

## SECOND REPORT





<b>INTERNET ADVISORY BOARD CHAIRWOMAN'S INTRODUCTION</b>	<b>3</b>	<b>STATISTICAL ANALYSIS OF HOTLINE REPORTS</b>	<b>17</b>	<b>CONCLUSIONS</b>	<b>34</b>
<b>PREFACE</b>	<b>5</b>	<b>1ST JULY 2001 - 30TH JUNE 2003</b>	<b>17</b>	<b>SAMPLE CASES.</b>	<b>37</b>
<b>EXECUTIVE SUMMARY</b>	<b>7</b>	Level of reporting to the Hotline	17	<b>APPENDICES</b>	<b>40</b>
<b>INTRODUCTION AND HISTORY OF THE HOTLINE</b>	<b>8</b>	Accessing the Hotline	19	Appendix 1 – www.hotline service: terms of reference	40
Special consideration of children using the Internet	9	Internet service where the content of concern is located	19	Appendix 2 – ISPAI membership	40
Current development of Hotline	9	Suspicion underlying reports	19	Appendix 3 – INHOPE Association members	40
<b>STRUCTURE OF THE HOTLINE</b>	<b>10</b>	Hotline determinations	21	Appendix 4 – Explanation of categories for classification of content	41
Organisation and management	10	Location of sites	24	Appendix 5 – EU Internet Action Programme	42
Governance	10	Actions on illegal material: source determined to be within Ireland	25	Appendix 6 – Ratified aims of the Internet Service Provider Association of Ireland	42
European Commission support	11	Actions on illegal material: source determined to be outside Ireland	25	Appendix 7 – References	42
<b>EXTERNAL RELATIONS</b>	<b>12</b>	<b>ISSUES ARISING</b>	<b>27</b>		
INHOPE Association	12	Increasing incidence of spam	27		
www.hotline input to INHOPE	12	Defamation attack UCEs	29		
Other international activities	13	Investigation of reports	30		
<b>OVERVIEW OF THE WORK OF THE HOTLINE</b>	<b>14</b>	Tracking and Managing reports	30		
Role of the Hotline	14	Archiving reports and material	31		
Scope of Hotline	14	Protocol with An Garda Síochána and with Internet Service Providers	31		
Procedures of the Hotline	15	Offers of assistance	31		
		Hotline visibility and promotional activities	31		
		Quality of reports	32		

## INTERNET ADVISORY BOARD CHAIRWOMAN'S INTRODUCTION

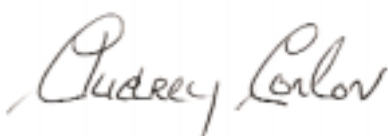


As a member of the Government Review Group on Illegal and Harmful Use of the Internet, I was strongly of the opinion that any attempt to regulate Internet content required a new approach.

In my professional capacity as a film censor, I had worked within a statutory framework classifying film and video. Here, the physical presence of the material made it possible to regulate content. Images from cyberspace presented a completely new set of challenges. I therefore welcomed the decision by Government to accept a self-regulatory regime by the Internet Service Providers in Ireland.

The [www.hotline.ie](http://www.hotline.ie) service has been crucial to the success of the self-regulatory model as this second report clearly indicates. The Internet Advisory Board is responsible for the supervision of Internet self-regulation in Ireland and as one of our partners, we will continue to work with the [www.hotline.ie](http://www.hotline.ie) service to make the Internet a safer environment for all users but particularly our children.

I would like to take this opportunity to join with Paul Durrant, General Manager of the [www.hotline.ie](http://www.hotline.ie) service, in thanking all our colleagues on the Internet Advisory Board and the Board's secretariat for their invaluable support.



**Audrey Conlon**  
Chairwoman, Internet Advisory board



*According to Comreg at the end of July 2001, 30% of adults in households with a fixed telephone line had Internet access. Over the two years, this has grown to 38% with 100% of businesses surveyed claiming to use e-mail. It is also clear that Internet traffic is an increasingly important component of the telecommunications industry with dial-up Internet access accounting for 39% (June '03) of all dialled minutes, compared with 25% in June '01.*

## PREFACE



This is the second report of [www.hotline.ie](http://www.hotline.ie), the service operated by the Internet Service Providers' Association of Ireland (ISPAI), which accepts and processes reports from the public in relation to illegal material, especially child pornography, found on the Internet. This report covers the period *1st July 2001 to 30th June 2003*.

Since the first report of the [www.hotline.ie](http://www.hotline.ie) service (hereafter referred to as the "Hotline") two years ago, use of the Internet in Ireland has grown considerably. According to Comreg (formerly ODTR), at the end of July 2001, 30% of adults in households with a fixed telephone line had Internet access. Over the two years, this has grown to 38% with 100% of businesses surveyed claiming to use e-mail. It is also clear that Internet traffic is an increasingly important component of the telecommunications industry with dial-up Internet access accounting for 39% (June '03) of all dialled minutes, compared with 25% in June '01.

With the vast growth in Internet usage in Ireland and world-wide, it is inevitable that, as with any other technology, a small minority of people will exploit it for socially unacceptable and criminal purposes. It is therefore in the public interest that an efficient and effective service exists to instigate removal of such material from the Internet. This service must be recognised as authoritative and neutral in its assessment of alleged illegal content and able to provide expert coherent information to law enforcement agencies on which they may initiate investigations. The Hotline provides this service in Ireland. The primary concern of the Hotline is to ensure, as far as is practicable, that illegal content is not hosted in, or

disseminated from, Internet Service Providers' (ISP) facilities in Ireland.

However, due to the global nature of the Internet what may be encountered by a user in Ireland could be held electronically anywhere on the planet. An organisation operating in a single country is limited in what it can achieve to combat child pornography, racist and other illegal material being distributed over the Internet. Therefore, of vital importance to its effectiveness, is the Hotline's full membership of INHOPE which is the association of international hotlines. This organisation ensures a rigorous standard of governance and operation of member hotlines and provides the rapid reaction network necessary to expedite action on illegal Internet content across international borders. The Irish Hotline is privileged to have been a founding member of INHOPE.

The success of the Hotline has become evident over the two year reporting period. Very few of the reports submitted by the public to the Hotline, have alleged that illegal content is either hosted on, or distributed from, servers in Ireland run by members of the ISPAI. Almost all reports refer to Web sites hosted outside the jurisdiction or to unsolicited e-mail (spam) received from abroad. This is not just an Irish assertion; it is substantiated by the work of our INHOPE colleagues around the World. In the two year reporting period, these organisations have not forwarded any reports to the Hotline where, after investigation, the content was found to have been hosted on or distributed from servers in the Republic of Ireland.

