/l\\_20120020731en00370047.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf)

<sup>136</sup> **Spyware** is software that is used to capture personal information without the user’s knowledge for business purposes, such as advertising, or criminal purposes such as theft.

<sup>137</sup> A **Trojan horse** is software hidden in messages or in other apparently innocent software.

<sup>138</sup> **Cookies** are information stored on a device for the purpose of tracking an end user’s use of a website or registering their preferences

The directive was followed in 2004 by the adoption of a regulation that created a new EU agency, the European Network and Information Security Agency<sup>139</sup>, with responsibility for developing a culture of e-security across Europe. The agency is directed under the regulation to enhance the capabilities of the EU as a whole, member states and businesses to prevent, address and respond to network and information security issues.

## **Programs to address online risk**

The EU has, since 1999, implemented a coordinated series of programs to address online risks across its member states<sup>140</sup> with the general objective of promoting ‘the safer use of the Internet and to encourage, at European level, an environment favourable to the development of the Internet industry.’ The first 1999–2002 program, the SIAP, was renewed for a further two years to December 2004 and the SIP program currently runs until December 2008.

All iterations of the program have included the creation of a safer environment by establishing a European network of hotlines and encouraging self-regulation and codes of conduct; developing filtering tools; and raising awareness.

Major emphases of the programs have been:

- cooperation with international organisations and countries outside Europe in implementing measures to mitigate online risks—in recognition of the global character of online risks—with the aim of extending the reach of the programs beyond Europe and moving towards a global solution for these problems; and
- achieving a fully functioning system of industry self-regulation with the purpose of limiting the flow of unwanted, harmful and illegal content.

The programs have sought to address online risks using an extensive range of strategies. These include:

- carrying out research into how children use new online technologies;
- stimulating the creation of a European network of hotlines to allow users to report illegal content they encounter while using the internet, collecting data to evaluate the effectiveness of the hotlines, and enhancing coordination across the network of hotlines to improve operational effectiveness;
- supporting telephone helplines for children confronted with illegal and harmful content;
- encouraging self-regulation about rating and filtering techniques, the adoption of industry codes of conduct aimed at restricting the flow of illegal and harmful content, and stimulating networks of bodies responsible for self-regulation;
- increasing the availability of comparative information about the performance and effectiveness of filtering technologies to allow users to make an informed choice;

---

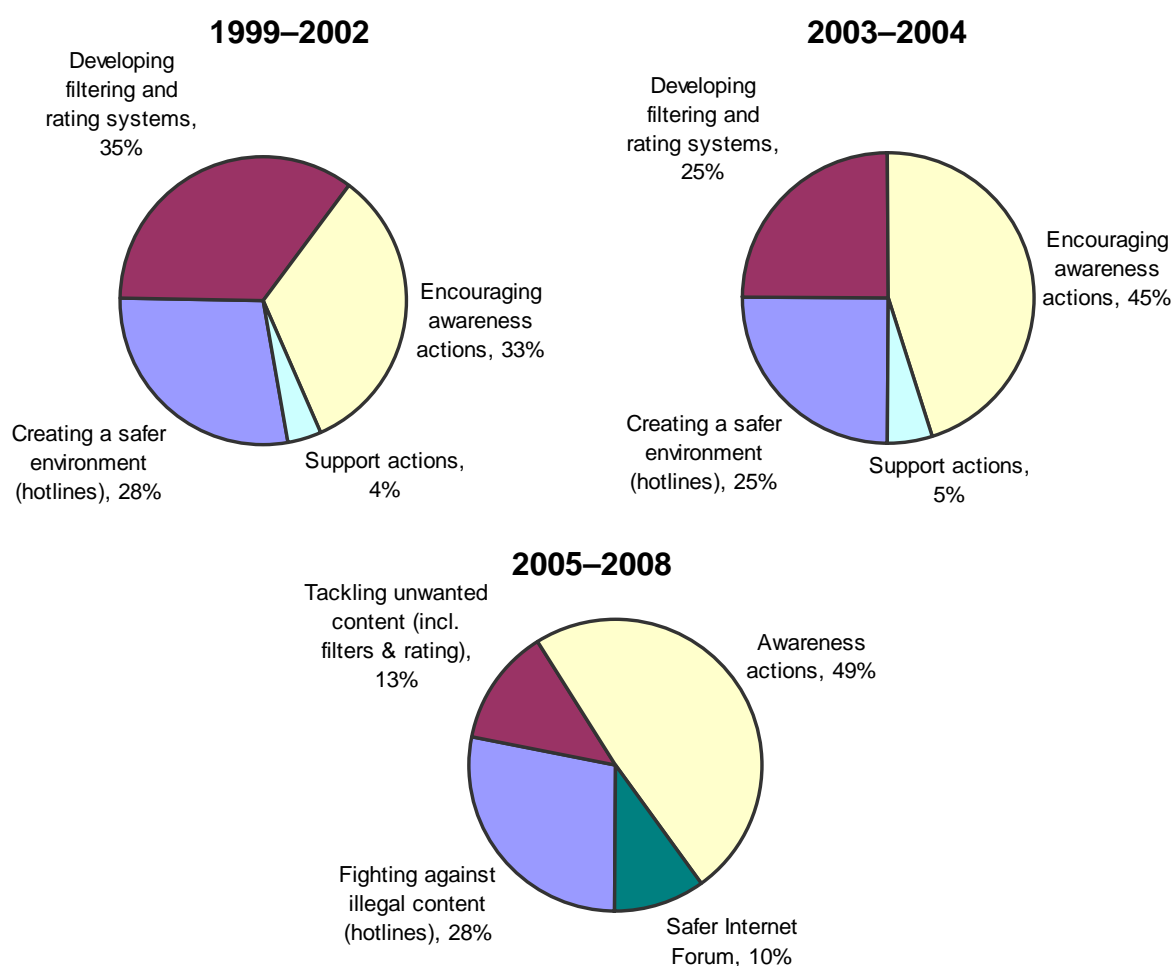
<sup>139</sup> *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, O.J. L 077/1 13.03.2004, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

<sup>140</sup> *Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, O.J. L33/1 6.2.1999, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l\\_033/l\\_03319990206en00010011.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l_033/l_03319990206en00010011.pdf)

- supporting appropriate bodies to inform parents and teachers about the best way to protect minors against exposure to content that could be harmful to their development;
- stimulating awareness actions by ISPs, content providers, consumer associations and the education sector, and facilitating exchanges on best practice in raising awareness about online safety;
- encouraging the use of technology to enhance privacy;
- assessing laws that are applicable to internet safety, mindful that the internet operates on a global basis; and
- ensuring coherence between initiatives in Europe and similar actions in other parts of the world.

The role of the EU in funding these programs has been to ensure, as far as possible, assignment of equal attention and resources across its member states to issues of online safety. This objective has been supported by EU legislation in the area of e-security risks, which have sought to ensure commonality of approach in mitigating these risks.

**Figure 4.1: Planned expenditures under the SIAP and SIP programs, 1999 to 2008**



The programs were allocated €83.3 million for the period from 1999 to 2008. Under the first tranche of the SIAP from 1999 to 2002, funds were split almost equally between establishing hotlines, developing filtering and rating systems and encouraging awareness campaigns with a small proportion dedicated to support actions. Under the SIAP extension through 2003 and

2004, approximately one quarter of funds were each dedicated to hotlines and developing filtering and rating systems, with awareness programs receiving almost half the funding. In the last four years of the program from 2005 to 2008, the proportion dedicated to awareness-raising measures has risen to a half, almost 30 per cent to hotlines with a smaller proportion dedicated to filtering, rating and privacy technologies, as highlighted in Figure 4.1.

The programs have evolved over their eight years, and have more recently broadened in scope to include new media and measures to combat spam.

The remainder of this chapter will discuss the scope of the SIAP and SIP programs in the EU, and specific initiatives in the EU member states, notably the UK and Germany. Both of these member countries have implemented a broad range of initiatives to address online risks and have contributed to the development of the SIAP and SIP programs.

## RESEARCH INITIATIVES

Under the SIAP and SIP programs, the EU has emphasised the importance of research to support and refocus its programs to enhance online safety. The research program helps ensure that online safety programs evolve in line with the evolution of online risks. Under these programs, the EU has funded research on:

- the performance and effectiveness of filtering technologies, discussed below under *Filtering initiatives*;
- use of new online technologies by children; and
- e-security.

In preparation for the deployment of the SIAP in 1999, the European Commission commissioned research into online safety education in Europe. The work was conducted by a partnership including Childnet International and involved an assessment of what messages would help children to stay safe online, and how to best communicate those messages to children, parents and teachers<sup>141</sup>. Employing this research, the SIAP program included a European commitment to raise awareness about both the benefits and risks of internet usage to promote the safe use of the internet by children. The EU described this work as a ‘necessary complement’ to the other initiatives associated with filtering and content labelling development, and the development of hotlines to restrict the proliferation of illegal content<sup>142</sup>.

The SIP program has provided funding for research into the online behaviour of young people across Europe through *EU Kids Online*<sup>143</sup>. *EU Kids Online* is a three-year study running between 2006 and 2009 to investigate children’s use of online technologies across 18 member states. The study aims to develop policy recommendations for awareness-raising and media literacy. *EU Kids Online* has produced 235 research projects into children’s

---

<sup>141</sup> Childnet International and Fleishman Hillard International Communications (1999), *Promoting Safe Use of the Internet – Final Report*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/PREP-ACT\\_4\\_Awareness\\_summary.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/PREP-ACT_4_Awareness_summary.pdf), accessed 21 November 2007

<sup>142</sup> *Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, O.J. L33/1 6.2.1999, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l\\_033/l\\_03319990206en00010011.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l_033/l_03319990206en00010011.pdf)

<sup>143</sup> More information about this program is available at: <http://www.lse.ac.uk/collections/EUKidsOnline/>.



online activities revealing that a high proportion of children across surveyed countries use the internet to do schoolwork, use email, play games, and communicate with friends using IM, while a small minority use the internet to seek out sexually explicit content<sup>144</sup>.

The Eurobarometer survey series, part of which is funded under the SIP program, collects data on a broad range of topics relating to the lifestyles of Europeans. The Eurobarometer research assists the European Commission to refine the SIP program.

Eurobarometer's internet-specific research includes an investigation into how children of different age groups use online technologies, including the internet and mobile phones, and how they perceive and respond to these risks. The study covers 29 countries (the 27 EU states plus Iceland and Norway) and aims at improving knowledge about:

- internet and mobile usage by children;
- children's online behaviour; and
- children's perceptions of risk and safety related questions.

In addition to the research specifically funded under the SIP program, the Cyberspace Research Unit contributes to the research initiatives of EU by sharing information, expertise and resources with EU members who have developed education and awareness material. Based at the University of Central Lancashire in the UK, the Cyberspace Research Unit<sup>145</sup> specialises in researching internet policy issues. Research by the CRU has been commissioned by the UK Home Office, as well as the European Commission. The Cyberspace Research Unit's work has recently included:

- conducting research to underpin the development of programs of education and raising awareness about internet safety for the European Commission<sup>146</sup>; and
- carrying out research for the UK Home Office Internet Task Force, which resulted in the report, *Children and Young People's Use of Chat Rooms: Implications for Policy Strategies and Programs of Education*. This project surveyed nearly 1,400 children aged 9 to 16 years across 42 schools in the UK about their real-time communication experiences while online (discussed further below).

Research on e-security is undertaken by the European Network and Information Security Agency (ENISA). ENISA was established in March 2004 and undertakes a program of research on security breaches and emerging risks. It also advises the EU and member states about e-security matters and stimulates cooperation between the public and private sectors to raise awareness about e-security issues.

To ensure its information remains current and relevant, ENISA supports a network of national liaison officers, providing an arena to exchange information between member states and with the three major European institutions (the Council, the European Parliament and the European Commission). ENISA also frequently hosts conferences, meetings and information sessions in cities across Europe, with specialist topics designed to address information security concerns as they arise.

---

<sup>144</sup> Livingstone, S. (2007), 'EU Kids Online', Paper delivered at the *Safer Internet Forum Conference*, 20-21 June 2007, Luxembourg, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/forum\\_june\\_2007/eukidsonline\\_livingstone.pdf](http://ec.europa.eu/information_society/activities/sip/docs/forum_june_2007/eukidsonline_livingstone.pdf)

<sup>145</sup> For more information, see [www.uclan.ac.uk/host/cru/internet\\_safety.htm](http://www.uclan.ac.uk/host/cru/internet_safety.htm).

<sup>146</sup> For more information about the CyberSpace Research Unit, see [www.uclan.ac.uk/host/cru/](http://www.uclan.ac.uk/host/cru/).

## FILTERING INITIATIVES

Alongside other measures under the SIAP and SIP programs, the EU has sought to promote technological means such as filtering to shield children from inappropriate content and all users from potentially illegal content.

The EU's approach to filters has changed over the life of its SIAP and SIP programs. It has included support for local or industry initiatives to enhance the technical capabilities of filtering products, self-regulatory measures at the national level to encourage the deployment of filters, and research on filter products for the purpose of informing parents' choices in selecting filtering solutions. Its support for filtering as part of its suite of measures to address content risks has led to complementary national-led initiatives including filtering of illegal content by ISPs and search engine providers, and the development of a UK national standard for filtering software.

In 1998, before establishing the SIAP, the EU allocated funds for scoping projects including a feasibility study for a European system of content rating and labelling, and also a review of third party filtering and rating software and services.

The review of third-party filtering and rating software and services assessed the effectiveness of selected filtering software in several European countries to determine how well they addressed the cultural and linguistic differences of the European community<sup>147</sup>. Similarly, the feasibility study for a European system of content self-rating assessed how well existing labelling schemes addressed the needs of the European community<sup>148</sup>. These studies found that the filtering solutions did not meet the needs<sup>149</sup> and concluded that the EU should support the development of a content labelling scheme suitable for European consumers that would enable them to configure their internet access in accordance with their personal preferences<sup>150</sup>.

Work by the European Commission under the SIAP focused on the development and production of filtering software products to protect internet users from harmful and illegal content<sup>151</sup>. The findings led to funding for 13 projects between 1999 and 2002<sup>152</sup>. The aim of

---

<sup>147</sup> IDATE, AIIP and DATABANK Consulting (1999), *Review of European third-party filtering and rating software and services*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/html/reports/idate/IDATEexec.htm](http://ec.europa.eu/information_society/activities/sip/docs/html/reports/idate/IDATEexec.htm), accessed 26 November 2007

<sup>148</sup> INCORE (2000), *Action Plan on promoting safer use of the internet: Self-labelling and filtering*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/html/reports/incore/INCOREexec.htm](http://ec.europa.eu/information_society/activities/sip/docs/html/reports/incore/INCOREexec.htm), accessed 21 November 2007

<sup>149</sup> IDATE, AIIP and DATABANK Consulting (1999), *Review of European third-party filtering and rating software and services*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/html/reports/idate/IDATEexec.htm](http://ec.europa.eu/information_society/activities/sip/docs/html/reports/idate/IDATEexec.htm), accessed 26 November 2007

<sup>150</sup> INCORE (2000) *Action Plan on promoting safer use of the internet: Self-labelling and filtering*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/html/reports/incore/INCOREexec.htm](http://ec.europa.eu/information_society/activities/sip/docs/html/reports/incore/INCOREexec.htm) accessed 21 November 2007

<sup>151</sup> *Communication from the Commission of 3 November 2003 concerning the evaluation of the multiannual Community action plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors*, COM(2003) 653 final .6.11.2006, available at: <http://www.europa.eu/scadplus/leg/en/lvb/124190.htm>

<sup>152</sup> European Commission (2007), 'Filtering and Rating: Closed Projects', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/targeted/filtering/closed\\_projects/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/closed_projects/index_en.htm), accessed 19 November 2007



these projects was to establish content rating and filtering systems that responded to the specific needs of the European community—by stimulating the use of labels by content providers, enabling filtering and labelling solutions to be implemented in a way that suited users' needs, and by filtering content in languages other than English, on various operating systems.

Under this approach, work was continued by ICRA (later FOSI) to convert other content labelling systems to ICRA labels so that consistent labels could be applied across web content and a web-based service developed where content providers could obtain content labels with which to describe their sites<sup>153</sup>.

Of particular interest is the Netprotect project, which was funded to review existing filtering tools, analyse requirements of European users and develop a prototype of multi-lingual filtering software. This project used a filtering solution that integrated Optenet's<sup>154</sup> filtering solution, the LTU Technologies'<sup>155</sup> Image Filter and a text classifier developed for the project<sup>156</sup>.

The European Commission formally evaluated its projects funded under the SIAP between 1999 and 2002. It found that, in comparison to other projects such as the establishment of hotlines, the benefit of filtering projects could not be established until the uptake of filtering and content rating software technologies was clear<sup>157</sup>. Accordingly, it decided to also focus on benchmarking filtering software and promoting the take-up of content labelling by content providers<sup>158</sup> and in 2003–04 it funded:

- one project for content rating, incorporating labelling standards developed by a group of organisations comprising, ICRA, Web Mèdica Acreditada (which developed a labelling system for medical sites in Spain and Latin America), and the Internet Quality Agency (which promotes an international website labelling scheme);
- one project for rating online games—the Pan European Game Information System, which provides parents with information about the content of games; and
- a three year benchmarking study—SIP-BENCH—into the performance and effectiveness of filters that can be deployed at network locations, including on home computers, to be undertaken from 2005 to 2008.

---

<sup>153</sup> European Commission (2007), 'ICRA Safe: Internet Content Rating Association', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/targeted/filtering/closed\\_projects/icrasafe/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/closed_projects/icrasafe/index_en.htm), accessed 19 November 2007

<sup>154</sup> Optenet is a vendor of filtering software and is a provider of filtering for the Australian Government's NetAlert program (see [www.optenet.com/en/index.asp](http://www.optenet.com/en/index.asp)).

<sup>155</sup> LTU Technologies provides software for search, retrieval, classification, analysis, recognition and mining of images and videos (see [www.ltutech.com/en/](http://www.ltutech.com/en/)).

<sup>156</sup> Netprotect (2002), *Netprotect: A European Prototype for Internet Access Filtering* [EC Commissioned Report], NETPROTECT:WP5:D5.1:2002, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/netproject\\_final\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/netproject_final_report.pdf)

<sup>157</sup> Technopolis (2003), *The Evaluation of the Safer Internet Action Plan 1999-2002*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/reports/evaluation\\_safer\\_internet\\_full\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/reports/evaluation_safer_internet_full_report.pdf), accessed 20 November 2007

<sup>158</sup> *Decision no 1151/2003/EC of the European Parliament and of the Council of 16 June 2003, amending Decision No 276/1999/EC adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*. O.J. L162/1 1.7.2003, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/programmes/extension/extension\\_decision\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/programmes/extension/extension_decision_en.pdf)

## SIP-BENCH

The objectives of the *Study on Safer Internet Programme Benchmarking of Filtering Software and Services*—SIP-BENCH—are to provide comparative information about a broad range of filtering products to assist parents and other responsible adults in selecting filtering products for installation on their home computer<sup>159</sup>.

The first report was undertaken by Deloitte and published in December 2006. It explores the performance, effectiveness and ease of use of several filters that are currently available in the market. The report also considered whether products were able to effectively filter out inappropriate content, including content relating to suicide and race hate, as well as content that could cause distress, fear or confusion in young children, such as cruelty to animals and child abandonment<sup>160</sup>.

The report found that the filters tested were generally good at blocking access to sexually explicit material on commonly accessed websites, expressed in a common language. The report also found that filtering could be undertaken using different methods, including blocking requests for content based on:

- lists of allowed or disallowed content;
- keywords (in URLs or website content);
- ICRA labels; or
- type of applications.

The report also found that increasingly filter products supported languages other than English.

However, the filters tested were not generally effective for limiting access to inappropriate content. It was found that well-established methods for filtering content based on blacklists will become increasingly ineffective for preventing users from accessing user-generated content.

The report detailed a number of limitations for filter products. These included:

- the lack of customisation features to enable the parent or responsible adult to modify filtering to their particular values and concerns;
- access to the internet being blocked when the product was uninstalled by some filter products, even though the majority of filtering products were considered relatively easy to install;
- conflicts with other software caused by the installation of filtering products, most notably security software such as anti-virus, firewalls and adware-blockers;
- incorrect decisions by the filters in 25 per cent of cases about inappropriate content; and
- a minimum doubling of time to display requested content for all filter products, with some products increasing the time to display content eightfold<sup>161</sup>.

<sup>159</sup> European Commission (2007), 'Safer internet shielding benchmark', available at: [www.sip-bench.org/sipbench.php?page=benchmark&lang=en](http://www.sip-bench.org/sipbench.php?page=benchmark&lang=en), accessed 12 November 2007

<sup>160</sup> Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, available at: <http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf>

<sup>161</sup> Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, available at: <http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf>

Filter products considered in the report generally did not perform well in more than one category for performance, effectiveness and ease of use. That is, a product that was easy to install was generally not also found to be free from conflicts with other software and introduced delays in accessing requested content.

When evaluating the progress of the SIAP, the European Commission considered that 'Filtering systems are also an essential element in the eyes of the stakeholders. However, there is too little knowledge among parents on how to handle them and the progress made in developing these technologies remains unsatisfactory.'<sup>162</sup>

Further benchmarking reports will be published in 2007 and 2008.

The EU programs have promoted industry's role in addressing issues associated with illegal and inappropriate content. Its encouragement of self-regulatory responses to the availability of potentially illegal content on the internet has, in conjunction with local concerns, stimulated the development of targeted measures in the UK and Germany. These include the development of systems to filter potentially illegal content and codes of practice to address internet user's access to inappropriate and potentially illegal content in member countries in 2004. Codes of practice include the *UK Code of Practice for the Self-Regulation of New Forms of Content on Mobiles* and the FSM Code of Conduct (FSM Code) in Germany.

### Illegal content filtering

To address increasing concerns about internet users' access to illegal content online, the UK's largest ISP, BT, developed in 2003 and implemented in 2004 a technology for filtering illegal content within its own network, known as Cleanfeed. The UK government has subsequently encouraged all UK ISPs to implement illegal content filtering at the ISP level, and a high proportion of ISPs have now implemented filtering solutions. To assist, BT has offered the design for its filter to other ISPs on a no-cost, non-disclosure basis, so that they can tailor and deploy the system on their own networks<sup>163</sup>. This system has also been deployed by many other ISPs internationally.

BT's content filter aims to prevent internet customers from accessing content contained in the IWF list<sup>164</sup>. The IWF list is an index of URLs of child pornography that is hosted outside the UK and is potentially illegal under UK legislation. The list is updated twice daily with approximately 80 new URLs added each week<sup>165</sup>. Compared with commercially developed indexes that may contain millions of URLs divided into categories, ACMA understand that the IWF list is a single undifferentiated index generally containing between 1,000 and 1,200 URLs. These URLs are reassessed regularly and non-current URLs are removed<sup>166</sup>.

---

<sup>162</sup> *Final evaluation of the implementation of the multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, COM(2006) 663 final, available at: [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexplus!prod!DocNumber&lg=en&type\\_doc=COMfinal&an\\_doc=2006&nu\\_doc=663](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2006&nu_doc=663), accessed 19 November 2007

<sup>163</sup> BT (2007), 'Changing World: Sustained Values', p. 7, available at: [www.networked.bt.com/pdfs/BT\\_CSR\\_Business\\_Overview.pdf](http://www.networked.bt.com/pdfs/BT_CSR_Business_Overview.pdf), accessed 8 October 2007

<sup>164</sup> Clayton, R. (2005), *Anonymity and Traceability in Cyberspace*, Technical Report No 653, Cambridge University, available at: [www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html](http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html), accessed 26 October 2007

<sup>165</sup> Internet Watch Foundation (2007), 'Commercialising the database', available at: [www.iwf.org.uk/corporate/page.121.251.htm](http://www.iwf.org.uk/corporate/page.121.251.htm), accessed 22 November 2007

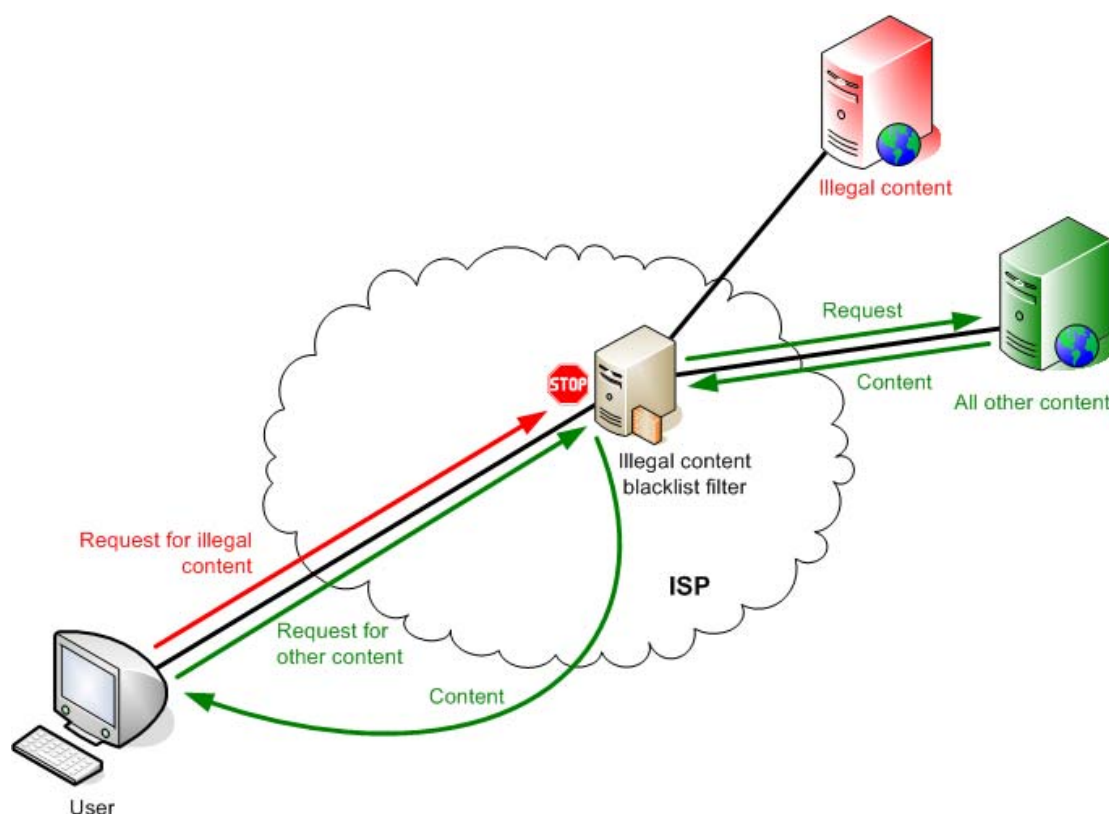
<sup>166</sup> Internet Watch Foundation (2007), 'Presentation to INHOPE Members' Technical Workshop' [Unpublished], 26 October 2007, Berlin

Under BT's filtering solution, all requests for content are checked against the IWF list and requests that are for content on the list are blocked by the filter. A key feature of BT Cleanfeed is the minimal impact it has on network performance because only a small amount of traffic undergoes any filtering or blocking. Filtering can be undertaken at individual image or page level. ACMA understands that customer URL requests are 'pre-qualified' by IP address, and only those which relate to 'suspect' IP addresses are subjected to further analysis. This initial prequalification causes minimal network latency and only users requesting URLs from suspect IP addresses are likely to notice any delay.

As a small, specific-purpose list or index, it requires less computational resources than would be required if content requests were to be assessed against a large index that contained a number of sub-categories that were activated based on each subscriber's individual preferences. However, network performance could be expected to be degraded where the list of content to be filtered went beyond child pornography material, resulting in more URL requests undergoing further analysis to determine whether they should be blocked (see under *Performance impacts* of filtering in Chapter 3).

ACMA understands that most deployments of BT Cleanfeed are blocking websites only, and while the system is likely to be effective for commercial sites offering child abuse material, it is not designed to filter peer-to-peer, chat or other protocols.

**Figure 4.2: Operation of illegal content filter deployed by ISPs**



The IWF makes its list available to those commercial filter and security software vendors that are IWF members so that it can be included in the indexes used in their products. These products include filter software, hardware and managed services designed to be deployed in the full range of network locations and filter markets discussed in Chapter 3—home computers, enterprises (including small or large business and schools), mobile networks,

search engines and ISP networks<sup>167</sup>. IWF members that use its list in their filtering solutions include:

- RM, which provides an internet filtering service for more than 3,000 UK schools<sup>168</sup>; and
- Vodafone UK, which uses both the IWF blacklist and analysis-based filtering as a default for all its mobile internet service for all customers under 18 years of age<sup>169</sup>.

## Other measures to encourage technological solutions

### German initiatives

In Germany, the hotline operator FSM developed a code of conduct for ISPs to promote online safety. The FSM Code, developed in 2004, uses a combination of measures to address online safety issues including:

- the education of children in media literacy;
- age verification to restrict access to age-restricted content; and
- reporting of illegal content to relevant authorities<sup>170</sup>.

A sub-code of conduct sets out filtering requirements for search engine providers. Under the sub-code, search engine providers, including ask.de, AOL, Google, Lycos, MSN, t-info and Yahoo, must implement technical measures to minimise the risk to young people of accessing content that is harmful to them<sup>171</sup>. In addition, search engine providers have agreed not to display search results that contain content that the state has certified to be harmful to young people<sup>172</sup>.

During 2006–07 the German Kommission für Jugendmedienschutz des Landesmedienanstalten [Commission for the Protection of Minors in the Media] (KJM)<sup>173</sup> and one of the German INHOPE hotlines, Jugendschutz.net, undertook research into the efficacy of filters in blocking access to content that is illegal or inappropriate for young audiences<sup>174</sup>. The research was intended to assess how effective filters were as a tool by which content providers could meet their obligations under the *Interstate Treaty on Media and Protection of Youth Regarding Preventing Access by Minors to Harmful Content*. The

---

<sup>167</sup> Internet Watch Foundation (2004), 'Filtering Solutions,' 8 September 2004, available at: [www.iwf.org.uk/public/page.28.34.htm](http://www.iwf.org.uk/public/page.28.34.htm), accessed 20 November 2007

<sup>168</sup> Internet Watch Foundation (2004), 'RM join IWF as funding member,' [Media Release] 11 May 2004, available at: [www.iwf.org.uk/media/news.archive-2004.30.htm](http://www.iwf.org.uk/media/news.archive-2004.30.htm), accessed 20 November 2007

<sup>169</sup> Internet Watch Foundation (2004), 'Nomination shortlist for IWF ISPA Award,' [Media Release] 23 December 2004, available at: [www.iwf.org.uk/media/news.archive-2005.149.htm](http://www.iwf.org.uk/media/news.archive-2005.149.htm), accessed 20 November 2007

<sup>170</sup> FSM (2007), *Code of Conduct for the Association Freiwillige Selbstkontrolle Multimedia*, available at: <http://fsm.de/en/CoC>, accessed 21 October 2007

<sup>171</sup> In accordance with the *German Penal Code and the Inter-State Agreement on Youth Protection in the Media*, § 5, Section 1

<sup>172</sup> FSM (2007) *Subcode of Conduct for Search Engine Providers of the Association of Voluntary Self-Regulating Multimedia Service Providers*, available at [http://fsm.de/en/SubCoC\\_Search\\_Engines](http://fsm.de/en/SubCoC_Search_Engines), accessed 21 October 2007

<sup>173</sup> KJM was established in 2003 and consists of 12 members from the media, youth protection and government sectors. KJM is responsible for overseeing the adherence to the JMStV, the primary piece of German legislation governing internet and media content, by internet and broadcast media organisations.

<sup>174</sup> KJM (2007), 'Jugendschutz im Internet: KJM-Prüfung zeigt erhebliche Defizite von Jugendschutzfiltern auf', [Media Release], 1 March 2007, available at: [www.kjm-online.de/public/kjm/index.php?news\\_id=89&show\\_1=59.53&z=14&action=show\\_details](http://www.kjm-online.de/public/kjm/index.php?news_id=89&show_1=59.53&z=14&action=show_details), accessed 20 November 2007



KJM-Jugendschutz tests found that filtering products were not optimal for blocking inappropriate content such as violent and race-hate material and blocked some content targeted to children<sup>175</sup>.

### **UK initiatives**

In the UK, the Home Office and Ofcom are seeking to empower parents to appropriately manage their children's access to material available on the internet<sup>176</sup> through the launch of a standard for filtering software in 2006, developed with the British Standards Institute. The standard covers filters deployed both on ISP networks and home computers, and sets out minimum performance requirements, including specifications regarding ease of use, effectiveness and minimum features.

### **Mobile initiatives**

By 2003, the appeal of mobile devices to children and young people as a 'personal gateway' was becoming increasingly apparent and UK mobile operators—Orange, O2, T-Mobile, Vodafone, Virgin and '3'—developed an industry code of practice targeting risks associated with mobile access to the internet. Under the code, mobile operators agreed to:

- offer parents and carers the opportunity to apply a filter to the mobile operator's internet service so that access to adult content is restricted for their children;
- appoint an independent classification body to provide a framework for classifying commercial content that is unsuitable for customers under the age of 18;
- place commercial content classified as 18+ behind access controls, only making this content available following verification that the customer is over 18; and
- take action against unsolicited bulk messages (spam) and malicious communications.

The code also provides for cooperation with law enforcement agencies regarding mobile online communications and other mobile content.

The benefits of this code for protecting children from potentially inappropriate internet content accessed over mobile devices were acknowledged by the European Commission. The EU has subsequently promoted the development of codes of practice by mobile providers to address issues including access controls for adult content, awareness-raising for parents and children about the risks posed by mobile phone usage, the classification of mobile phone content according to national standards, and action to prevent illegal content on mobile phones<sup>177</sup>.