As a country, we should be proud of this achievement. This has not

happened by chance but through development of world-leading industry practices, strong commitment and close co-operation between Government, An Garda Síochána, the Internet Service Provider Industry and the Hotline. As a result, those seeking a location in which to host or, from which to distribute, illegal content on the Internet, do not regard Ireland as a safe haven.

It is essential that as a country Ireland remains vigilant. Complacency would inevitably result in misuse of systems located here by those with criminal intent. The ISPAI continues to give its commitment to the Irish public and the International Internet community, that it will do its part, within the constraints of the law, to make that phenomenal information resource that is the Internet, a safer place for all, especially children.

I would like to thank the Ministers of Government, particularly Michael McDowell T.D., Minister of Justice, Equality and Law Reform and Minister of State for Children, Brian Lenihan T.D. and his predecessor Mary Hanafin T.D., Members of the Internet Advisory Board, An Garda Síochána and the European Commission's Safer Internet Programme whose continued support has enabled [www.hotline.ie](http://www.hotline.ie) to successfully continue in its work over the reporting period.

Paul Durrant  
General Manager  
[www.hotline.ie](http://www.hotline.ie)



*In this reporting period from the 1st July 2001 until 30th June 2003 the Hotline received 1792 reports. This is a 123% increase on the total received in the previous two years. In the current reporting period, no valid report was received by the Hotline where the content was confirmed as probably illegal and the source of the material proved to be in Ireland.*

## EXECUTIVE SUMMARY

The Hotline is now well established as the key operational component of the self-regulatory regime operated by the ISP industry in Ireland. The Hotline was established to provide the public with a mechanism to report material that they encounter on the Internet and which they suspect may be illegal. It has been in operation since November 1999. It is through the Hotline and its membership of the INHOPE association of international hotlines, that the ISP industry in Ireland makes its contribution to combat illegal content on the Internet both at home and abroad.

In its initial years, the Hotline gained from the operational experience of its longer established and larger INHOPE counterparts but has now moved into a phase of providing experience into the network. This may prove particularly relevant to the smaller EU accession countries setting up Hotlines on a scale which Ireland largely pioneered.

In this reporting period from the 1st July 2001 until 30th June 2003 the Hotline received 1792 reports. This is a 123% increase on the total received in the previous two years. In the current reporting period, no valid report was received by the Hotline where the content was confirmed as probably illegal and the source of the material proved to be in Ireland.

Analysis of reports has shown that a high percentage prove not to refer to illegal material. 16% proved to be child pornography hosted or distributed from other jurisdictions and 39% were assessed as not illegal. However, of concern, are the 42% of reports where the material reported could not be found by the Hotline. This is primarily caused by inaccurate or overly broad information being submitted in the report.

70% of reports received by the Hotline were suspected as being child pornography by the reporter. A considerable proportion (approx. 26%) of these were determined as actually being adult pornography. Many of these reports resulted from UCEs (spam) that contained terminology, which many people would infer as advertising child related material. However, on investigation the Hotline found the UCEs were promoting adult pornographic sites. There is an issue, outside of the Hotline remit, about advertising standards being employed by sections of the adult pornography industry.

The Hotline task is a labour intensive and time-consuming process of methodically locating reported content, identifying the target of the complaint, verifying whether or not it may be illegal, recording the results and, when appropriate, preparing onward reports to INHOPE or law enforcement. It can be aided to a small degree by semi-automation of the report input mechanism but requires co-operation of the reporting public to use the web-based facilities provided. The Hotline must continue its exploration of the options to reduce the number of ineffective reports made.

Over the reporting period Internet technologies have evolved which place new demands on the skills of Hotline employees. For example "peer to peer" file-sharing and mobile access add new levels of complexity and time required to find reported material and ascertain in which country it is hosted.

The techniques being used by criminals to avoid detection are constantly evolving. Knowledge of how sources are disguised is becoming a field of study in itself. Virus-born relays and web-site cloaking systems being the

latest in a long line of measures aimed at making the task of law enforcement and Hotlines more difficult. The Hotline invests in staff training to meet these demands and is supported through the INHOPE network of hotlines by sharing of expertise.

The Hotline is very cognisant of the plight of the children who are being abused in the production of the illegal images reported to us. It is the goal of ISPAL in running the Hotline that the industry reacts quickly and plays its part in curtailing this misuse of the Internet to distribute these images. It must be emphasised that it is only An Garda Síochána who fulfil the role of law enforcement and conducting criminal investigations of the perpetrators of such content on the Internet. In any case of reported illegal content, once the Hotline has passed its assessment of the content and the technical Internet information it has gathered to the Gardaí, the Hotline's role is completed. The Hotline very much appreciates the support it has received for its operations over the reporting period from An Garda Síochána.

The report is testament to the effectiveness of self-regulation of the Internet in Ireland over the two-year reporting period. The ISPAL and Hotline are committed to ensuring as best as is practicable and within the constraints of the law that Irish Internet facilities should not be misused for the dissemination of illegal material. Unfortunately criminal intent in any field can never be eliminated and the INHOPE Hotlines are witnessing new measures of deception being employed. The Hotline must therefore continue to develop its skills if it is to contribute effectively to global measures being taken against illegal content on the Internet.

## INTRODUCTION AND HISTORY OF THE HOTLINE

The Internet and more particularly, the World Wide Web and e-mail, have positively transformed everyone's life and the way we conduct business. New services based on the Internet using fixed and mobile telecommunications are evolving and will undoubtedly continue this trend. When used for legitimate purposes, the Internet is a wonderful tool. It offers an inexpensive means through which people and businesses can communicate worldwide. It has brought immeasurable benefits to education, social services and has revolutionised the way commercial services can be accessed and transacted. Unfortunately, there is a minority who in parallel have developed negative uses for the facilities available on the Internet. The Industry is particularly aware that these downside issues must be countered, especially as the Internet is used by children, who must be taught its use as a modern life skill. Responding to this challenge is a matter for all of us.

While there are many potential dangers on the Internet, as in the physical world, child pornography is of particular concern. The Child Trafficking and Pornography Act (1998), is regarded by many legal commentators as one of the leading pieces of legislation in this area in the world. This law makes it illegal for anyone to knowingly produce, distribute, print, publish, import, export, sell, show or possess any child pornography. It is the main pillar allowing the Hotline and ISPs in conjunction with An Garda Síochána to work effectively against such material existing on the Internet in Ireland.