Under an in-principle agreement to develop codes—the European Framework on Safer Mobile Use by Younger Teenagers and Children<sup>178</sup>—major European mobile providers have

---

<sup>175</sup> KJM (2007), 'KJM fordert die Entwicklung effizienter Jugendschutzprogramme Prüfung zeigt Defizite auf: Filtersysteme im Internet nicht ausreichend wirksam', [Media release] 29 October 2007, available at: [www.kjm-online.de/public/kjm/index.php?news\\_id=101&show\\_1=59.53&z=3&action=show\\_details](http://www.kjm-online.de/public/kjm/index.php?news_id=101&show_1=59.53&z=3&action=show_details), accessed 20 November 2007

<sup>176</sup> Ofcom (2006), *Ofcom Media Literacy Bulletin* (8), available at: [www.ofcom.org.uk/advice/media\\_literacy/medlitpub/bulletins/issue\\_8.pdf](http://www.ofcom.org.uk/advice/media_literacy/medlitpub/bulletins/issue_8.pdf), accessed 16 November 2007

<sup>177</sup> European Commission (2007), 'Mobile operators agree on how to safeguard children using mobile phones,' [Media Release] 6 February 2007, IP/07/139, available at: [www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=HTML&aged=0&language=EN&guiLanguage=en](http://www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=HTML&aged=0&language=EN&guiLanguage=en), accessed 21 October 2007

<sup>178</sup> European Commission (2007), 'Mobile operators agree on how to safeguard children using mobile phones,' [Media release] 6 February 2007, IP/07/139, available at:

committed to the development of codes by 2008. The mobile network operators and content providers that signed the agreement comprise Bouygues Telecom, Cosmote, Debitel, Deutsche Telekom, GmbH, Go Mobile, Hutchison 3G, Jamba!, KPN, Mobile Entertainment Forum, Orange, SFR, Telecom Italia, Telefonica Moviles, Telenor, TeliaSonera and Vodafone.

## HOTLINES

The first internet **hotlines**<sup>179</sup> to address concerns about illegal content, particularly child pornography, included hotlines in Austria, France, Germany, the Netherlands and the UK.

### German hotlines

In 1997, three organisations run hotlines in Germany—Jugendschutz, as a government initiative, and eco and FSM, which in partnership operate the *Internet-Beschwerdestelle* [the Internet Complaints Office] with an industry remit.

#### *Jugendschutz.net*

Jugendschutz.net<sup>180</sup> was founded by the federal states of Germany as a hotline focused on protecting youth from harmful content that may endanger their wellbeing. Jugendschutz.net was founded in 1997 and is the joint organisation of all German states for the protection of minors. Its remit flows from child protection law<sup>181</sup>.

#### *eco*

As an industry association that aims to enhance the commercial use of the internet in Germany and to represent German internet business in political, legislative and international forums, eco represents about 250 members, who transmit approximately 85 per cent of the internet traffic in Germany<sup>182</sup>. It operates a hotline with FSM to respond to the public's complaints about potentially illegal and offensive content, including race-hate and material that is deemed to be detrimental to the development of children, on the internet. While this hotline was established in 1997, it has been open to complaints from the public since 2001.

#### *FSM*

FSM was formed by an alliance of content providers, service providers and other media organisations. In addition to its hotline role, FSM provides information and advice to service providers and the public about media youth protection, related technologies and responsible media usage through detailed pages on its website.

FSM's hotline responds to reports on potentially illegal or harmful web content. Specifically, FSM responds to complaints about sites that:

- offer freely-accessible pornography;
- depict children and minors in unnatural poses;
- glorify or trivialise violence;

---

[www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=HTML&aged=0&language=EN&guiLanguage=en](http://www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=HTML&aged=0&language=EN&guiLanguage=en), accessed 21 October 2007

<sup>179</sup> **Hotlines** are initiatives that receive complaints from users about illegal material on the internet and have formal procedures for processing these complaints (Childnet International, 1998)

<sup>180</sup> For more information about Jugendschutz.net, see [www.jugendschutz.net](http://www.jugendschutz.net).

<sup>181</sup> *Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia*, art 18, 01.03.2007, [English Version], available at: [www.kjm-online.de/public/kjm/downloads/JMStV2007-englisch.pdf](http://www.kjm-online.de/public/kjm/downloads/JMStV2007-englisch.pdf)

<sup>182</sup> European Commission (2007), 'Hotlines for Germany IBSDE', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/hotlines/germany/ibside/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/hotlines/germany/ibside/index_en.htm), accessed 20 November 2007

- glorify war or forward propaganda of illegal organisations; and
- offer content that is potentially illegal or threatens children and under Articles 5 of the *Jugendmedienschutz-Staatsvertrag [Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia]* (JMStV)<sup>183</sup>.

FSM also supports industry self-regulation of the internet through an internet code of practice<sup>184</sup>, outlined above.

In 1998, Childnet International's report under the EU's Daphne Programme proposed that internet hotlines should work more cooperatively, and explored how:

- hotlines could work more closely in a network;
- a network of hotlines would best be organised and funded; and
- hotlines could be established in countries where they did not yet exist<sup>185</sup>.

Building on this work, in 1999 the European Commission called for proposals to establish a European network of hotlines as part of the SIAP. In particular, the commission highlighted the need to establish effective hotline reporting mechanisms in cooperation with law enforcement authorities, who would remain responsible for prosecution of illegal content providers<sup>186</sup>.

As a result, the INHOPE network of hotlines was formed to enable hotlines that dealt with child pornography and other illegal material on the internet to meet, share knowledge and discuss common issues of concern<sup>187</sup>. Founding INHOPE hotlines included the three German hotlines, the IWF, Meldpunt, and the Austrian and French hotlines. However, non-EU countries with hotlines, such as the US and Australia, were also able to participate as associate members.

### Role of INHOPE hotlines

INHOPE hotlines investigate complaints from the public about potentially illegal internet content. The definition of illegal internet content varies from country to country and hotlines work within the legislation of the country where they operate. If the content is hosted locally, the complaints are referred to the industry so that the content can be taken down. If necessary, the content is referred to law enforcement agencies or authorities for prosecution. Where the content is hosted outside the country in which it is reported, it is referred to the

---

<sup>183</sup> Article 5 of *Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia*, art 5, 01.03.2007, [English Version], available at: [www.artikel5.de/gesetze/jmstv.html](http://www.artikel5.de/gesetze/jmstv.html)

<sup>184</sup> FSM (2007), 'Welcome to the FSM website', available at <http://fsm.de/en/>, accessed 16 October 2007.

<sup>185</sup> Childnet International (1998) *Actions in Preparation for a future Action Plan on promoting safe use of the internet* [PREP ACT Lot 1 – Hotlines], available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/PREP-ACT\\_1\\_final\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/PREP-ACT_1_final_report.pdf), accessed 21 November 2007

<sup>186</sup> *Final Evaluation of the implementation of the multiannual Community Action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions*, COM(2006) 663 final 6.11.2006, available at [http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_evaluation/comm\\_final\\_eval\\_siap\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_evaluation/comm_final_eval_siap_en.pdf)

<sup>187</sup> INHOPE, (2007), History of INHOPE, available at: <https://www.inhope.org/en/about/history.html>, accessed 6 November 2007



INHOPE member hotline in the host country for action or, if there is no INHOPE hotline, it is referred directly to a law enforcement agency or authority.

To qualify for membership, hotlines must have an effective, transparent mechanism for responding to complaints. While they may be established by government, industry or private organisations, they must have the support of government, industry, law enforcement agencies and authorities, and internet users in the country<sup>188</sup> where they operate.

To achieve its mission of ‘ensuring swift action is taken in responding to reports of illegal content to make the internet a safer place’<sup>189</sup>, INHOPE fosters cooperation between its members and between the hotlines and key stakeholders, including law enforcement agencies, government, and policy-makers. Further, INHOPE seeks to raise awareness about its member hotlines as ‘one stop shops’ for global reports of illegal content from around the world, and encourages non-member hotlines to join the INHOPE network.

The review of the SIAP in 2003 highlighted as a success the establishment of the INHOPE network<sup>190</sup>. As a consequence, a focus of the SIAP extension in 2003–04 was to expand the network of hotlines with funding directed to the establishment of new hotlines and the consolidation of early hotlines<sup>191</sup>. With European Commission funding from the SIAP, the INHOPE network has expanded to include almost all EU member states, and has been recognised as one of the main achievements of the EU’s programs—the network of hotlines could not have been achieved without EU funding<sup>192</sup>. In addition, following an amendment to the INHOPE constitution in 2004, non-EU members were able to become full members (although they were not eligible to receive funding from the EU).

In 2005, with the establishment of the SIP program, emphasis on consolidating and extending the geographical coverage of the hotlines and cooperation between INHOPE members was maintained<sup>193</sup>. In addition, financial support for the INHOPE network was provided by industry partner Microsoft in 2006<sup>194</sup>.

From its origins as an EU project, INHOPE has expanded to include hotlines in Australia, Austria, Belgium, Bulgaria, Canada, Chinese Taipei, Cyprus, the Czech Republic, Denmark,

---

<sup>188</sup> INHOPE (2007), ‘Membership’, available at: <https://www.inhope.org/en/about/members.html>, accessed 6 November 2007

<sup>189</sup> INHOPE (2007), ‘Mission and Objectives of INHOPE’, available at: [www.inhope.org/en/about/mission.html](http://www.inhope.org/en/about/mission.html), accessed 6 November 2007

<sup>190</sup> Technopolis (2003), *The Evaluation of the Safer Internet Action Plan 1999-2002*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/reports/evaluation\\_safer\\_internet\\_full\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/reports/evaluation_safer_internet_full_report.pdf), accessed 10 November 2007

<sup>191</sup> *Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, O.J. L162/1 01.07.2003, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l\\_162/l\\_16220030701en00010004.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_162/l_16220030701en00010004.pdf)

<sup>192</sup> *Final Evaluation of the implementation of the multiannual Community Action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*. COM(2006) 663 final 6.11.2006, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_evaluation/comm\\_final\\_eval\\_siap\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_evaluation/comm_final_eval_siap_en.pdf)

<sup>193</sup> *Communication on the implementation of the multiannual Community Programme on promoting the safer use of the Internet and new online technologies (Safer Internet Plus)*, COM(2006) 661 final 12.03.2004, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/si\\_plus/exante.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/si_plus/exante.pdf)

<sup>194</sup> INHOPE (2007), ‘Partners’, available at: [www.inhope.org/en/partners/partners.html](http://www.inhope.org/en/partners/partners.html), accessed 22 November 2007

Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Malta, the Netherlands, Poland, Portugal, Slovenia, South Korea, Spain, the UK and the US.

Cooperation between members of INHOPE has facilitated the removal of illegal content from the internet and avoided the ‘difficulties in the complex diplomatic procedures necessary for cross border cooperation of law enforcement authorities’<sup>195</sup>. The expansion of the INHOPE network to 27 countries with a total of 30 hotlines facilitates this process and INHOPE’s recent Global Internet Trend Report found that 9,600 confirmed reports of child pornography were processed per month by member hotlines<sup>196</sup>.

## **Spam hotline**

In Germany, complaints about spam are directed to the industry organisation eco, which distinguishes between spam that contains potentially illegal content, which is referred to the Bundeskriminalamt, the German federal police, and other unsolicited messages, which are addressed by the hotline. eco takes enforcement action against parties located in Germany including the sender of the spam, the website operator, the registrant of the domain and the ISP who hosts the content.

To facilitate an international approach to addressing spam, eco has recently launched its SpotSpam initiative. Established by eco’s Internet Content Task Force and Poland’s Naukowa i Akademicka Siec Komputerowa [Research and Academic Computer Network] in 2005, the initiative is funded under the EU’s SIP program and aims to facilitate international legal action against those who send illegal electronic communication, including spam and phishing<sup>197</sup>. SpotSpam responds to spam complaints and where appropriate:

- issues cease and desist orders;
- issues administrative fines; and
- supports criminal prosecution against those who continue to produce spam.

To do this, SpotSpam receives complaints about spam from internet users through Spamboxes located in partner countries. The Spamboxes are a contact point for complainants in the local language; these complaints are then collated into a central SpotSpam data base. The information in this database is then used to enable enforcement authorities to act against spammers both locally and through collaboration with other spam hotlines on an international level<sup>198</sup>.

## **HELPLINES**

The INHOPE hotlines have achieved success at local levels and in a coordinated fashion across Europe in combating illegal content, principally child pornography. However, there remains a task to address the harm that can be caused to children’s development when they

---

<sup>195</sup> Waltermann, J. and Machill, M. (Eds) (2000), *Protecting our Children on the Internet: Towards a New Culture of Responsibility*, Gutersloh: Bertelsmann Foundation Publishers, p. 30

<sup>196</sup> INHOPE (2007), ‘INHOPE publish landmark Global Internet Trend Report - 9,600 reports of child pornography processed per month’, [Media release] 19 September 2007, available at: [www.inhope.org/en/node/296](http://www.inhope.org/en/node/296), accessed 22 November 2007

<sup>197</sup> eco (2007), ‘Goals – Enforcement and Threat Assessment’, available at: [www.spotspam/goals.net/](http://www.spotspam/goals.net/), accessed 21 November 2007

<sup>198</sup> eco (2007), Goals: Enforcement and Threat Assessment, available at: [www.spotspam.net/goals.html](http://www.spotspam.net/goals.html), accessed 19 November 2007

encounter internet content that is unsuitable for their age or have contact with threatening or predatory people through the internet.

A new initiative of the SIP program, introduced in 2006, seeks to address this concern through actions at the national level in member states. As part of the EU's awareness-raising program, INSAFE, member states were invited to apply for funding to establish internet helplines—or to cooperate with existing national helplines—to respond to the questions and concerns of young people linked to their experiences online or the harmful or illegal online content they encounter<sup>199</sup>. As of August 2007, a total of 10 helplines in Austria, the Czech Republic, Denmark, Finland, Iceland, Ireland, Luxembourg, Poland, Slovakia and Sweden have been provided with financial support<sup>200</sup>.

At the European level, SIP has enhanced work in this area through Europe Direct, a Europe-wide helpline<sup>201</sup>, established in 2005 to offer European citizens practical information about a broad range of topics, including advice on how to use the internet more safely<sup>202</sup>.

## AWARENESS INITIATIVES

The EU's preference for online safety initiatives that are guided at the European level but developed and implemented at national and local levels, and for coordination of these initiatives through pan-European networks, is most clearly perceived in its approach to enhancing children's and parents' awareness of online risks and mitigation strategies.

Online safety education in EU member states is supplemented and supported through the INSAFE program. The program provides a parallel function to the INHOPE program by coordinating activities in EU member countries and sharing information. The INSAFE program coordinates awareness-raising in each member country through bodies that implement awareness campaigns at a national level, referred to as 'nodes'. INSAFE informs program deployment in member states and draws from member states' experiences and outcomes, using collaboration and information-sharing as a tool to continuously improve the information being provided to European citizens.

The network promotes shared responsibility for online safety by government, educators, parents, media, and industry. INSAFE nodes, including the Child Exploitation and Online Protection Centre (CEOP) formed in the UK in April 2006 and Klicksafe.de established in Germany two years earlier, monitor and address emerging trends and risks, while seeking to raise awareness of internet safety among users and reinforce the image of the internet as a place to learn.

---

<sup>199</sup> European Commission (2007), *Call for proposals for indirect actions under the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet Plus)*, [2006], available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/call\\_2006/call\\_announcement\\_2006/sip\\_call\\_announcement\\_2006\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/call_2006/call_announcement_2006/sip_call_announcement_2006_en.pdf)

<sup>200</sup> European Commission (2007), 'Safer Internet Plus: Helplines: Helpline running projects', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/helplines/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/helplines/index_en.htm), accessed 22 November 2007

<sup>201</sup> For more information about Europe Direct, see [http://ec.europa.eu/europedirect/index\\_en.htm](http://ec.europa.eu/europedirect/index_en.htm).

<sup>202</sup> *Communication on the implementation of the multiannual Community Programme on promoting the safer use of the Internet and new online technologies (Safer Internet Plus)*, COM(2006) 661 final 6.1.2006, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006\\_0661en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0661en01.pdf)

### **Educaunet**

In 2001, SIAP provided €495,000 in funding for the development of 'Educaunet,' an education program to help children in France and Belgium develop 'an autonomous, responsible attitude in their use of the Internet'<sup>203</sup>. Educaunet has proved to be a key initiative in the safety arena and, in 2002, a further €840,000 in funding aided the expansion of the program to a total of seven European countries: Austria, Belgium, France, Denmark, Greece, Portugal and the UK<sup>204</sup>. This expansion is an example of the EU commitment to use information developed by organisations within its member states and to make it widely available, rather than developing education programs afresh in each jurisdiction<sup>205</sup>.