### HISTORY OF THE HOTLINE

In 1997, the Department of Justice, Equality and Law Reform established the Working Group on the Illegal and Harmful Use of the Internet and it presented its report in July 1998. The Working Group recommended a self-regulatory regime. This package of strategic measures focused on four main areas:

- The introduction of a system of self-regulation by the Internet Service provider industry, to include common codes of practice and common acceptable usage conditions.
- The establishment of a Hotline to investigate and process complaints about illegal material on the Internet.
- The report also instigated the establishment of the Internet Advisory Board (IAB) by the Department of Justice. The IAB's role is to monitor the efficacy of self-regulation in this context, and to enable ongoing dialogue between the Internet industry and all major stakeholders.
- Development of awareness programmes for users which will empower them to protect themselves, or others in their care, from illegal and harmful material on the Internet.

The Internet Service Providers Association had its inaugural meeting in April 1997 and by May 1998 was established as a not-for-profit company limited by guarantee.

Following extensive consultations with Government the ISPAI established a Code of Practice and Ethics on which the self-regulatory regime for the Internet industry in Ireland is based. This framework is the cornerstone on which initiatives have been built to curb misuse of Irish Internet facilities for the hosting and

dissemination of illegal material.

In this consultative process, special consideration was given to the fact that there is increasing use of the Internet by children in the educational environment and at home for entertainment and communication.



### **SPECIAL CONSIDERATION OF CHILDREN USING THE INTERNET**

There are usually three major concerns expressed in relation to children accessing the Internet:

- The Internet is a medium where people can find unpleasant or harmful content about children who are victims of paedophiles. Responding to this requires hotlines to initially receive complaints and international co-operation to fight these criminal activities.
- The Internet is a communication tool used by paedophiles to get in touch with children and entice them into liaisons. Combating this requires education and awareness programmes for children and parents.
- The Internet is a medium where children can accidentally or deliberately discover material that can be disturbing and harmful to them, depending on their age and stage of development. This requires parental supervision, technical tools and awareness programs.

To address all these dangers properly, a clear framework of co-operation was set up. It clarified the different tasks of the stakeholders involved (e.g., users, child welfare organisations, industry, governments and law enforcement), according to their knowledge, and their legal and technical means.

Following extensive consultation process between the stakeholders, Government and the ISPAI, the Hotline was launched in November 1999. The ISPAI funds the operating costs of the Hotline with support funding from the EU Commission's Internet Action Plan (1999-2004). The Irish Government, through the Information

Technology Fund, provided funds for the initial promotion and launch of the Hotline.

### **CURRENT DEVELOPMENT OF HOTLINE**

While originally introduced to combat child pornography on the Internet, the Hotline structure in this country can readily be applied to tackle other forms of illegal material. At present the public reports other suspected illegal content such as Internet based financial scams, racist material and illegal computer related issues (e.g. hacking instruction sites). Already, the Hotline accepts such reports and where possible passes them to the appropriate authorities. The EU Commission also encourages and supports European Internet hotlines to widen their scope. Under the coming EC programme, financial support is being provided to improve hotline processes to deal with racist and xenophobic content.

In January 2003, Cormac Callanan, the Director of www.hotline, was appointed to the full time position of Secretary General of the INHOPE Association (see section on External Relations). In February 2003, The Board of the ISPAI decided that a new position of General Manager should be created to run its Hotline service and this position was filled in February 2003 with the appointment of Paul Durrant.

## STRUCTURE OF THE HOTLINE

The Hotline is run as a service of the Internet Service Providers' Association of Ireland (ISPAI). The functions of the Hotline are those which were recommended by the Working Group on the Illegal and Harmful Use of the Internet and are listed in Appendix 1.

### ORGANISATION AND MANAGEMENT

The ISPAI is a not-for-profit limited company, established by Internet Service Providers operating in the Republic of Ireland. It is completely funded by the industry on a cost-sharing basis. A General Manager, who is an employee of the ISPAI, manages the administrative, financial and operational functions of the Hotline. The Hotline General Manager reports to the ISPAI Board of Directors.

### GOVERNANCE

The Internet Advisory Board, established in February 2000 by the Department of Justice, Equality and Law Reform, supervises self-regulation of the Internet Service Provider industry.

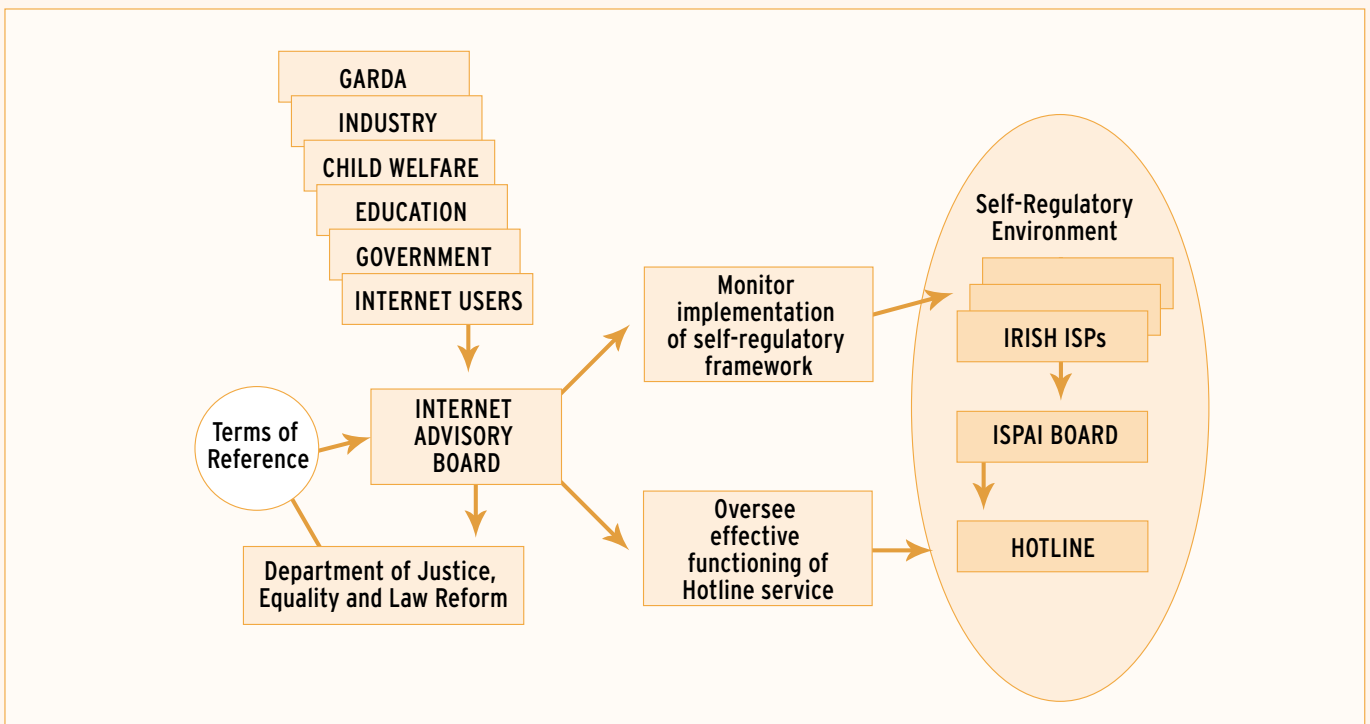
Members of the Board include representatives of the Internet service providers, An Garda Síochána, Internet users, Government, the Information Society Commission, education and child protection bodies, a legal advisor and the General Manager of the Hotline. This is illustrated in Figure 1.

Over the two year reporting period the Internet Advisory Board (IAB) has continued to oversee the Hotline and monitor the effectiveness of

self-regulation. It has undertaken many awareness initiatives to assist the public and businesses to understand downside issues of the Internet. A full description of its activities may be found in the Internet Advisory Board, Ireland, Report 2000 - 2002.

Through its continued support and promotion by the IAB, the Hotline has become increasingly used by the public. It is recognised as the established service in the country to combat illegal content on the Internet and is the tangible face of self-regulation of the Internet industry.

FIGURE 1 Hotline Governance



### EUROPEAN COMMISSION SUPPORT

The Internet Service Providers' Association of Ireland provides funding for the Hotline with the assistance of the European Commission.

The Directorate General Information Society provides the EU Commission funding by way of the "Internet Action Plan 1999 - 2004". More information on this Programme may be found at [http://europa.eu.int/information\\_society/programmes/iap/index\\_en.htm](http://europa.eu.int/information_society/programmes/iap/index_en.htm). Under this programme, a number of action lines exist where projects were selected on a competitive basis in response to a "call for proposals". The ISPAI [www.hotline.ie](http://www.hotline.ie) is a partner in a consortium of European hotlines that won funding for their project (INHOPE-2) under the previous call for proposals. This funding expired at the end of February 2003.

The formal extension of this Multi-annual Community Action Plan was approved by Decision No. 1151/2003/EC of the European Parliament and of the Council on 16 June 2003. The ISPAI has applied for renewed funding for the Hotline, as a "project", under the associated "call for proposals" which closed on 14th November 2003. The new contract is under negotiation at the time of writing. If successful, this will provide 50% funding of allowable Hotline running costs for a further 2 years.

## EXTERNAL RELATIONS

The usefulness of the Hotline would be extremely limited if it could only deal with Internet content hosted or distributed from within the Irish jurisdiction. To be effective and successful in its goals, the Hotline must have an International dimension.

The Hotline addresses the issue of responding to reported content that is outside the Irish jurisdiction, through two means:

- Membership of the INHOPE Association ([www.inhope.org](http://www.inhope.org)) and,
- An Garda Síochána contacts who liaise with International police organisations such as Interpol and Europol.

### INHOPE ASSOCIATION

The [www.hotline.ie](http://www.hotline.ie) service is a founding member of the INHOPE Association (INTERNET HOTline Providers in Europe). INHOPE's mission is to facilitate and co-ordinate the work of European Hotlines in responding to illegal use and content on the Internet. It facilitates good working relationships between European hotlines and the exchange of reports by ensuring trust built on a rigorous hotline approval process. It interfaces with initiatives outside Europe to forge working relationships with hotlines around the World and to build an increasing co-operative network. Expertise is shared through regular INHOPE meetings, where training sessions on specific aspects of the Hotline work are run and working sessions develop best practices for the operation of Internet hotlines and tracing of illegal content.

The key functions of the Association are to:

- Exchange expertise
- Support new hotlines
- Exchange reports

- Interface with relevant initiatives outside the EU
- Educate and inform policy makers, particularly at the international level.

Its goals are to:

- Establish and resource effective national hotlines.
- Train and support new hotlines
- Foster ongoing Internet safety awareness and education throughout Europe
- Establish effective common procedures for receiving and processing reports.

In addition to the fifteen member hotlines in Europe, there are three members covering the United States of America, Australia and Korea. Appendix 3 provides a full list of the INHOPE members.

INHOPE provides a forum for hotline staff to learn from each other. This is vital as the technological facilities of the Internet are continually evolving. Unfortunately, as with any other field of human endeavour, criminal elements using the Internet are also evolving their methods to try and avoid detection. INHOPE provides a forum to allow technical knowledge and the experiences gained to be shared among hotline staffs. Through seminars and conferences which have been organised by Inhope members, this knowledge is also shared with the law enforcement fraternity.

### [www.hotline.ie](http://www.hotline.ie) INPUT TO INHOPE

The General Manager of the Hotline represents the organisation as a member of the General Assembly of the INHOPE Association. Cormac Callanan, while Director of [www.hotline.ie](http://www.hotline.ie), was instrumental in establishing INHOPE, being a member of the executive from the outset and serving as President of the Association from May 2001 to May 2002. He was appointed full time Secretary General of INHOPE in January 2003.

The Hotline, through Cormac Callanan, participated very actively in developing the INHOPE organisation, instigating planning meetings for all members, organising training courses and developing the original INHOPE web site. This organisation is now well established and operational co-operation between its members has provided key information that has initiated many successful police actions against child pornographers throughout the world.

In addition, the Hotline Director (and subsequently, the General Manager) has actively contributed to all meetings of the General Assembly in the period (Copenhagen, Sept 2001; Madrid, Jan 2002; Berlin, May 2003; Cambridge, 2002; Dublin, February 2003; Reykjavik, May 2003). Special working groups have been set up to tackle specific issues and the Irish Hotline staff has served on these. Currently Paul Durrant is Chairperson of the Statistics Working Group, tasked with defining common standards and definitions for the recording, collating and analysis of reports submitted to INHOPE Hotlines.