#### **Educaunet**

The Educaunet program continues to train young people to 'take an independent, critical and responsible approach'<sup>206</sup> to use of the internet through balanced, age-appropriate activities. In the United Kingdom the program is cross-referenced with the English National Curriculum in England and Wales, which contains a mandatory requirement to study media texts, in the context of the wider literacy curriculum.

Activities available through Educaunet address content, contact and e-security issues and include:

- Treasure Hunt—a quiz for 8–12 year-olds aimed at developing efficient ways to use search engines.
- Make your own internet Charter—an activity for 9–14 year-olds in which participants evaluate advice documents and develop a charter for internet use at home and/or school.
- Quest on the Web—a research activity for 12–18 year-olds aimed at developing critical skills for evaluating information collected from the internet.
- Truth or Rumour?—an activity for 12–18 year-olds in which participants evaluate rumours and hoaxes found on the internet.
- Guess Who—an online game for 8–16 year-olds in which participants enter a closed chatroom using a false identity and guess the identities of their peers.
- E-Commerce—an activity for 14–16 year olds aimed at developing abilities to become critical consumers of internet content.

The activities are designed to both increase skills—such as internet navigation, and assessment of information quality and bias—and encourage users to 'observe' themselves as users and question the content choices they make when faced with online content and communication choices.

---

<sup>203</sup> European Commission (2002), 'Educaunet,' *European Commission, Information Society Thematic Portal*, available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/awareness/closed\\_projects/educaunet/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/awareness/closed_projects/educaunet/index_en.htm), accessed 21 November 2007

<sup>204</sup> Educaunet Consortium (2004), *Educaunet: Final Report October 1 2002-July 31 2004*, p. 2, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/educaunet2\\_final\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/educaunet2_final_report.pdf), accessed 21 November 2007

<sup>205</sup> Technopolis (2003), 'Executive Summary' *The Evaluation of the Safer Internet Action Plan 1999-2002*, European Commission DG Information Society, Luxembourg, p. 5, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/reports/evaluation\\_safer\\_internet\\_exec\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/reports/evaluation_safer_internet_exec_report.pdf), accessed 21 November 2007

<sup>206</sup> Educaunet (2007), 'Risk and the Internet', available at: [www.educaunet.org/eng/](http://www.educaunet.org/eng/), accessed 20 October 2007

Educaunet is based on the premise that as users gradually attain confidence in the various uses of the internet they will acquire the skills to better identify potential risks. In addition, the incremental exposure to different risks, as part of a process of increasing awareness, will facilitate users' ability to appropriately address risks that they encounter. The program aids children to develop multiple skills, including the application of critical awareness to determine if content is 'appropriate' according to their own values and judgment.

In 2003 when the SIAP program was extended for a further two years, the focus within the program on education programs was extended and the proportion of SIAP funding devoted to education and awareness functions was increased. In particular, the EU emphasised its commitment to providing a coordination role in online safety awareness activities.

The purpose of the Community support is to pump-prime broadly-based awareness actions and to provide overall coordination and exchange of experience so that lessons can be drawn from the results of the action on an ongoing basis (for instance by adapting the material distributed)<sup>207</sup>.

#### **Klicksafe.de**

Klicksafe.de is a joint German government and industry initiative commissioned to raise public awareness of internet safety<sup>208</sup>. Established in 2004 as the German node of the INSAFE network, Klicksafe.de receives funding from the SIP Program (over €970,000 for the period 2007–08)<sup>209</sup>. A national marketing campaign undertaken by klicksafe.de in recent years has employed a variety of complementary strategies to raise public awareness, including a television advertisement, *Wo ist Klaus?* (Where's Klaus?).

#### ***Where's Klaus?***

The *Where's Klaus?* component of the Klicksafe.de campaign was aimed at raising awareness among children and their parents about risks associated with internet use including inappropriate content, illegal contact and e-security. Although the message it imparts is serious, the clip is engaging and has received international advertising awards.

The advertisement features a young boy's mother allowing a variety of people into her home, including right-wing extremists, pornographers and a character from a violent game. Each character is apparently responding to an invitation from her son, Klaus, who is presumably upstairs on the internet. A further character, a sexual predator, is then allowed by the mother to take her daughter away. The tagline: *In real life you would protect your children, so why not protect them on the internet?*

<sup>207</sup> Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, O.J. L162/1 1.7.2003, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/programmes/extension/extension\\_decision\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/programmes/extension/extension_decision_en.pdf)

<sup>208</sup> For more information about the Klicksafe.de program, see [www.klicksafe.de/common/english.php](http://www.klicksafe.de/common/english.php).

<sup>209</sup> European Commission (2007), 'Safer Internet Plus: Awareness Activities', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/awareness/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/awareness/index_en.htm), accessed 20 November 2007



The *Where's Klaus?* campaign has benefitted from viral distribution, which has vastly increased its reach. After the initial advertising campaign, the clip was requested by other television networks, presented multiple times as part of news media interest, and was posted on YouTube.com, where it has been viewed over 50,000 times<sup>210</sup>. Beyond Germany, *Where's Klaus?* has been broadcast on Austrian and Spanish television, and is available on the internet in several languages, including English, Dutch and French, extending its reach even further.



Image strip from *Where's Klaus?* [CTRL + click to play]<sup>211</sup>

To strengthen the delivery of the online safety message, Kicksafe.de has also developed a complementary program including directly approaching target groups, a training course for educators, and online safety events held regionally and nationally<sup>212</sup>.

The establishment of the SIP program in 2005 resulted in a change in the focus of online safety education and awareness activities for the EU. Alongside another increase in the proportion of funding allocated to awareness there is a particular emphasis on the importance of partnerships, dialogue and exchange of information and experiences in order to develop and improve online safety programs. This was particularly true in education and awareness programs, where the EU directed that INSAFE awareness-raising nodes should:

... establish and maintain a partnership (formal or informal) with key players (government agencies, press and media groups, ISP associations, user organisations, education stakeholders) and actions in their country relating to safer use of the Internet and new online technologies<sup>213</sup>.

### **Task force approaches to child protection on the internet**

The importance of a coordinated approach has steadily gained recognition with an influential example being the UK Home Office Task Force on Child Protection on the Internet (Task Force). The Task Force was established in March 2001 in response to concerns about contact risks to children online. It has worked through a number of sub-groups that focus on issues around the criminal law, law enforcement, training, industry standards and co-regulation, child protection measures, and education and awareness.

The Task Force has developed initiatives to promote safer use of the internet bringing together representatives from industry, service providers, law enforcement agencies, government and children's charities. The Task Force draws on the collective knowledge of its members and current research into children's use of online services. It uses this

<sup>210</sup> As at 15 October 2007—see [www.youtube.com/](http://www.youtube.com/)

<sup>211</sup> [http://a124.g.akamai.net/7/124/30915/v0001/gff.download.akamai.com/30915/klicksafe\\_english.mpg](http://a124.g.akamai.net/7/124/30915/v0001/gff.download.akamai.com/30915/klicksafe_english.mpg)

<sup>212</sup> [www.klicksafe.de](http://www.klicksafe.de)

<sup>213</sup> Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies, O.J. L149/1 11.06.2005, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_decision\\_2005/sip\\_decision\\_2005\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2005/sip_decision_2005_en.pdf)

knowledge base to establish the current risks to internet users and develop good practice guidance that helps inform online service providers about measures that can be taken to minimise those risks. Several of the guidelines developed by the Task Force focus on communications risks that have not been specifically addressed under the SIAP/SIP programs.

In 2005, the Task Force published the *Good Practice Guidance for Search Engine Providers and Advice to the Public on How to Search Safely* (Search Guidance) and the *Good Practice Guidance for the Moderation of Interactive Services for Children* (Moderation Guidance). In 2006, the Task Force began developing the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Social Networking Guidance). The guidance documents have benefited from the cooperation of members representing a range of interests and, in the case of the Social Networking Guidance, from an international approach to its development as services cross multiple jurisdictions.

The Search Guidance offers advice to search engine providers about making safety advice available to their users, blocking URLs that contain potentially illegal child abuse images, using the IWF blacklist, and enabling their users to report illegal or objectionable material they encounter via use of the search engine. It makes recommendations about the use of filters by search engine providers and the management of search services aimed at children, and image search.

The Moderation Guidance provides advice to service providers on addressing risks to children using interactive services such as online games and chat services. The guidance provides advice on how to assess risks to children using services, focusing on the moderation of interactive services and issues to consider when implementing moderation.

The Social Networking Guidance is currently being finalised. It provides a framework for addressing safety issues associated with the use of social networking and user interactive services. The Social Networking Guidance comprises:

- background information on issues associated with social networking and user interactive services;
- recommendations for implementation by service providers to minimise the risks to users; and
- information that can be incorporated into safety campaigns targeted to parents, carers and users of services.

### **E-security awareness**

A further example of the benefits of collaboration in addressing online risks is a German partnership between government, industry and non-government organisations, including INHOPE hotlines, FSM and eco, to produce an e-security education program. This program responds to a new focus on e-security risks by the EU under the SIP, following the release of the EU Directive on Privacy and Data protection in 2004. Launched in 2005, *Deutschland sicher im Netz* aims to increase awareness of e-security risks such as spam and viruses among internet users (particularly children), and the business and public sectors<sup>214</sup>.

---

<sup>214</sup> For more information about *Deutschland sicher im Netz*, see [www.sicher-im-netz.de](http://www.sicher-im-netz.de).

### Deutschland sicher im Netz – Germany Safe on the Net

*Deutschland sicher im Netz* (DSIN) is a multimedia campaign that centres on an e-security information website for children, parents and teachers. This site encourages parents and teachers to accompany children as they learn about safer internet behaviour through animated characters, interactive puzzles and games.



Rio



Nina



Ben

**Rio, Nina and Ben, three characters that guide young people through the DSIN child education site, [www.internauten.de](http://www.internauten.de).**

Other components of the DSIN program include media kits for primary schools, and information videos, posters, pens, stickers, cups and t-shirts on internet safety. In addition, DSIN distributes e-security checklist CDs at IT fairs and as free inserts cover-mounted on magazines.

DSIN provides online courses on e-security topics including phishing and online trading, and has set up a web academy that provides free online and offline seminars for adults, including university students<sup>215</sup>.

In 2005, a DSIN promotional truck tour across 18 locations in Germany gave users the opportunity to have their e-security questions answered, and to take part in integrated live security checks of computer equipment; these checks detected and removed viruses, trojans and spyware programs from equipment.

The introduction of the SIP program in 2005 also saw a specific emphasis from the EU on the targeting of messages to key groups such as children of particular ages, parents and teachers. Under the SIP, the EU specified that awareness raising programs should be targeted and use ‘the most appropriate media, taking into account best practice and experience in other countries’<sup>216</sup>.

### **Child Exploitation Online Protection Centre (CEOP)**

Launched in April 2006, the Child Exploitation Online Protection Centre (CEOP) focuses on addressing child sex abuse, offline and online, by working with local and international law enforcement authorities, industry, government, children’s charities and other interested organisations. It is the UK node for the INSAFE program with a role in research on

<sup>215</sup> Obert, T. (2005), ‘German Security Initiative ‘Germany safe on the Net’. A Best-Practice for Europe’, Paper delivered at the *ENISA Good Practice in Awareness Raising Workshop*, Brussels, 14 December 2005, available at: [www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_raising\\_the\\_security\\_bar.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_raising_the_security_bar.pdf), accessed 4 November 2007

<sup>216</sup> *Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies*, O.J. L149/1 11.06.2005, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_decision\\_2005/sip\\_decision\\_2005\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2005/sip_decision_2005_en.pdf)



children's internet usage<sup>217</sup> and in developing education programs for children, parents and educators<sup>218</sup>.

CEOP's *Think U Know*<sup>219</sup> is the cornerstone of its education program for young children, teenagers, their parents and educators.

#### Think U Know

The *Think U Know* website includes downloadable information and videos, each tailored to a target audience. The materials for children are presented in three age groups<sup>220</sup>, from the very young to teenagers, and include information on how to have fun and stay safe online and how to report unwanted contact and content.

- Children aged 8–11 are provided with a interactive game, which offers safety information in a cybercafe-style environment.
- Young people aged 12–16 are invited to complete surveys and join the CEOP Youth Advisory Panel which assists CEOP and law enforcement agencies communicate more effectively with young people, including through the website.
- Parents are supported through a separate section that offers hints through an easy-to read guidance sheet on how to discuss internet safety with children. The parents' information web page also provides information on assisting children to adopt safe practices in all online applications, including peer-to-peer, gaming, chat and social networking.
- Teachers are provided with detailed lesson plans and teaching hints, to encourage them to introduce internet safety into the school curriculum from early primary to senior high school. These materials are complemented with training seminars held regularly across the UK to maximise the effectiveness of the teaching program.
- Following the first evaluation of the SIP program in 2006, which recommended that education programs should focus more on children under 10 years<sup>221</sup>, CEOP will be introducing a new section devoted to five to seven year olds, from February 2008<sup>222</sup>.

A new education and awareness campaign aimed at children, teachers, parents and carers is currently being developed and, by 30 June 2009, CEOP aims to have delivered internet safety resources into every primary and secondary school in the UK.

#### Childnet International

Know IT All is an interactive education program to assist in the understanding a broad range of issues associated with using the internet or a mobile phone. Produced by children's internet charity Childnet International, with funding and support from MSN UK, Microsoft and the Virtual Global Taskforce, Know IT All aims to help young people 'reflect on their

<sup>217</sup> CEOP (2007), 'Survey for 11–16 year olds', available at: [www.thinkuknow.co.uk/11\\_16/survey.aspx](http://www.thinkuknow.co.uk/11_16/survey.aspx), accessed 16 November 2007

<sup>218</sup> Insafe (2007), 'United Kingdom EMPOWER', available at: [www.saferinternet.org/ww/en/pub/insafe/focus/uk.htm](http://www.saferinternet.org/ww/en/pub/insafe/focus/uk.htm), accessed 16 November 2007

<sup>219</sup> For more information on CEOP's *Thinkuknow* program, see [www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/).

<sup>220</sup> An information section for 5–8 year olds is currently under development, to be launched in 2008, see [www.thinkuknow.co.uk/5\\_7/](http://www.thinkuknow.co.uk/5_7/), accessed 16 November 2007

<sup>221</sup> *Communication on the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet Plus)*, COM(2006) 661 final 6.11.2006, p. 5, available at:

[http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_evaluation/impl\\_report\\_sipp\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_evaluation/impl_report_sipp_en.pdf)

<sup>222</sup> See: [www.thinkuknow.co.uk/5\\_7/](http://www.thinkuknow.co.uk/5_7/).

own use of communication technology, be aware of the dangers and develop safe and discriminating behaviour when using new technology'<sup>223</sup>.

### Know IT All

Childnet International provides resources targeted at a diverse range of audiences in the UK, from educators and parents, to young children and teenagers. Education programs are tailored, maximising their effectiveness by taking into account the needs and communication preferences of each audience.

Childnet's Know IT All program was first launched as a CD-ROM, which was provided to all secondary schools in the UK in 2005. It was targeted at teenagers, covering a range of issues, including bullying and 'stranger danger' and included a teacher's guide. This schools program included a volunteer education program, in which volunteers from Microsoft and the UK police were trained to present the program to schools<sup>224</sup>.



**Know IT All for Parents, with talking video narrator to guide users through the program.**

Following the success of this program, the UK government commissioned Childnet International to expand the program<sup>225</sup>:

<sup>223</sup> Childnet International (2007), 'Overview of Know IT All', available at: [www.childnet-int.org/kia/overview.aspx](http://www.childnet-int.org/kia/overview.aspx), accessed 13 December 2007

<sup>224</sup> Childnet International (2005), 'About KIA,' available at: [www.childnet-int.org/kia/about/](http://www.childnet-int.org/kia/about/), accessed 22 November 2007

<sup>225</sup> Childnet International (2005), 'About KIA,' available at: [www.childnet-int.org/kia/about/](http://www.childnet-int.org/kia/about/), accessed 22 November 2007

- Know IT All for Parents is a series of video and text-based guides prepared to assist guardians to broaden their knowledge of information technology so that they can 'help children stay safe online'<sup>226</sup>. The program was based on research that showed that parents need specifically targeted activities for the information to reach them<sup>227</sup>.
- The Know IT All materials have been made available English and other community languages, including Arabic, Bengali, Gujarati, Mandarin, Polish, Punjabi, Urdu and the UK sign language, and has a video narrator, which is helpful for those with literacy and technical challenges (Figure 2).

The program has been developed by a cooperative effort between education, law enforcement, industry and government sectors. Independent evaluation of Know IT All has shown the program to be a success with volunteers, teachers and students<sup>228</sup>. Feedback from parents who had attended the school-based program has also been positive, participants reporting that they have 'learnt a great deal from the experience'<sup>229</sup>.

As discussed in Chapter 2, changes to internet technologies and the way they are used have consequent impacts for the range of risks for families online. As risks emerge, industry participants and online safety groups have moved to develop new programs and messages to keep pace with these changes.

As it became clear to the mobile industry in the UK that children were increasingly at risk from emerging mobile phone technologies, including mobile access to the internet, Vodafone UK developed a booklet in partnership with the National Family and Parenting Institute, a UK charity that promotes the welfare of children and their families. The booklet was designed to provide parents with information about new mobile services, including access to the internet. The booklet, entitled *Staying in Touch: A Parent's Guide to Mobile Phones*, and released in 2006, includes background information on specific services and includes tips for parents about how they can discuss mobile services with their child<sup>230</sup>.

In response to concerns about the increase in risks associated with use of the internet for communication in 2007, Childnet International released a package of cyber-bullying resources, *Let's Fight it Together*, which raises awareness and provides support and education about the problem of cyber-bullying<sup>231</sup>.

---

<sup>226</sup> For more information about this program, see [www.childnet-int.org/kia/parents/cd/textVersion/parents/index.html](http://www.childnet-int.org/kia/parents/cd/textVersion/parents/index.html).

<sup>227</sup> Wishart, J., Andrews, J. and Wan, C.Y. (2006), 'Evaluation of the 'Getting to Know IT All' presentation as delivered in UK schools during November 2005', University of Bristol, available at: [www.childnet-int.org/downloads/gtkiaEvaluation.pdf](http://www.childnet-int.org/downloads/gtkiaEvaluation.pdf), accessed 22 November 2007

<sup>228</sup> One hundred per cent of volunteers and 98 per cent of teachers said they would recommend the program to a colleague, and more than 80 per cent of students reported an intention to act on the advice provided by the Know IT All program (see [www.childnet-int.org/downloads/gtkiaEvaluation.pdf](http://www.childnet-int.org/downloads/gtkiaEvaluation.pdf)).

<sup>229</sup> Wishart, J., Andrews, J. and Wan, C.Y. (2006), 'Evaluation of the 'Getting to Know IT All' presentation as delivered in UK school s during November 2005', University of Bristol, p. 10, available at: [www.childnet-int.org/downloads/gtkiaEvaluation.pdf](http://www.childnet-int.org/downloads/gtkiaEvaluation.pdf), accessed 22 November 2007

<sup>230</sup> Vodafone (2006), *Staying in Touch: A Parent's Guide to Mobile Phones*, [brochure], available at: [www.familyandparenting.org/Filestore/Documents/publications/A5\\_Parents\\_Guide\\_to\\_Mobile\\_Phones.pdf](http://www.familyandparenting.org/Filestore/Documents/publications/A5_Parents_Guide_to_Mobile_Phones.pdf)

<sup>231</sup> Digizen (2007), *Let's Fight it Together: Cyberbullying Film*, available at: [www.digizen.org/cyberbullying/film.aspx](http://www.digizen.org/cyberbullying/film.aspx), accessed 28 November 2007

### Cyberbullying – Let's Fight it Together

Let's Fight it Together is centred on a video story about a teenage boy, Joe, who is tormented by his fellow students at a UK high school. The film depicts the boy receiving abusive messages over a range of communication technologies, including MSN, mobile text, emails, SNS and crank calls.

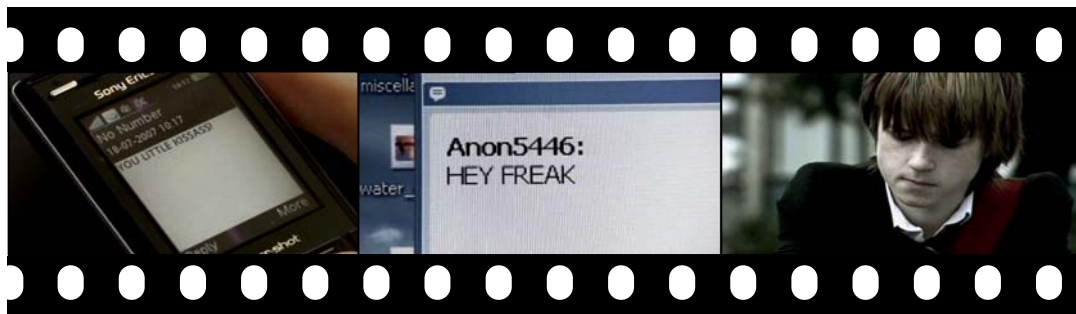


Image strip from *Let's Fight it Together* [CTRL + click to play]<sup>232</sup>

Importantly, the story follows the impact of cyber-bullying, such as social withdrawal of the victim, loss of self esteem and heightened anxiety. Further, the film shows the positive response by adults who are eventually told of the cyber-bullying, and hints at the potential impact of the behaviour on the bully herself, the police arriving to question her at school.

In addition to the film, downloadable video interviews with the primary characters—the bully, the victim, the victim's teacher, the victim's mother and a bystander—provide teenagers and adults with genuine insight into the impacts of bullying behaviour. The click-and-play presentation style used in these materials renders this program simple and attractive to both young children and their guardians.

The film is also supported by teaching materials, which are distributed through downloads and by hardcopy post. The organisation aims to distribute the package to every secondary school across the UK by the end of November 2007.

## Evaluations

In September 2007, INHOPE released the findings from 'the first detailed analysis of illegal activity on the internet'<sup>233</sup>, a statistical analysis over 28 months and more than 25 countries as its first step towards a global action plan to eradicate illegal activity from the internet. It found that, between September 2004 and December 2006:

- the INHOPE network received 900,000 reports from the general public;
- in total, INHOPE processed 1.9 million reports; and
- 160,000 reports were forwarded to law enforcement agencies for action—an average of 5,800 per month.
- 20,000 per month or 21 per cent of all processed reports were about illegal or harmful content;
- 50 per cent of these contained child pornography;

<sup>232</sup> [www.digizen.org/cyberbullying/fullFilm.aspx](http://www.digizen.org/cyberbullying/fullFilm.aspx)

<sup>233</sup> INHOPE (2007), 'INHOPE publish landmark Global Internet Trend Report – 9,600 reports of child pornography processed per month' [Media Release] 19 September 2007, available at: [www.inhope.org/en/node/296](http://www.inhope.org/en/node/296), accessed 22 November 2006

- 19 per cent of these contained other child-related content;
- 28 per cent of these contained adult pornography;
- child pornography grew by 15 per cent per year;
- adult pornography grew by 24 per cent per year; and
- racism and xenophobia grew by 33 per cent per year.

While INHOPE is regarded internationally as successful, it notes that when illegal content such as child pornography is reported to a hotline it is not unusual for it to transcend traditional national boundaries. It is therefore crucial that swift action continues to be taken to make the internet a safer place.

The UK also maintains a close interest in the success of its initiatives and its Prime Minister announced in September 2007 that Dr Tanya Byron, consultant clinical psychologist, will conduct an independent review of the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games. Comment is specifically being sought from children on the issues.

The review is supported by officials from the Department for Children, Schools and Families and the Department for Culture Media and Sport, which have released documentation, including consultation papers, and calls for evidence from adults<sup>234</sup> and children<sup>235</sup>. The review is due to report in March 2008.

The objectives of this review are:

- to undertake a review of the evidence on risks to children's safety and wellbeing of exposure to potentially harmful or inappropriate material on the internet and in video games; and
- to assess the effectiveness and adequacy of existing measures to help prevent children from being exposed to such material and help parents understand and manage the risks of access to inappropriate content, and to make recommendations for improvements or additional action.

The inquiry will look at:

- benefits and opportunities;
- understanding the potential risks;
- helping children, young people and parents manage the risks; and
- need and potential for improvement and change.

More generally, over the past decade, internet safety initiatives have burgeoned with governments, industry, law enforcement, NGOs and users increasingly focusing on ways to address content, contact and e-security concerns. Countries such as the UK and Germany responded early to these risks and have both influenced and been influenced by the EU's comprehensive and integrated programmatic approach when developing activities and

---

<sup>234</sup> Department for Children Schools and Families (2007), 'The Byron Review – Call for Evidence: Adult Version', available at: [www.dfes.gov.uk/byronreview/](http://www.dfes.gov.uk/byronreview/), accessed 22 November 2007

<sup>235</sup> Department for Children Schools and Families (2007), 'The Byron Review – Call for Evidence: Child and Young Person's Version', available at: [www.dfes.gov.uk/consultations/conDetails.cfm?consultationId=1511](http://www.dfes.gov.uk/consultations/conDetails.cfm?consultationId=1511), accessed 22 November 2007

partnerships. However, the area remains under scrutiny. It is the EU's practice to have its programs formally and independently evaluated. These evaluations are then used to refine the programs to ensure that they meet the needs of the European community.

## Chapter 5: Trends and observations

This report has provided an overview of the development of internet technologies and use, measures that have been used to promote online safety and examples of how those measures have been deployed in the European Union, particularly the UK and Germany. This chapter will highlight the trends identified in the preceding chapters and provide some observations on how online risks have been addressed in other jurisdictions.

### ONLINE RISKS

Developments in internet technologies, services and applications over the past 15 years have brought both benefits and risks to users. Initial concerns about online risks focused on static content. While perceptions and attitudes to risk may vary from country to country for cultural reasons, the risks to users have broadened and can be categorised into content, communication and e-security risks.

Given the global nature of the medium, Australian users experience both the benefits and the risks. In Australia, there has on the one hand been a strong increase in use of IM in the past two years, on the other there has been a decrease in the use of email as users increasingly employ social networking sites for communication with peers. Such changes in use of online services have the potential to increase risk of contact by adults with a sexual interest in children, and allow young people to post personal information online that may enable predators to track them.

As access to high bandwidth has become commonplace and developments in online technologies facilitate the production of content by users, young people have reduced their consumption of static internet content in favour of Web 2.0 sites and applications given the opportunities they offer for communication and interactive and user-generated content. This has increased availability of personal information online. **The risks to Australian youth are primarily the risks that are associated with Web 2.0 services—potential contact by sexual predators, cyber-bullying by peers and misuse of personal information.**

The availability of personal information on the internet also presents issues for adults in terms of privacy and e-security, particularly in terms of economic interests.

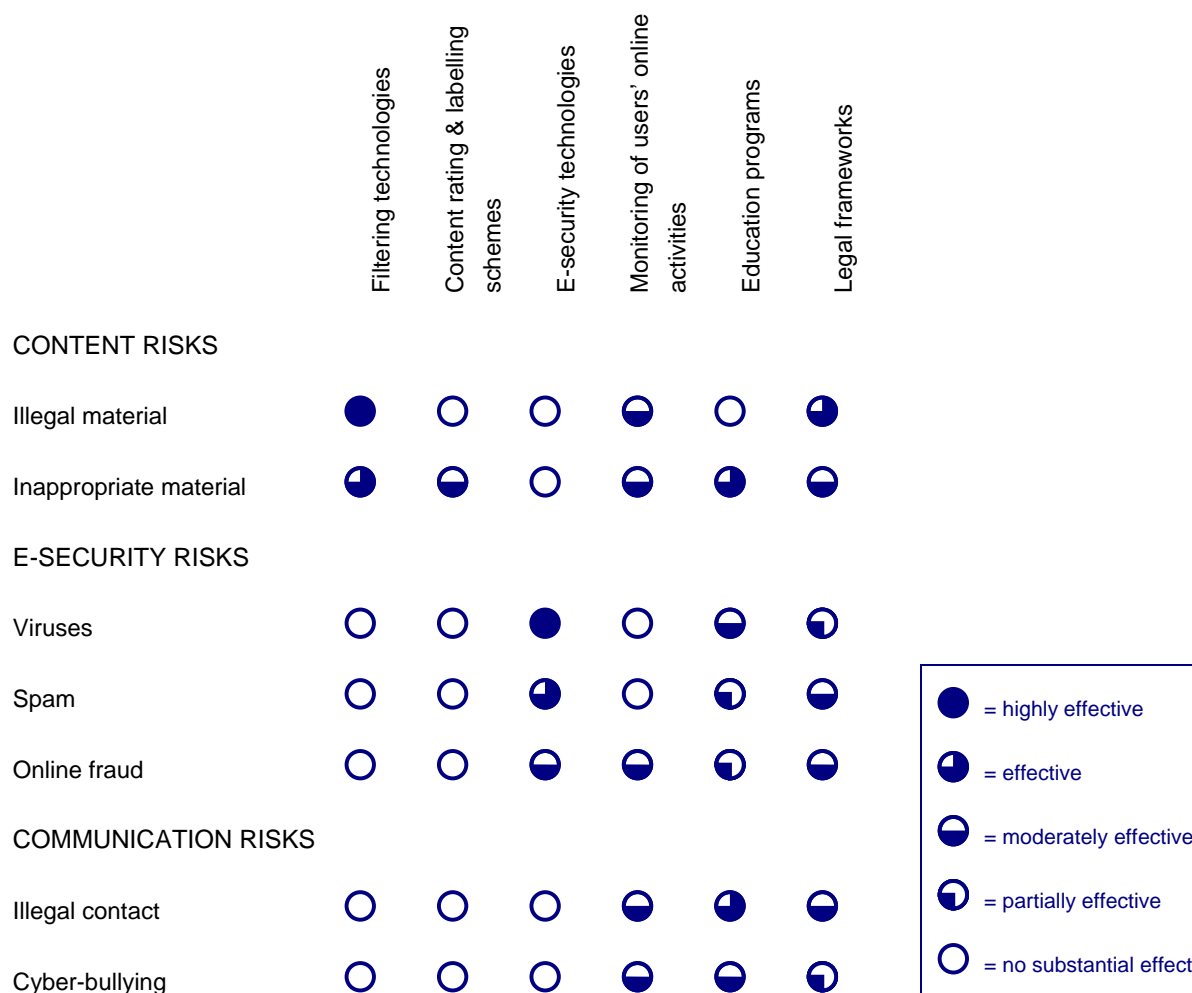
### METHODS FOR REDUCING RISKS TO USERS

Each risk mitigation measure discussed in this report has strengths and limitations, and varying levels of efficacy in addressing the risks identified in Chapter 2. For example, home computer filters can be useful in managing the kinds of content accessed by young children, while education programs can be effective in raising awareness of risks, empowering users and embedding safe internet usage behaviours in teenagers. Figure 5.1 summarises the



relative effectiveness of the online safety measures discussed in this report in addressing online risks.

**Figure 5.1: Effectiveness of measures in addressing risks**



**Internet content filtering has particular effect in preventing access to illegal content**, such as child pornography. When implemented for this purpose, filters use purpose-specific indexes, compiled by internet hotlines such as IWF. Filtering of this content was first implemented in the UK and involves minimal performance impacts.

**Filtering is also effective for managing access to inappropriate content**, particularly for younger users. Filters may be deployed by parents on home computers, in enterprises such as schools and public libraries, by ISPs, by mobile service providers, by third party providers and in search engines. Filters used for this purpose may enable parents or administrators to configure the filter according to their own values or the age of their child. When deployed by ISPs, the different filtering policies of each user can potentially introduce performance impacts.

Content filtering does not appear to have the same level of effectiveness in addressing the risks associated with the use of interactive content services. Filters are suited to blocking access to static web content and are able to completely block access to IM and chat



applications. However, **filters are currently unable to filter the content of communication between users using IM or chat services**. Moreover, as filters either block requests for content, or prevent particular content from being delivered to a user, they cannot prevent children and young people from uploading content to social networking and other user-generated content sites that are popular with Australian users.

Some filter vendors supplement home-based products by incorporating parental control software into filtering packages. Parental control software offers functions including monitoring and reporting tools. **Parental control software enables parents to monitor their children's use of IM and chat services and can alert them to particular risks**, for example, the release of personal information about a child such as home address or phone number. However, the usefulness of parental control software relies on parents checking logs regularly, engaging with their children about the type of services they access online and providing relevant advice on how to stay safe. It cannot prevent the release of personal information.

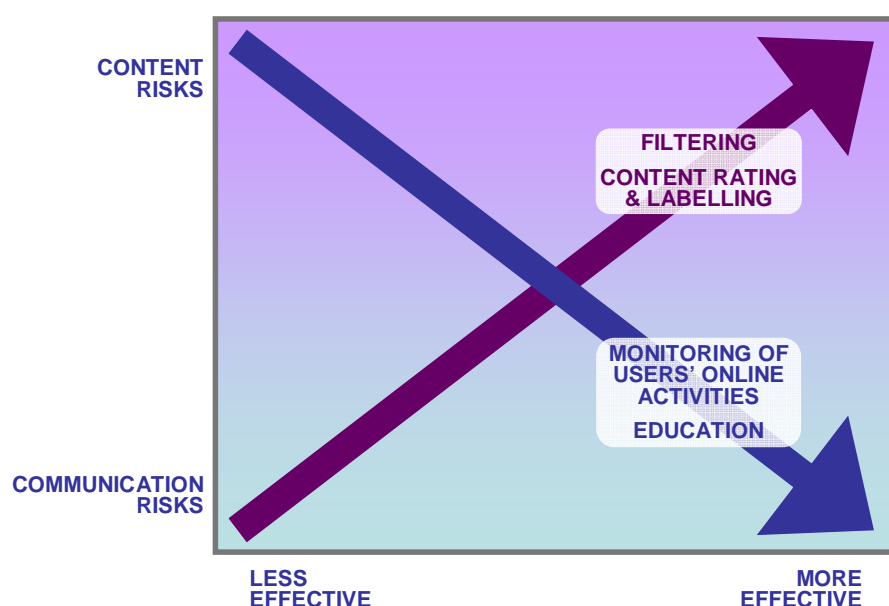
Education campaigns appear to be effective in addressing a broad range of online risks. Of the range of alternative risk mitigation measures, **education is the most effective method of addressing risks associated with illegal contact online**. Education is a viable alternative or supplement to filtering in targeting risks associated with inappropriate content, particularly for older children who may endeavour to circumvent filtering that they perceive to be restrictive. There is evidence from programs deployed in other countries that **education can be deployed to address bullying**. However, there is little evidence that educational measures contribute significantly to addressing risks associated with illegal content. Education can also be deployed to address e-security risks by developing self-protective behaviour for dealing with spam, viruses and online fraud.