Cormac Callanan chaired the working group on Code of Practice Development and was involved in producing best practice papers on exchange of reports and staff welfare.

By actively taking part in these exchanges at INHOPE meetings, during the period, the Irish Hotline has benefited from case expertise gained from other countries. But equally, Ireland has brought innovative strategies and procedures and provided leadership to the overall INHOPE organisation.

#### **OTHER INTERNATIONAL ACTIVITIES**

The Hotline has contributed its expertise at many international events dealing with cyber-crime. The Hotline Director was an invited participant at the 2001 Annual High Level Experts Meeting on Cyber-Crime by Europol, represented INHOPE at the Symposium on the Protection of Children Online held in Hong Kong in March 2002 and was also an invited speaker at the UN Symposium "The Rule of Law in the Global Village" in December 2002 in Palermo Italy, which took place during the high level signing conference of the UN Convention on Trans-national Organised Crime.

The Hotline has also contributed strongly to the continued development of the international hotline network. The Hotline Director provided regular advice from October 2001 to May 2002 to assist the establishment and operation of the Icelandic hotline, co-ordinated the full hotline reviews held in Luxembourg in April 2002 and, as President of INHOPE, co-ordinated the application for funding of a consortium of INHOPE hotlines which successfully won an EU Commission contract (INHOPE-2 project) which was in operation from September 2002 and continued through the end of this reporting period.

## OVERVIEW OF THE WORK OF THE HOTLINE

This section explains the daily work of the hotline and how reports are processed by the service.

### ROLE OF THE HOTLINE

The [www.hotline.ie](http://www.hotline.ie) service, run by the ISPAI, is the main component of self-regulation by the ISP industry in Ireland, to combat Internet facilities in this country being misused to host or distribute illegal content. To respect the privacy of the individual and comply with the privacy laws of the country, ISPs must act in a reactive way. That is, should illegal content be reported to them, the hosting ISP will endeavour to promptly remove it from public access.

The Hotline exists to receive reports from the public about potentially illegal material, so it may be assessed and, if considered to be probably illegal, to instigate its removal from the Internet. The Hotline treats all reports from the public with complete confidentiality. Reports may be submitted by the following methods:

- via the secure website ([www.hotline.ie](http://www.hotline.ie)),
- via email ([report@hotline.ie](mailto:report@hotline.ie))
- via "lo-call" phone service (1890 610 710)
- via "lo-call" fax service (1890 520 720)
- via post (26 Upper Baggot Street, Dublin 4, Ireland)

Reports can be anonymous if desired.

When the Hotline receives a report it follows a procedure which has been agreed with the Internet Advisory Board, An Garda Síochána and with the Internet Service Providers.

The Hotline also worked closely with the Internet Service Providers, An Garda Síochána and the Data Protection Commissioner to develop a protocol for the controlled exchange

of personal data in the course of a criminal investigation.

### The overwhelming majority of suspect material encountered by the Irish public on the Internet originates outside the State.

Processing reports from the public of alleged illegal material is time consuming and involved process. The Hotline provides assistance to An Garda Síochána by filtering reports to determine what is probably illegal and is also located in Ireland or has an Irish dimension. This assists the Gardaí to dedicate their specialist resources to pursuing investigations within the jurisdiction by not having to deal with the majority of reports that do not contain illegal content or relate to material held in other jurisdictions.

As the Internet is a truly global facility, it is vitally important that Ireland is seen to actively play its part in International efforts to curb illegal use of the Internet. Through the Hotline's membership of INHOPE (the International network of Hotlines) and its well established cooperation with An Garda Síochána, who in turn work through Europol and Interpol, Ireland is recognised by the International community as being committed to this goal. Ireland is also an International leader in the development of an ISP Code of Practice and Ethics that is truly effective and, as this report shows, has an excellent record of ensuring that Internet facilities located in the country are not used to host and disseminate illegal material.

### SCOPE OF HOTLINE

There have been calls from many groups that ISPs should be more proactive in preventing illegal use of Internet services. The Hotline is the primary component of this response but it must be recognised that there are limitations, both legal and practical, that apply to its operations and those of the ISPs in relation to finding and dealing with 3rd party content.

The Hotline can not engage in pre-emptive searching for illegal material under the procedures that were agreed with Government - nor has it the resources to do so if it could. The Hotline can only react to reports from the public who have encountered suspected illegal content (presumably accidentally) when using the Internet or who have had such content sent to them as e-mail. It is on such reports received that the Hotline carries out its task under carefully controlled procedures which reflect INHOPE best practice developed from the experience of its collective hotline members.

ISPAI members strive to be responsible corporate citizens and co-operate fully to support the Hotline in its tasks. They have clear "Acceptable Usage Policies (AUPs)", to which customers agree to adhere on signing up to Internet services and the sanction for breaking these is discontinuance of service. However, under Irish telecommunications and privacy laws, ISPs can only react when probably illegal content is notified to them or when they become aware that AUPs are being broken. The Hotline is acknowledged by ISPs as having the expertise to be authoritative in determining that content is probably illegal. If an ISP receives notification for "take-down" from the Hotline, it will act very promptly to that notice.

## PROCEDURES OF THE HOTLINE

The Hotline's operational process starts when a submission is received from the public or from another international hotline. The submissions are generated through electronic forms that are available on the [www.hotline.ie](http://www.hotline.ie) web site or alternatively by email, telephone, fax or letter. When a submission is received, the Hotline will send an acknowledgement where contact information has been given. The preference is to provide this reply by e-mail.

A single submission may contain a complaint about a single item or multiple items encountered on the Internet. A report record is opened in the Hotline database for each item (or related set of items) cited in the submission. The relevant details about the content are extracted from the submission and logged into the report record. The original submission is then archived.

Under the legal system in this country, only a court of law can determine that a criminal offence has been committed and that material (i.e. child pornography) relating to that offence is actually illegal. Therefore, the Hotline can only determine that something is "probably illegal". Hence this term is used throughout the report.

Once the report has been logged, a trained member of the Hotline staff will try to find the material on the Internet. Taking as an example a report of suspected child pornography, if the subject of the report is found, it will be assessed as to whether it is probably illegal under the Irish Child Trafficking and Pornography Act (1998). If it is not illegal, no further investigatory action is taken. A brief

note on the determination is recorded in the database and the report is closed. However, if the content is considered to be probably illegal under this act, the next step is to determine the location of the material as accurately as possible.

The Hotline staff use a suite of tools and their experience to attempt to trace and locate the source, be it a web host server, e-mail server or other Internet based service. While in most cases a country and hosting network can be found, unfortunately (particularly in relation to e-mail) Internet tracing down to the originating server is not always possible under current conditions. Dates, times and details of the trace are recorded in the Hotline database as a source of evidence if required by law enforcement agencies.

If the reported material is located on an Irish based server then the ISP managing that server is identified. The Hotline then issues notification to An Garda Síochána and simultaneously a "take down" notice is issued to the ISP. The ISP is responsible for the timely removal of the specified probably illegal content from their servers to ensure that other Internet users cannot access the material. Once this notification is complete, the Hotline records the action that was taken in the database and closes the report. The decision to initiate a criminal investigation is a matter for An Garda Síochána.

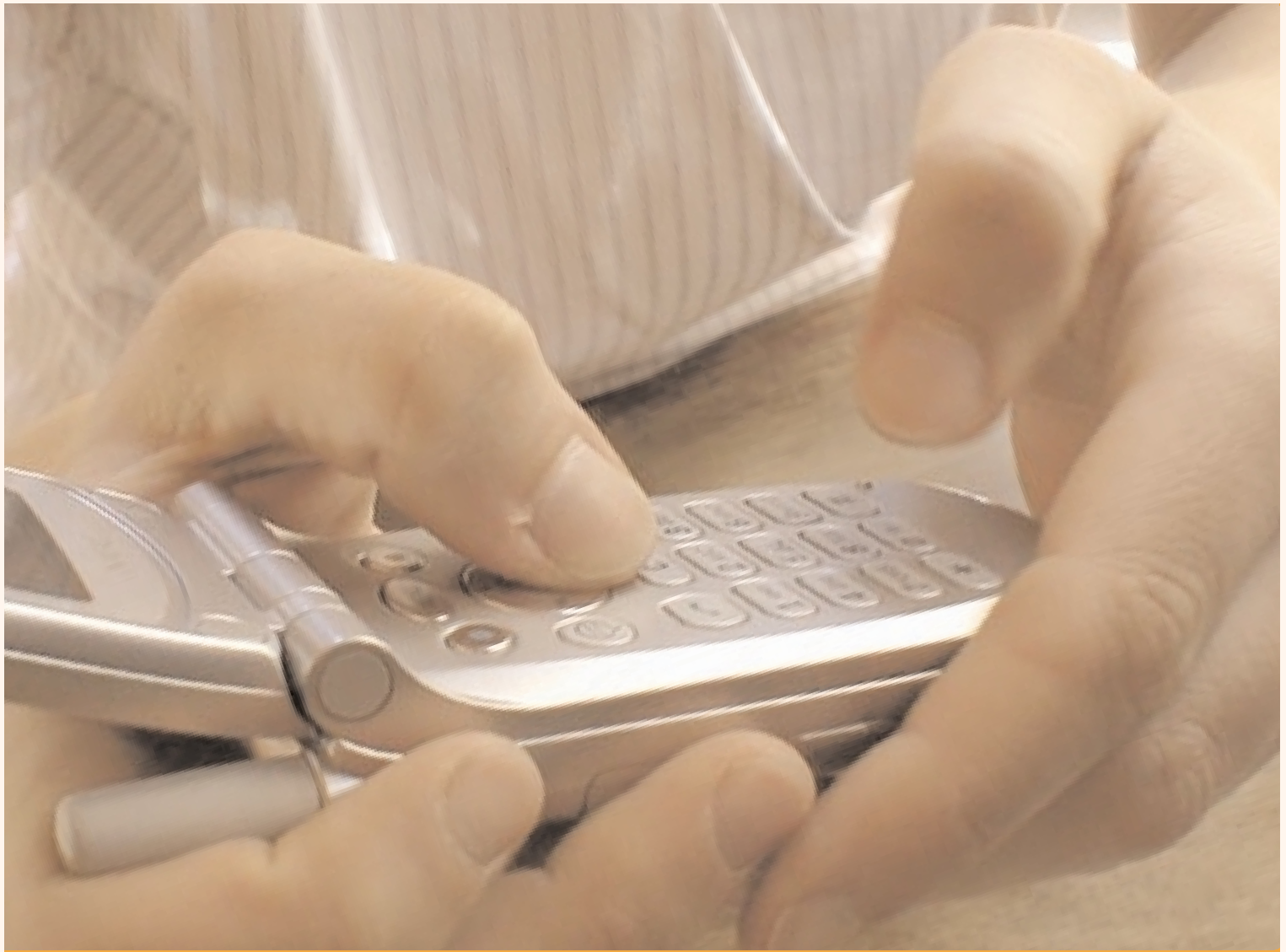
If the material is located on a server in a country where there is an INHOPE hotline, then details based on the original report, including the Hotline's findings, are forwarded to the other hotline for processing. The case report is

then closed within the [www.hotline.ie](http://www.hotline.ie) service.

If the material is located in a country having no INHOPE presence, the Hotline will attempt to have action taken by the following means:

- Details are provided through an established contact in An Garda Síochána for transmission to the source country through international law enforcement channels.
- Where there is an established relationship between an ISP in the source country and a parent ISP in an INHOPE country, a report is submitted to the INHOPE hotline for transmission to the hosting ISP organisation.
- Where the report is about potentially illegal UCE and an abuse desk exists in a reputable ISP, an e-mail report is sent to alert of the misuse of the account.

Unfortunately it is a reality that there are a considerable number of countries where none of these actions are possible. It is only through concerted government and international community pressure through diplomatic channels that change in this area will come about over time. However, it is important that responsible countries like Ireland and our INHOPE partners continue to lead the way.



*The Hotline's preferred method of receiving reports is via the web forms provided on the [www.hotline.ie](http://www.hotline.ie) web-site. This provides a structured report format that allows the receiving, report detail logging and preparation of information for investigation to be processed semi-automatically. This saves a lot time by eliminating manual extraction of information from free-form e-mails.*



## STATISTICAL ANALYSIS OF HOTLINE REPORTS 1ST JULY 2001 - 30TH JUNE 2003

The First Report of the Hotline covered the period from the Hotline's establishment in November 1999, to the end of June 2001. This, the Second Report, follows on from this and covers the period from the start of July 2001 to the end of June 2003.