The effectiveness of education initiatives depends on a number of factors, particularly the ability of the message to resonate with the target audience. To increase their effectiveness, **education initiatives are best underpinned by research** into children and young people's use of online services, children's risk profiles, appropriate safety messages and the most appropriate methods to disseminate information to the target audience.

ACMA has observed, from the study of online risks and risk mitigation strategies and the European Union case study presented in this report, that there is no single mitigation measure that is effective against all online risks. Neither is there a single mitigation measure that is effective in addressing even one category of online risks, that is, content risks, e-security risks and communication risks.

Focusing on content risks and communication risks, it is evident to ACMA that **certain clusters of mitigation measures tend to be more effective against one or the other category of online risks**. As illustrated in Figure 5.2, measures that centre on filtering and content rating and labelling are more usually effective against content risks. By contrast, measures which centre on monitoring of users' online activities and education are usually more effective against communication risks and risks associated with interactive services.

Figure 5.2: Clusters of measures to promote online safety



Children and young people in Australia today increasingly engage with Web 2.0 content, socialise with friends online and share content that they have generated themselves. These activities can be positive and constructive for Australian children and young people, and assist them in engaging with and building the new digital economy. Accordingly, the new online risks associated with these activities require different approaches to those targeting the predominantly content-based risks that have dominated concerns about the online environment.

Measures have been used internationally to address the range of online risks—content, contact and e-security. However, currently available software tends to address either content risks or e-security risks and does not address contact risks adequately due to limitations in filtering the content of communication between users. From ACMA’s research, there appears to be a gap in fulfilling consumer demand for multi-purpose filters that addresses all of these risks. The research also shows how the coordination of education campaigns across jurisdictions can benefit children, who can then access both content and information about online safety locally or globally, as well as educators, who can collaborate and exchange information on effective strategies for mitigating online risks.

# Appendix A: Direction to ACMA



**Australian Government**  

---

**Department of Communications,  
Information Technology and the Arts**

**Commonwealth of Australia**

*Australian Communications and Media Authority Act 2005*

## **PROTECTING AUSTRALIAN FAMILIES ONLINE DIRECTION NO. 2 of 2007**

I, HELEN LLOYD COONAN, Minister for Communications, Information Technology and the Arts, make the following Direction under section 171 of the *Broadcasting Services Act 1992*.

Dated 9/6 2007.

HELEN LLOYD COONAN

Minister for Communications, Information Technology and the Arts

---

### **1 Name of Direction**

This Direction may be cited as the *Protecting Australian Families Online Direction No. 2 of 2007*.

## **2 Definitions**

In this Direction:

**ACMA** means the Australian Communications and Media Authority;

**Internet service provider** (*ISP*) means a carriage service provider that supplies a service that enables the public to access the Internet.

**Carriage service provider** has the same meaning as in section 87 of the *Telecommunications Act 1997*.

## **3 Direction to investigate developments and report**

3.1 ACMA must investigate developments in Internet content filtering technologies and other safety initiatives to protect consumers, including minors, who access content on the Internet.

3.2 ACMA must report its findings to the Minister for Communications, Information Technology and the Arts by 31 December 2007, and by the anniversary of that date in each subsequent year until 31 December 2009

3.3 In investigating the matters referred to in 3.1 above, ACMA must have regard to:

3.3.1 developments in Internet content filtering technologies deployable at the following levels:

- (a) on ISP servers; or
- (b) on personal computers; or
- (c) on mobile devices;

3.3.2 how content filtering is currently deployed at all those levels in other countries;

3.3.3 legislative and administrative developments in other countries designed to promote safe and appropriate use of the Internet by minors;

3.3.4 contextual considerations which might impact on the relevance to Australia of the experience of other countries; and

3.3.5 the challenges for Internet content filtering and other Internet safety initiatives posed by new technologies and platforms that permit high levels of user-generated content and social interaction.

# Appendix B: Australian initiatives in online safety

## Overview

The approach to online safety in Australia involves several government agencies and complementary programs. One of the central programs is the online content co-regulatory scheme, discussed below. The scheme has several elements, including a hotline for complaints about illegal content, criminal provisions relating to the publication of prohibited material online and a series of education initiatives.

The *Broadcasting Services Act 1992* establishes the regulatory framework for broadcasting and online services. In 2007, the Broadcasting Services Act was amended by the *Communications Legislation Amendment (Content Services) Act 2007* (Content Services Act), which commences in January 2008. The amendment introduces a new Schedule 7 to the Broadcasting Services Act and extends the regulatory framework for online services established by Schedule 5 to include stored content services, including commercial content services and to ‘live’ content services, such as chat.

The regulatory framework established under the Broadcasting Services Act is underpinned by principles set out in the National Classification Code (NCC), which is agreed between Commonwealth, state and territory governments. The NCC specifies four principles, which are that:

- (a) adults should be able to read, hear and see what they want;
- (b) minors should be protected from material likely to harm or disturb them;
- (c) everyone should be protected from exposure to unsolicited material that they find offensive; and
- (d) there is a need to take account of community concerns about:
  - (i) depictions that condone or incite violence, particularly sexual violence; and
  - (ii) the portrayal of persons in a demeaning manner.

These principles are used to determine classification categories for content appropriate for audiences of different ages. The classification categories set out in the *Classification (Publications, Films and Computer Games) Act 1995* (the Classification Act) range from G to RC (Refuse Classification), with some categories being advisory only while others are legally restricted. There are guidelines that describe in more detail the nature of the different classification categories, and the scope and limits of material suitable for each category. The guidelines are revised from time to time in consultation with members of the public,

community groups and organisations and must be approved by the Commonwealth, state and territory ministers with responsibilities under the Classification Act.

An interim regulatory framework dealing with certain types of mobile premium content has been reviewed and provisions that overlap with the new Schedule 7 to the Broadcasting Services Act will be revoked in January 2008.

Other functions related to promoting the safety of children online are performed by other Australian Government organisations. Law enforcement agencies investigate and enforce law relating to online child sexual exploitation and harassment, including online bullying. Other agencies conduct research or administer programs designed to promote the safety of Australian families online, including the national filter scheme.

## **Online content co-regulatory scheme**

The online content co-regulatory scheme includes:

- regulatory measures around the publication of material on the internet, including:
  - administrative mechanisms for removing prohibited content from Australian servers; and
  - criminal provisions relating to child online sexual exploitation and other illegal conduct online; and
- non-regulatory measures, particularly education and awareness activities.

## **HOTLINE FOR POTENTIALLY PROHIBITED CONTENT**

The Attorney-General's Department administers the **National Classification Scheme**, which forms the basis for the classification of broadcasting and online content, and for the new content services arrangements. The National Classification Scheme is a cooperative arrangement under which the Classification Board classifies films (including videos and DVDs), computer games and certain publications. It is the role of the Classification Board to decide which classification should be given, by applying the relevant law and classification guidelines. The classifications for films and computer games are G, PG, M, MA 15+ and RC. Films have two additional classifications—R 18+ and X 18+. RC (refused classification) material cannot be legally shown, sold or hired in Australia.

ACMA administers a hotline for complaints about potentially prohibited internet content. Complaints may be made on the complaints form on ACMA's website. Potentially prohibited internet content is internet content that is, or is likely to be, classified X18+ or RC by the Classification Board and, in the case of content that is hosted in Australia, content that is classified R18+ and not subject to a restricted access system. On commencement of Schedule 7 to the Broadcasting Services Act, commercial content that is likely to be classified MA15+ will also be potentially prohibited if it is not subject to a restricted access system.

If prohibited content is determined to be hosted in Australia, the scheme requires ACMA to direct the relevant content host to remove the content from its service. If hosted overseas, ACMA will notify the content to the suppliers of accredited filters under the Internet Industry Association's (IIA) Content Codes of Practice, and filters provided under the National Filter Scheme, so that the content will be blocked for users of those filters.

If content that is the subject of a complaint is ‘sufficiently serious’ (including material such as child pornography), ACMA refers the matter to a law enforcement agency for criminal investigation. ACMA has formalised agreements with law enforcement agencies throughout Australia, including the Australian Federal Police (AFP). Where ACMA determines that sufficiently serious content is hosted in another INHOPE member’s jurisdiction, ACMA will notify the affiliate hotline in that jurisdiction who may then make seek to have the content taken down. Where ACMA determines that sufficiently serious content is hosted in a country in which no INHOPE member operates, ACMA will refer the content to the AFP for notification to the relevant overseas police service via Interpol.

## **CRIMINAL LAWS RELATING TO THE INTERNET**

Offence provisions under the *Criminal Code Act 1995* cover the use of the internet to access, transmit and make available child pornography, as well as the possession or production of such material with the intent to place it on the internet. Each offence carries a maximum penalty of 10 years imprisonment. Included is an obligation on ISPs and content hosts to refer details of offences to the AFP. There are fines for ISPs and content hosts who do not meet these obligations in a timely way.

There are also offences for using the internet to:

- procure or ‘groom’ a person aged less than 16 years—penalties range from 12 to 15 years imprisonment; and
- menace, harass, cause offence, encourage or incite violence or to vilify persons on the basis of their race or religion.

These provisions extend to online bullying.

State and territory laws also impose obligations on producers of content and persons who upload or access content.

## **EDUCATION AND AWARENESS INITIATIVES**

ACMA’s community awareness programs comprise activities operated under the Cybersmart Kids and NetAlert brands.

The Cybersmart Kids website provides internet safety advice to children parents and teachers. Safety information on the site continues to be updated to reflect emerging areas of concern, such as social networking and content issues related to mobile phones.

ACMA also operates Cybersmart Detectives, an online activity developed for use in schools. ACMA conducts regular national or state-based activities, often working with state or federal police. Through a partnership with the Government of Western Australia’s Department of Education and Training, ACMA is now rolling out the activity to all schools in that state, with the intention that it will be made available to other states from 2008.

The NetAlert program consists of a variety of initiatives which aim to promote online safety to Australian families. ACMA shares responsibility for the NetAlert program with the Department of Broadband, Communications and the Digital Economy.

ACMA’s responsibilities under the NetAlert initiative include the rollout of an outreach training program, the development of education and advisory materials, and the operation of a research program looking at trends in online safety.



Under the outreach program, trainers visit schools and communities to promote the internet safety message to parents, teachers and young people.

ACMA has educational resources targeting safety advice to particular age groups and for use in homes and the classroom, include Netty's World (targeting ages 2–7 years), Cyberquoll (8–12 years), Cybernetrix (13–16 years) and Wise Up To IT (for older teens). New resources are being developed to meet emerging areas of need.

ACMA is also undertaking a research program to explore current trends in online use by young people, including the types of risks that young people encounter online, and the ways they are dealing with those risks. This research will allow ACMA to better target online safety messages for young people.

ACMA works closely with other agencies involved in the area of online safety in delivering these programs, including state and federal police, education departments, and international safety organisations such as NetSafe (New Zealand), Childnet International (UK), the Child Exploitation and Online Protection Centre (UK), and the UK Home Office.

The role of the Department of Broadband, Communications and the Digital Economy under the NetAlert program includes the operation of the National Filter Scheme, aiming to provide every Australian household with access to a free internet content filter; and a website ([www.netalert.gov.au](http://www.netalert.gov.au)) and free national helpline to provide advice to parents on online safety issues.

## **Other actions to promote online safety**

Functions performed by Australian Government agencies to promote the safety of Australian children online include the following:

- Launched in March 2005, the **Online Child Sex Exploitation Team (OCSET)**, a unit of the AFP, has a role in investigating and coordinating international and national referrals of child pornography.
- The **National Filter Scheme** is an initiative administered by the Department of Broadband, Communications and the Digital Economy with the goal of providing free PC filters to potential users, particularly parents/guardians, and to subsidise ISP content filters.
- A Department of Education, Employment and Workplace Relations initiative regarding cyber-bullying includes funding for two **research projects into covert bullying**: a study by Edith Cowan University on the key factors leading to covert bullying and strategies to deal with it; and a technology project by the University of South Australia to record 'spoken stories' from students, parents and teachers to develop practical solutions.
- The **National Child Protection Clearinghouse** is funded by the Department of Families, Housing, Community Services and Indigenous Affairs under the auspices of the Australian Council for Children and Parenting as part of the government's response to the problem of child abuse. The Clearinghouse provides information about internet safety and guidelines for parents of children and young people in using the internet on its website.

# Glossary

ACMA	<p>Australian Communications and Media Authority</p> <p>An Australian Government regulatory authority for broadcasting, online content, radiocommunications and telecommunications, with responsibilities under the <i>Broadcasting Services Act 1992</i>, the <i>Radiocommunications Act 1992</i>, the <i>Telecommunications Act 1997</i> and related Acts. Established on 1 July 2005 following a merger of the Australian Communications Authority and the Australian Broadcasting Authority.</p>
blog	An online log, similar to a public journal or diary.
CEOP	<p>Child Exploitation and Online Protection Centre</p> <p>A UK law enforcement organisation that combines children’s charities, industry, government and other interested parties. It works across the UK and in partnership with international organisations through the Virtual Global Taskforce.</p>
chat services	Chat services take two primary forms—internet relay chat (IRC) and web-based chat services. As use of the web grew, web-based chat services developed. Initially chat sites provided users with access to a number of chat ‘rooms’ organised topically. While these sites are still available, web-based chat functionality is increasingly integrated into individual sites to encourage discussion about the content of the site or a topic of interest.
Childnet International	A registered charity in the UK, Childnet was established in 1996 in response to increasing public concerns about internet dangers. Formed by a partnership between industry, government, education and law enforcement, it aims to work in partnership with others around the world to ‘help make the Internet a great and safe place for children’ In working towards this goal, Childnet seeks to assist young people to use the net constructively, raise awareness among organisations, parents, teachers and carers about internet and mobile safety, and work to protect children from being exploited in online environments. The organisation also takes an active role in policy development, seeking to initiate and respond to policy changes that relate to online safety for children.
cookie	Information stored on a device for the purpose of tracking an end user’s use of a website or registering their preferences
DNS	<p>domain name system</p> <p>A distributed client-server database system that links domain names with their numerical IP addresses.</p>

eco	eco – Verband der Deutschen Internetwirtschaft (e.V) [Federation of the German Internet Economy]  German internet service providers’ organisation founded in 1995.
Electronic Frontiers Australia	A national non-profit organisation representing internet users concerned with online freedoms and rights.
email	electronic mail  Service on a specific protocol that enables users to send text-based messages and documents, using a store and forward mechanism, through the internet to users at a specific destination.
European Commission	The executive branch of the EU, responsible for proposing legislation, implementing decisions, upholding the EU’s treaties and general day-to-day running.
European Council	The highest political body of the EU, which brings together the heads of state or government of the EU and the president of the Commission. It defines the general political guidelines of the EU.
EU	European Union  A political and economic community of 27 member states with supranational and intergovernmental features, primarily located in Europe.
EverQuest	A fantasy role-playing game in which players create avatars that are used to explore a fantasy world and interact with other players.
exclusion	A form of cyber-bullying that involves blocking a particular user, the victim, from a social group or deleting them from friendship lists where the victim may feel socially isolated.
FOSI	Family Online Safety Institute  An international, non-profit organisation with the primary objective of developing innovative solutions for family online safety, which is involved in international standards development work for content rating and labelling schemes, and is responsible for the ICRA labelling system.
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter  A registered German association founded in 1997 by e-commerce alliances and companies dedicated to the protection of the youth and minors. As an organisation for the voluntary self-control of the internet, the FSM operates a hotline that deals with reports on illegal or harmful web content that any person or organisation may report.
Geocities	An early web-hosting service that provides a forum for users to build their own websites.
happy slapping	A form of cyber-bullying that involves posting images of bullying incidents online.
header	Refers to the information at the beginning of a packet, which contains information about the handling of the packet. Like an envelope around a letter, header information will

	include, among other things, destination and source IP addresses.
hotlines	Initiatives that receive complaints from users about illegal material on the internet and have formal procedures for processing these complaints, which usually include mechanisms to report illegal content to law enforcement agencies and the issuing of ‘take-down notices’ for content hosted by ISPs in their jurisdiction.
HTTP	hypertext transfer protocol The communications protocol used to publish and retrieve pages on the internet.
ICRA	Internet Content Rating Association The previous name for the Family Online Safety Institute. ICRA is still the name for FOSI’s content labelling scheme, which aims to empower parents to make choices about what digital content their children can and cannot see.
identity theft	A catch-all term for crimes involving illegal usage of another individual's identity. The most common form of identity theft is credit card fraud. While the term is relatively new, the practice of stealing money or getting other benefits by pretending to be a different person is not.
IM	instant messaging Near real time or real time text-based or video communications between two or more users via the internet. IM applications commonly include contact lists that enable users to indicate their online presence.
impersonation	A form of cyber-bullying that involves setting up fake web pages that are attributed to the victim of bullying to make manipulative or derogatory comments about other users. This may involve stealing passwords and using them to gain access to other users’ websites to make comments about other users that are later attributed to the victim.
INHOPE	International Association of Internet Hotlines A group of national hotlines for complaints about potentially illegal internet content, which came together in 1999. There are now 28 members of INHOPE, located in Europe, Asia, North America and Australia. Members meet regularly to share knowledge and best practice, and work together to tackle the global problem of illegal content online.
INSAFE	INSAFE is a network of national nodes that coordinate internet safety awareness in Europe. The network is set up and co-funded within the framework of the European Commission’s Safer Internet plus program, which comprises four action lines.
intimidation	A form of cyber-bullying that involves posting personally abusive and threatening comments on another user’s website, profile, blog or email.
IP	internet protocol The language that computers use to communicate over the internet. A protocol is the pre-defined way that someone who wants to use a service talks with that service. The ‘someone’ could be a person but more often it is a computer program like a web browser.