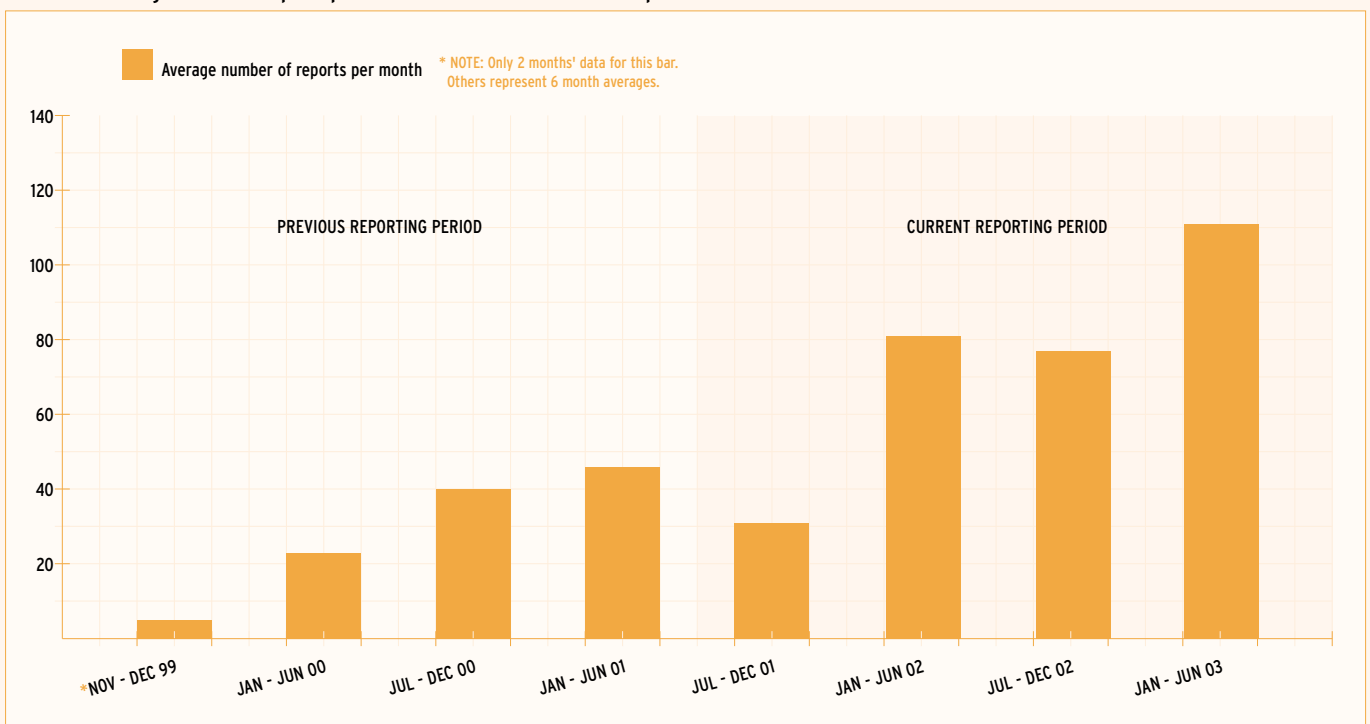
### LEVEL OF REPORTING TO THE HOTLINE

The Hotline primarily receives reports from the public about content that they have encountered while using the Internet and which they suspect to be illegal. In the two year period from 1st July 2001 to 30th June 2003 the Hotline received 1792 reports from the public. This is a marked increase on the 671 reports that the Hotline received in the 20 months from its inception (November 1999) to the end of June 2001 (first reporting period).

A more meaningful comparison is possible between the two periods if the first period is extrapolated to 24 months. An equivalent level of reporting by the public would have resulted in 805 being received. Using this number as a basis for calculation, 1792 represents more than a doubling of reports (approx. 123% increase) since the last period. This trend of increase over the two periods is shown in Figure 2 below.

As already stated, the Hotline does not undertake any pre-emptive searching for illegal content on the Internet. Therefore report numbers represent the reaction of the public to material they have encountered on various facilities provided on the Internet or which was sent to them as e-mail.

**FIGURE 2** Average number of reports per month received in each six month period since the Hotline was established.



**TABLE 1 METHOD USED BY THE PUBLIC TO SUBMIT REPORTS TO THE HOTLINE**

REPORTING METHOD	Reports Received		Reports Received	
	Current Reporting Period		Previous Reporting Period	
	(July 01 to June 03)		(Nov. 99 to Jun. 01)	
Hotline website form	807	45.0%	451	67.2%
e-Mail	926	51.7%	168	25.1%
Telephone	53	3.0%	27	4.0%
Fax	0	0%	0	0%
Letter	4	0.2%	20	3.0%
Referral from INHOPE	2	0.1%	5	0.7%
<b>Total</b>	<b>1792</b>	<b>100%</b>	<b>671</b>	<b>100%</b>

**TABLE 2 INTERNET SERVICE AT TARGET OF REPORT RECEIVED**

INTERNET SERVICE	Reports Received		Reports Received	
	Current Reporting Period		Previous Reporting Period	
	(July 01 to June 03)		(Nov. 99 to Jun. 01)	
Web	726	40.5%	574	85.5%
Spam	864	48.2%	2	0.3%
Peer to Peer	25	1.4%	0	0%
Newsgroups	13	0.7%	17	2.5%
e-Mail	30	1.7%	28	4.2%
Chat	17	1.0%	8	1.2%
Other (i.e. not specific)	117	6.5%	42	6.3%
<b>Total</b>	<b>1792</b>	<b>100%</b>	<b>671</b>	<b>100%</b>

**TABLE 3 SUSPICION STATED OR IMPLIED IN REPORTS RECEIVED**

SUSPICION	Reports Received		Reports Received	
	Current Reporting Period		Previous Reporting Period	
	(July 01 to June 03)		(Nov. 99 to Jun. 01)	
Child Pornography	1261	70.4%	567	84.5%
Adult Pornography	159	8.9%	18	2.7%
Racist Material	3	0.2%	1	0.1%
Illegal Material	131	7.3%	26	3.9%
Terrorist Related	0	0%	2	0.3%
Financial Scam	22	1.2%	2	0.3%
Drugs Related	0	0%	1	0.1%
IPR violation	0	0%	3	0.5%
Virus Attack	7	0.4%	2	0.3%
Spam e-Mail	38	2.1%	4	0.6%
Query	125	7.0%	39	5.8%
Complaint	4	0.2%	1	0.1%
Other	42	2.3%	5	0.8%
<b>Total</b>	<b>1792</b>	<b>100%</b>	<b>671</b>	<b>100%</b>

### ACCESSING THE HOTLINE

The public can contact the service via a number of methods. Reports for investigation that may have an Irish dimension are also forwarded from other INHOPE member Hotlines. Table 1 shows the number of reports received by these various methods.