IP address	<p>internet protocol address</p> <p>Essentially a network address. An IP address is a unique identifier that electronic devices such as computers, routers and printers use in order to identify and communicate with each other on a computer network that uses the internet protocol. The internet is one such network.</p>
IRC	<p>internet relay chat</p> <p>Available since 1988, IRC enables both communication between groups of users and private communication between two users. IRC enables real time, text-based discussion, organised into topics of interest. Users of IRC must use software to connect to the IRC network and receive traffic from other users. IRC is also commonly used to facilitate file sharing by enabling users to send files directly to users.</p>
ISP	<p>internet service provider.</p> <p>A company that provides internet access for individuals, organisations, and companies.</p>
IWF	<p>Internet Watch Foundation</p> <p>An organisation in the UK that operates an internet ‘hotline’ for the public and IT professionals to report their exposure to potentially illegal content online. It works in partnership with the police, government, the public, internet service providers and the wider online industry.</p>
KJM	<p>Kommission für Jugendmedienschutz [Commission for the Protection of Minors in the Media]</p> <p>Established in 2003 and consisting of 12 members from the media, youth protection and government sectors, KJM is responsible for overseeing the adherence to the Jugendmedienschutz-Staatsvertrag, the primary piece of German legislation governing internet and media content, by internet and broadcast media organisations.</p>
malware	<p>Malicious software, which includes viruses, worms, trojan horses, spyware and keystroke loggers. Many early forms of malware were written as pranks that were intended to disrupt organisations’ functioning rather than cause serious damage. However, malware is now increasingly used for extortion through denial of service attacks and to perpetrate online fraud.</p>
message boards	<p>Enable users to post messages online, accessed through a web browser. Content may be text based or may include images, video or audio content.</p>
metadata	<p>Information delivered with content that is about the content being delivered. Metadata is available to the client application, e.g. the web browser reading html, and forms part of the web page’s code, but is not displayed to the user.</p>
National Classification Scheme	<p>The National Classification Scheme is a cooperative arrangement under which the Classification Board classifies films (including videos and DVDs), computer games and certain publications. It is the role of the Classification Board to decide which classification should be given, by applying the relevant law and classification guidelines. The classifications for films and computer games are G, PG, M, MA 15+ and RC. Films have two additional classifications—R 18+ and X 18+. The classification categories for</p>

	publications are Unrestricted, Category 1-Restricted, Category 2-Restricted and Refused Classification. RC material cannot be legally shown, sold or hired in Australia.
newsgroups	Provided an early facility for communication between multiple users. Users access content using specific software called a news-reader. Enables open discussion between users on matters of common interest. Content is usually text-based and is displayed in chronological order or organised topically.
OECD	Organisation for Economic Co-operation and Development  An international organisation of 30 countries helping governments tackle the economic, social and governance challenges of a globalised economy.
Ofcom	Office of Communications  Ofcom is the independent regulator and competition authority for the United Kingdom communications industries with responsibilities across television, radio, telecommunications and wireless communications services.
online fraud	The use of personal information to commit theft or fraud online. Online fraud may involve theft through harvesting personal information that has been posted by users on websites to create fake credit accounts, or the use of malware to access banking information or passwords.
online games	Computer games that use the internet to enable users to engage in collaborative play and communicate with other players.
Optenet	A vendor of filtering software and a provider of filtering for the Australian Government's NetAlert program.
over-blocking	The blocking of sites that should not be blocked as a result of filtering. Past examples have included the blocking of sites discussing breast cancer, and the home pages of high profile people with the first name of 'Dick'.
Ovum	A research organisation that provides worldwide industry research for telecommunications and information technology services.
P2P	Peer-to-peer  A computer communications model in which 'peer' computer systems are connected to each other via the internet. Primarily used to share files, P2P systems enable file sharing directly between computers on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as an end-user.
packet	A formatted block of data that can be transmitted over a network. It will include both header information and the content to be delivered.
phishing	An email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients.
port	A logical channel on which network connections are established and communications are conducted. For example, by default, HTTP connections and information exchange between computers on a network occur on port 80 and port 81 is used to establish secure

	HTTP connections by default.
profiles	Personal information about a user, contained within web pages, which is often shared with a network of other users that may or may not be known to the user in the physical world. Profile information is primarily used to socialise or network with other users.
unauthorised sharing of information	A form of cyber-bullying that involves publishing content such as information, communications or images that were intended to be private to a public space to embarrass or antagonise the victim.
social networking	Using the internet to build and maintain relationships with other users. Most social networking websites contain personal profile information, blogs, message boards, chat and email.
spam	Unsolicited messages often sent in bulk to a large number of email addresses.
spyware	Software that is used to capture personal information without the user's knowledge for business purposes, such as advertising, or criminal purposes such as theft.
The Australia Institute	A public policy research centre funded by grants from philanthropic trusts, memberships and commissioned research.
Trojan horse	Malware hidden in messages or in other apparently innocent software.
URL	uniform resource locator  A string of characters used to identify or name a resource on the internet. It provides users seeking access to a resource (such as a website, or a picture or other element within a website) with a means to locate it.
UGC	user-generated content  Publicly available content that is generated by end-users on the internet. This can include profiles and blogs.
virus	A form of malware that infects other programs on an individual's computer. Viruses may contain a single message or image that is intended to consume memory and degrade computer performance or may be more malicious and destroy data or computer hard drives.
VoIP	voice over internet protocol  VoIP uses internet technology to transmit voice signals over the internet. Voice information is coded format and transmitted in packets of information in the form of data. The data packets are then sent across the internet and reassembled into sound at the other end for the receiver to hear.
W3C	World Wide Web Consortium  Develops interoperable technologies (specifications, guidelines, software, and tools) to allow the World Wide Web to develop to its full potential. W3C is a forum for information, commerce, communication, and collective understanding.



Web 2.0	The growing collection of internet-based services that enable a high level of interaction between users and websites, and among internet users themselves.
web forums	Similar to newsgroups, but users access content through a web browser. Enables open discussion between users on matters of common interest. Content is usually text-based and is displayed in chronological order or organised topically.

# Bibliography

- ACLU (2007), 'Internet Free Speech,' available at: [www.aclu.org/privacy/speech/index.html](http://www.aclu.org/privacy/speech/index.html), accessed 12 November 2007
- Australian Communications and Media Authority (2007), *Media and Communications in Australian Families 2007*, ACMA, Canberra
- Brennan Center for Justice (2006), *Internet Filters: a Public Policy Report*, The Brennan Centre for Justice at NYU School of Law, Free Expression Policy Project, available at: [www.fepproject.org/policyreports/filters2.pdf](http://www.fepproject.org/policyreports/filters2.pdf)
- BT (2007), 'Changing World: Sustained Values', available at: [www.networked.bt.com/pdfs/BT\\_CSR\\_Business\\_Overview.pdf](http://www.networked.bt.com/pdfs/BT_CSR_Business_Overview.pdf), accessed 8 October 2007
- CEOP (2007), *Strategic Overview: Making every child matter ... everywhere*, available at: [www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf](http://www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf)
- CEOP (2007), 'Survey for 11–16 year olds', available at: [www.thinkuknow.co.uk/11\\_16/survey.aspx](http://www.thinkuknow.co.uk/11_16/survey.aspx), accessed 16 November 2007
- Childnet International (1998), *Actions in Preparation for a future Action Plan on promoting safe use of the internet* [PREP ACT Lot 1 – Hotlines], available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/PREP-ACT\\_1\\_final\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/PREP-ACT_1_final_report.pdf)
- Childnet International (2003), 'Childnet Academy: Cable & Wireless Childnet Academy Winners 2005', available at: <http://www.childnetacademy.org/winners/>, accessed 12 November 2007
- Childnet International (2003), 'Childnet Academy: Winners, Individual 2004', available at: [www.childnetacademy.org/winners/winners/ind04-03.aspx](http://www.childnetacademy.org/winners/winners/ind04-03.aspx), 12 November 2007
- Childnet International (2003), 'Childnet Academy: Winners, Individual 2003', available at: [www.childnetacademy.org/winners/winners/ind03-04.aspx](http://www.childnetacademy.org/winners/winners/ind03-04.aspx), 12 November 2007
- Childnet International (2003), 'Childnet Academy: Winners, Individual 2002', available at: [www.childnetacademy.org/winners/winners/ind02-01.aspx](http://www.childnetacademy.org/winners/winners/ind02-01.aspx), 12 November 2007
- Childnet International (2003), 'Childnet Academy: Winners, Individual 1999', available at: [www.childnetacademy.org/winners/winners/ind99-02.aspx](http://www.childnetacademy.org/winners/winners/ind99-02.aspx), 12 November 2007
- Childnet International (2003), 'Childnet Academy: Winners, Individual 1998', available at: [www.childnetacademy.org/winners/winners/ind98-01.aspx](http://www.childnetacademy.org/winners/winners/ind98-01.aspx), 12 November 2007
- Childnet International (2005), 'About KIA', available at: [www.childnet-int.org/kia/about/](http://www.childnet-int.org/kia/about/), accessed 22 November 2007
- Childnet International (2007), 'Overview of Know IT All', available at: [www.childnet-int.org/kia/overview.aspx](http://www.childnet-int.org/kia/overview.aspx), accessed 13 December 2007

- Childnet International and Fleishman Hillard International Communications (1999), *Promoting Safe Use of the Internet – Final Report*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/PREP-ACT\\_4\\_Awareness\\_summary.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/PREP-ACT_4_Awareness_summary.pdf)
- Clayton, R. (2005), *Anonymity and Traceability in Cyberspace*, Technical Report No 653, Cambridge University, available at: [www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html](http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html), accessed 26 October 2007
- Clayton, R. (2005), 'Failures in a Hybrid Content Blocking System' available at: [www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf](http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf), accessed 8 August 2007
- Deloitte (2006), *Safer Internet: Test and benchmark of products and services to filter internet content for children between 6 and 16 years* [Synthesis Report], prepared for European Commission, DG Information Society – Directorate E, available at: [www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf](http://www.sip-bench.eu/SIPBench%202006%20Synthesis%20Report.pdf)
- Department for Children Schools and Families (2007), 'The Byron Review – Call for Evidence: Adult Version', available at: [www.dfes.gov.uk/byonreview/](http://www.dfes.gov.uk/byonreview/), accessed 22 November 2007
- Department for Children Schools and Families (2007), 'The Byron Review – Call for Evidence: Child and Young Person's Version', available at: [www.dfes.gov.uk/consultations/conDetails.cfm?consultationId=1511](http://www.dfes.gov.uk/consultations/conDetails.cfm?consultationId=1511), accessed 22 November 2007
- Digizen (2007), *Let's Fight it Together: Cyberbullying Film*, available at: <http://www.digizen.org/cyberbullying/film.aspx>, accessed 28 November 2007.
- Dornseif, M. (2003), 'Government Mandated Blocking of Foreign Web Content', in: von Knop, J., Haverkamp, W. and Jessen, E. (Eds), *Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze*, Düsseldorf, available at: <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>
- eco (2007), 'Goals – Enforcement and Threat Assessment', available at: [www.spotspam/goals.net/](http://www.spotspam/goals.net/), accessed 21 November 2007
- Educaunet (2007), 'Risk and the Internet', available at: [www.educaunet.org/eng/](http://www.educaunet.org/eng/), accessed 20 October 2007
- Educaunet Consortium (2004), *Educaunet: Final Report October 1 2002-July 31 2004*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/educaunet2\\_final\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/educaunet2_final_report.pdf), accessed 21 November 2007
- Electronic Frontiers Australia (2004), 'About Us' available at: [www.efa.org.au/AboutEFA/](http://www.efa.org.au/AboutEFA/), accessed 8 November 2007
- Electronic Frontiers Australia (2003), 'Comments on Mandatory Filtering and Blocking by ISPs,' available at: [www.efa.org.au/Publish/ispblocking.html](http://www.efa.org.au/Publish/ispblocking.html), accessed 8 November 2007
- European Commission (2006), *Call for proposals for indirect actions under the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet plus)*, [2006], [http://ec.europa.eu/information\\_society/activities/sip/docs/call\\_2006/call\\_announcement\\_2006/sip\\_call\\_announcement\\_2006\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/call_2006/call_announcement_2006/sip_call_announcement_2006_en.pdf)
- European Commission (2002), 'Educaunet', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/awareness/closed\\_projects/educaunet/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/awareness/closed_projects/educaunet/index_en.htm), accessed 21 November 2007
- European Commission (2007), 'Filtering and Rating: Closed Projects', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/targeted/filtering/closed\\_projects/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/closed_projects/index_en.htm), accessed 19 November 2007

- European Commission (2007), 'Hotlines for Germany IBSDE', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/hotlines/germany/ibsde/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/hotlines/germany/ibsde/index_en.htm), accessed 20 November 2007
- European Commission (2007), 'ICRA Safe: Internet Content Rating Association', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/targeted/filtering/closed\\_projects/icrasafe/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/closed_projects/icrasafe/index_en.htm), accessed 19 November 2007
- European Commission (2007), 'Mobile operators agree on how to safeguard children using mobile phones', [Media Release] 6 February 2007, IP/07/139, available at: [www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=HTML&aged=0&language=EN&guiLanguage=en](http://www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=HTML&aged=0&language=EN&guiLanguage=en), accessed 21 October 2007
- European Commission (2007), 'Safer internet shielding benchmark', available at: [www.sip-bench.org/sipbench.php?page=benchmark&lang=en](http://www.sip-bench.org/sipbench.php?page=benchmark&lang=en), accessed 12 November 2007
- European Commission (2007), 'Safer Internet Plus: Awareness Activities', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/awareness/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/awareness/index_en.htm), accessed 20 November 2007
- European Commission (2007), 'Safer Internet Plus: Helplines: Helpline running projects', available at: [http://ec.europa.eu/information\\_society/activities/sip/projects/helplines/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/projects/helplines/index_en.htm), accessed 22 November 2007
- European Commission, Directorate-General Information Society and Media (2007), *Safer Internet for Children: Qualitative Study in 29 European Countries*, available at: [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm#overall\\_report](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm#overall_report), 13 September 2007
- Family Online Safety Institute (2007), 'About ICRA', available at: [www.fosi.org/icra/](http://www.fosi.org/icra/) accessed 31 October 2007
- Family Online Safety Institute (2007), 'Everyone has an opinion on the web,' available at: [www.fosi.org/archive/everyonehasanopinion/](http://www.fosi.org/archive/everyonehasanopinion/), accessed 7 November 2007.
- Family Online Safety Institute (2007), 'ICRAchecked,', available at: <http://checked.icra.org/>, accessed 12 November 2007
- Family Online Safety Institute (2007), 'ICRAPlus,', available at: <http://www.icra.org/icraplus/>, accessed 12 November 2007
- Flood, M., and Hamilton, C. (2003), *Regulating Youth Access to Pornography*, Discussion Paper Number 53, The Australia Institute, p. vi, available at: [www.tai.org.au/documents/dp\\_fulltext/DP53.pdf](http://www.tai.org.au/documents/dp_fulltext/DP53.pdf)
- Frost & Sullivan (2006), *World Content Filtering Market*, #BAoD-74, Frost & Sullivan, London
- Frost & Sullivan (2007), *Asia Pacific Secure Content Management Market 2005*, Frost & Sullivan, London
- FSM (2007), *Code of Conduct for the Association Freiwillige Selbstkontrolle Multimedia*, available at: <http://fsm.de/en/CoC>, accessed 21 October 2007
- FSM (2007), *Subcode of Conduct for Search Engine Providers of the Association of Voluntary Self-Regulating Multimedia Service Providers*, available at: [http://fsm.de/en/SubCoC\\_Search\\_Engines](http://fsm.de/en/SubCoC_Search_Engines), accessed 21 October 2007
- FSM (2007), 'Welcome to the FSM website', available at: <http://fsm.de/en/>, accessed 16 October 2007
- Herman, I. (2007), 'Semantic Web Activity Statement,' available at: [www.w3.org/2001/sw/Activity](http://www.w3.org/2001/sw/Activity), accessed 8 November 2007
- Herman, I. (2004), 'Resource Description Framework (RDF),' available at: [www.w3.org/RDF/](http://www.w3.org/RDF/), accessed 8 November 2007

- Home Office (2006), 'Home Office Circular 042 / 2006', available at: [www.knowledgenetwork.gov.uk/HO/circular.nsf/WebPrintDoc/4597CD4C98B621418025724B004D9C6A?OpenDocument](http://www.knowledgenetwork.gov.uk/HO/circular.nsf/WebPrintDoc/4597CD4C98B621418025724B004D9C6A?OpenDocument), accessed 6 November 2007
- Home Office (2005), 'Good Practice Guidance for Moderation of Interactive Services for Children', available at: <http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation.pdf?view=Binary>, accessed 31 October 2007
- Howstuffworks Inc (2007), 'Antivirus Software Buying Guide,' *How Stuff Works* website, available at <http://products.howstuffworks.com/antivirus-software-buying-guide.htm>, accessed 23 October 2007
- IDATE, AIIP and DATABANK Consulting (1999), *Review of European third-party filtering and rating software and services*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/html/reports/idate/IDATEexec.htm](http://ec.europa.eu/information_society/activities/sip/docs/html/reports/idate/IDATEexec.htm)
- INCORE (2000), *Action Plan on promoting safer use of the internet: Self-labelling and filtering*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/html/reports/incore/INCOREexec.htm](http://ec.europa.eu/information_society/activities/sip/docs/html/reports/incore/INCOREexec.htm)
- INHOPE (2007), 'About INHOPE', available at: [www.inhope.org/en/about/about.html](http://www.inhope.org/en/about/about.html), accessed 31 October 2007
- INHOPE (2007), 'History of INHOPE', available at: [www.inhope.org/en/about/history.html](http://www.inhope.org/en/about/history.html), accessed 6 November 2007
- INHOPE (2007), 'INHOPE publish landmark Global Internet Trend Report - 9,600 reports of child pornography processed per month', [Media release] 19 September 2007, available at: [www.inhope.org/en/node/296](http://www.inhope.org/en/node/296), accessed 22 November 2007
- INHOPE (2007), 'Mission and Objectives of INHOPE', available at: [www.inhope.org/en/about/mission.html](http://www.inhope.org/en/about/mission.html), accessed 6 November 2007
- INHOPE (2007), 'Membership', available at: [www.inhope.org/en/about/members.html](http://www.inhope.org/en/about/members.html), accessed 6 November 2007
- INHOPE (2007), 'Partners', available at: [www.inhope.org/en/partners/partners.html](http://www.inhope.org/en/partners/partners.html), accessed 22 November 2007
- Insafe (2007), 'United Kingdom EMPOWER', available at: [www.saferinternet.org/ww/en/pub/insafe/focus/uk.htm](http://www.saferinternet.org/ww/en/pub/insafe/focus/uk.htm), accessed 16 November 2007
- Internet Watch Foundation (2007), 'Commercialising the database', available at: [www.iwf.org.uk/corporate/page.121.251.htm](http://www.iwf.org.uk/corporate/page.121.251.htm), accessed 22 November 2007
- Internet Watch Foundation (2007), 'Presentation to INHOPE Members' Technical Workshop' [Unpublished], Berlin, 26 October 2007
- Internet Watch Foundation (2007), 'Filtering Solutions', available at: [www.iwf.org.uk/public/page.28.34.htm](http://www.iwf.org.uk/public/page.28.34.htm), accessed 20 November 2007
- Internet Watch Foundation (2004), 'RM join IWF as funding member,' [Media Release] 11 May 2004, available at: [www.iwf.org.uk/media/news.archive-2004.30.htm](http://www.iwf.org.uk/media/news.archive-2004.30.htm), accessed 20 November 2007
- Internet Watch Foundation (2004), 'Nomination shortlist for IWF ISPA Award,' [Media Release] 23 December 2004, available at: [www.iwf.org.uk/media/news.archive-2005.149.htm](http://www.iwf.org.uk/media/news.archive-2005.149.htm), accessed 20 November 2007
- Johnson, S. (2005), *Everything Bad is Good for You: how today's popular culture is actually making us smarter*, Riverhead
- KJM (2007), 'Jugendschutz im Internet: KJM-Prüfung zeigt erhebliche Defizite von Jugendschutzfiltern auf', [Media Release], 1 March 2007, available at: [www.kjm-online.de/public/kjm/index.php?news\\_id=89&show\\_1=59,53&z=14&action=show\\_details](http://www.kjm-online.de/public/kjm/index.php?news_id=89&show_1=59,53&z=14&action=show_details), accessed 20 November 2007

- KJM (2007), 'KJM fordert die Entwicklung effizienter Jugendschutzprogramme Prüfung zeigt Defizite auf: Filtersysteme im Internet nicht ausreichend wirksam', [Media release], 29 October 2007, available at: [www.kjm-online.de/public/kjm/index.php?news\\_id=101&show\\_1=59.53&z=3&action=show\\_details](http://www.kjm-online.de/public/kjm/index.php?news_id=101&show_1=59.53&z=3&action=show_details), accessed 20 November 2007
- Legal Information Institute (1997), 'Syllabus: Reno, Attorney General Of The United States, et al. v. American Civil Liberties Union et al.', available at: [www.law.cornell.edu/supct/html/96-511.ZS.html](http://www.law.cornell.edu/supct/html/96-511.ZS.html), accessed 12 November 2007
- Livingstone, S. (2007), 'EU Kids Online', paper delivered at the *Safer Internet Forum Conference*, 20–21 June 2007, Luxembourg, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/forum\\_june\\_2007/eukidsonline\\_livingstone.pdf](http://ec.europa.eu/information_society/activities/sip/docs/forum_june_2007/eukidsonline_livingstone.pdf)
- Netprotect (2002), *Netprotect: A European Prototype for Internet Access Filtering* [EC Commissioned Report], NETPROTECT:WP5:D5.1:2002, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/projects/netproject\\_final\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/projects/netproject_final_report.pdf)
- Nielsen//NetRatings (2007), *Australian eGeneration Report*, Fifth Edition. Nielsen//NetRatings
- Obert, T. (2005), 'German Security Initiative 'Germany safe on the Net', A Best-Practice for Europe', Paper delivered at the *ENISA Good Practice in Awareness Raising Workshop*, Brussels, 14 December 2005, available at: [www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_raising\\_the\\_security\\_bar.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_raising_the_security_bar.pdf), accessed 4 November 2007
- OECD (2001), *Household access by type of service, 2001*, available at: [www.oecd.org/dataoecd/43/26/2766850.xls](http://www.oecd.org/dataoecd/43/26/2766850.xls), accessed 6 November 2007
- OECD (2007), 'OECD Broadband Statistics to December 2006', available at: [www.oecd.org/documentprint/0,3455,en\\_2649\\_201185\\_38446855\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/documentprint/0,3455,en_2649_201185_38446855_1_1_1_1,00.html), accessed 1 November 2007
- OECD (2007), *Mobile Commerce*, Directorate for Science, Technology and Industry, Committee on Consumer Policy, Organisation for Economic Co-operation and Development, 16 January 2007, available at: [www.oecd.org/dataoecd/22/52/38077227.pdf](http://www.oecd.org/dataoecd/22/52/38077227.pdf)
- Ofcom (2006), *Ofcom Media Literacy Bulletin* (8), available at: [www.ofcom.org.uk/advice/media\\_literacy/medlitpub/bulletins/issue\\_8.pdf](http://www.ofcom.org.uk/advice/media_literacy/medlitpub/bulletins/issue_8.pdf), accessed 16 November 2007
- Ovum (2003), *Internet content filtering. A report to DCITA*, available at: [www.dcita.gov.au/data/assets/file/10915/Ovum\\_Report\\_-\\_Internet\\_content\\_filtering.rtf](http://www.dcita.gov.au/data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf)
- Paul Budde Communication Pty Ltd (2007), *Australia – Digital Media – Video Comms, P2P, Instant messaging, Blogging, Social Networks*, Paul Budde Communication Pty Ltd
- Resnick, P. (1999) 'PICS, Censorship, & Intellectual Freedom FAQ,' available at: [www.w3.org/PICS/PICS-FAQ-980126.html](http://www.w3.org/PICS/PICS-FAQ-980126.html), accessed 8 November 2007.
- RMIT Test Lab (2006), *A Study on Server Based Internet Filters: Accuracy, Broadband Performance Degradation and some Effects on the User Experience*, prepared for NetAlert, May 2006, available at: [www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf](http://www.netalert.net.au/03100-A-Study-on-Server-Based-Internet-Filters---26-May-2006.pdf)
- Stark, P. B. (2006), 'Expert report of Philip B. Stark, PhD, 8 May 2006' given in *ACLU v Gonzales* Civ. Action No. 98-5591 (E.D. Pa.), available at: <http://seth.com/infothought/blog/archives/copa-censorware-stark-report.pdf>, accessed 29 September 2007
- Technopolis (2003), *The Evaluation of the Safer Internet Action Plan 1999-2002*, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/reports/evaluation\\_safer\\_internet\\_full\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/reports/evaluation_safer_internet_full_report.pdf)



- Technopolis (2003), 'Executive Summary' *The Evaluation of the Safer Internet Action Plan 1999-2002*, European Commission DG Information Society, Luxembourg, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/reports/evaluation\\_safer\\_internet\\_exec\\_report.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/reports/evaluation_safer_internet_exec_report.pdf)
- The Australia Institute (2006), 'About Us' available at: [www.tai.org.au/index.php?option=com\\_content&task=view&id=25&Itemid=37](http://www.tai.org.au/index.php?option=com_content&task=view&id=25&Itemid=37), accessed 8 November 2007
- Thornburgh, D and Lin, H (Eds) (2002), *Youth, Pornography and the Internet*, National Academy Press, Washington
- Trend Micro (2007), 'Virus Primer', available at: <http://us.trendmicro.com/us/support/virus-primer/index.html>, accessed 28 November 2007
- U.S Supreme Court (1997), 'Syllabus: Reno, Attorney General Of The United States, et al. v. American Civil Liberties Union et al.', available at: [www.law.cornell.edu/supct/html/96-511.ZS.html](http://www.law.cornell.edu/supct/html/96-511.ZS.html), accessed 12 November 2007
- Vodafone (2006), *Staying in Touch: A Parent's Guide to Mobile Phones*, [brochure], available at: [www.familyandparenting.org/Filestore/Documents/publications/A5\\_Parents\\_Guide\\_to\\_Mobile\\_Phones.pdf](http://www.familyandparenting.org/Filestore/Documents/publications/A5_Parents_Guide_to_Mobile_Phones.pdf)
- Waltermann, J and Machill, M. (Eds.), (2000), *Protecting our Children on the Internet: Towards a New Culture of Responsibility*, Bertelsmann Foundation Publishers, Gutersloh, available at: [www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst\\_engl/474.pdf](http://www.bertelsmann-stiftung.de/cps/rde/xbcr/SID-0A000F14-78EE8AB7/bst_engl/474.pdf)
- Wishart, J., Andrews, J. and Wan, C.Y. (2006), 'Evaluation of the 'Getting to Know IT All' presentation as delivered in UK schools during November 2005', University of Bristol, available at: [www.childnet-int.org/downloads/gtkiaEvaluation.pdf](http://www.childnet-int.org/downloads/gtkiaEvaluation.pdf), accessed 22 November 2007
- W3C (2005), 'W3C Content Labels,' available at: [www.w3.org/2005/Incubator/wcl/XGR-report/](http://www.w3.org/2005/Incubator/wcl/XGR-report/), accessed 29 October 2007
- W3C. (2007), 'A Little History of the World Wide Web', available at: [www.w3.org/History.html](http://www.w3.org/History.html), accessed 12 November 2007
- YouTube (2007), 'YouTube Community Guidelines,' available at: [http://uk.youtube.com/t/community\\_guidelines](http://uk.youtube.com/t/community_guidelines), accessed 28 November 2007

## LEGISLATION

### Australia

*Spam Act 2003*, available at: [www.austlii.edu.au/au/legis/cth/consol\\_act/sa200366/](http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/)

*Crimes Legislation Amendment (Telecommunications Offences and Other Measures Bill (No.2) 2004*, available at:

[www.frli.gov.au/comlaw/Legislation/Bills1.nsf/0/609515684FFB15C0CA256F72002610E7/\\$file/04149b.rtf](http://www.frli.gov.au/comlaw/Legislation/Bills1.nsf/0/609515684FFB15C0CA256F72002610E7/$file/04149b.rtf)

### Canada

*Criminal Code 1985*, available at: <http://laws.justice.gc.ca/en/C-46/>

### European Union

*Communication from the Commission of 3 November 2003 concerning the evaluation of the multiannual Community action plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors*, COM(2003) 653 final .6.11.2006, available at: [www.europa.eu/scadplus/leg/en/lvb/124190.htm](http://www.europa.eu/scadplus/leg/en/lvb/124190.htm)

*Communication on the implementation of the multiannual Community Programme on promoting the safer use of the Internet and new online technologies (Safer Internet Plus)*, COM(2006) 661 final 12.03.2004, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/pdf/si\\_plus/exante.pdf](http://ec.europa.eu/information_society/activities/sip/docs/pdf/si_plus/exante.pdf)



*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 (98/560/EC)*, O.J. L270/48 7.10.98, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/1998/l\\_270/l\\_27019981007en00480055.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/1998/l_270/l_27019981007en00480055.pdf)

*Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, O.J. L33/1 6.2.1999, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l\\_033/l\\_03319990206en00010011.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l_033/l_03319990206en00010011.pdf)

*Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, O.J. L162/1 01.07.2003, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l\\_162/l\\_16220030701en00010004.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_162/l_16220030701en00010004.pdf)

*Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies*, O.J. L149/1 11.06.2005, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_decision\\_2005/sip\\_decision\\_2005\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2005/sip_decision_2005_en.pdf)

*Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, O.J. L201/37 31.07.2002, available at: [http://eur-lex.europa.eu/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf)

*Final Evaluation of the implementation of the multiannual Community Action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions*, COM(2006) 663 final 6.11.2006, available at: [http://ec.europa.eu/information\\_society/activities/sip/docs/prog\\_evaluation/comm\\_final\\_eval\\_siap\\_en.pdf](http://ec.europa.eu/information_society/activities/sip/docs/prog_evaluation/comm_final_eval_siap_en.pdf)

*Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry (2006/952/EC)* O.J. L378/72 27.12.2006, available at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l\\_378/l\\_37820061227en00720077.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_378/l_37820061227en00720077.pdf)

*Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, O.J. L 077/1 13.03.2004, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

*Treaty on European Union*, art. 2, ¶1, [2002 consolidated version], O.J. C325/33 24.12.2002, available at: [http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E\\_EN.pdf](http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E_EN.pdf)

*Treaty on European Union*, art. 5 and protocol, [2002 consolidated version], O.J. C325/33 24.12.2002, available at: [http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E\\_EN.pdf](http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/pdf/12002E_EN.pdf)

## **Germany**

*Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia*, art 5, 01.03.2007, [English Version], available at: [www.artikel5.de/gesetze/jmstv.html](http://www.artikel5.de/gesetze/jmstv.html)

*Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia*, art 18, 01.03.2007, [English Version], available at: [www.kjm-online.de/public/kjm/downloads/JMStV2007-englisch.pdf](http://www.kjm-online.de/public/kjm/downloads/JMStV2007-englisch.pdf)

## **United Kingdom**

*The Privacy and Electronic Communications (EC Directive) Regulations 2003*, available at: [www.opsi.gov.uk/si/si2003/20032426.htm](http://www.opsi.gov.uk/si/si2003/20032426.htm)

*Sexual Offences Act 2003*, available at: [www.opsi.gov.uk/ACTS/acts2003/20030042.htm](http://www.opsi.gov.uk/ACTS/acts2003/20030042.htm)

**United States**

*US Code*, available at: [www.law.cornell.edu/uscode/](http://www.law.cornell.edu/uscode/)