The Hotline's preferred method of receiving reports is via the web forms provided on the [www.hotline.ie](http://www.hotline.ie) web-site. This provides a structured report format that allows the receiving, report detail logging and preparation of information for investigation to be processed semi-automatically. This saves a lot time by eliminating manual extraction of information from free-form e-mails.

The telephone, while associated by the public with Hotlines, is probably the least efficient method. It requires the recording to be manually transcribed and then entered into the database. There are relatively few telephone reports in total. Most of these are made after business hours and therefore are left on the automated answering system. In the majority of cases insufficient detail is given to allow the Hotline find the suspected content. Also, as the calls are generally anonymous, the Hotline can't return the call to obtain clarification.

While the Hotline continues to have 1890 "Lo-Call" numbers for phone and fax reporting, the aim is to encourage all reports to be submitted via the forms on the [www.hotline.ie](http://www.hotline.ie) web site.

### INTERNET SERVICE WHERE THE CONTENT OF CONCERN IS LOCATED

The Internet offers many different communication services such as e-mail, web pages, chat rooms, newsgroups, etc. It is interesting to note the proportion of reports attributable to each Internet service as shown in Table 2.

The most startling result is the enormous growth in reports generated as a result of spam. This warrants further examination and is discussed separately under "Increasing incidence of spam" in the section "Issues Arising".

### SUSPICION UNDERLYING REPORTS

To gain an understanding of what the public perceives as being offensive on the Internet, it is worth analysing the nature of the material that has triggered the sending of a report. The Hotline endeavours to establish this on the reporting forms available on the web site. The reporter is requested to identify the closest match from a list of possible options: child erotica, child pornography, racism and other.

The reporter's optional description often allows the Hotline to categorise the nature of the material more precisely. Many reports are also made by e-mail and a few by telephone, fax and post. In these cases, the reporter often does not make a direct statement of their suspicion but, in processing the report, the Hotline operator selects the most appropriate category from the description provided. Where the intended suspicion is not clear, it is classified as "other". Table 3 enumerates reports received by category of the suspected material.

Most of the categories in Table 3 are self-explanatory (a description of the categories is provided in Appendix 4), however an explanation of how the Hotline categorises spam e-mail is warranted. During the reporting period, the action of sending spam was not illegal within this jurisdiction. (This situation has changed with the transposition of recent EU Directives on data privacy into Irish law.)

In categorising a report, most people will select a suspicion irrespective of the medium, so if a spam advertises (for example) a financial scam, they will classify it as such. The Hotline endeavours to classify the reports according to the suspicion, that is, type of potentially illegal material. Therefore a spam e-mail reported as suspected advertising of child pornography is classified under "Child Pornography" not "Spam e-mail". However, sometimes the reporter is complaining simply about the volume of spam being sent to them irrespective of the content of the spam. It is in these cases that the Hotline classifies the suspicion as "spam e-mail".

To assist in the interpretation of the data, the possible categories are grouped together as shown in Table 4.

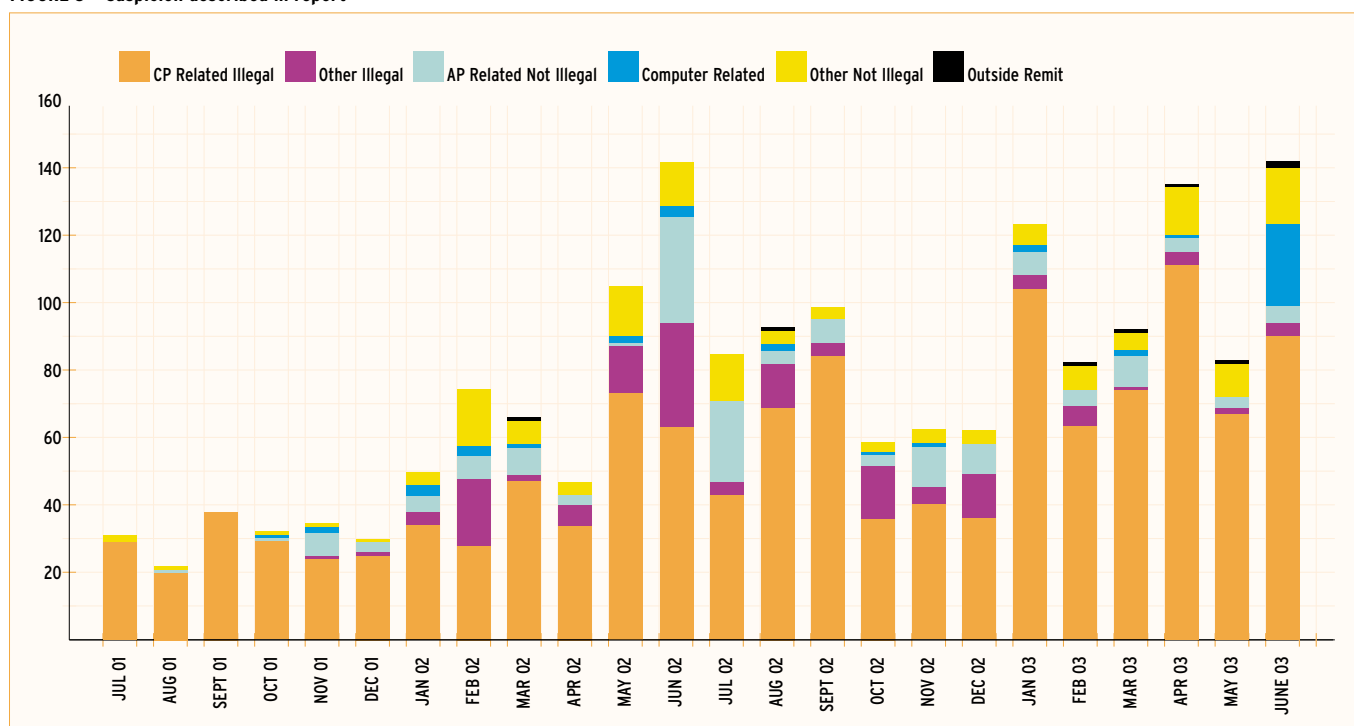
Figure 3 shows the suspicion described, or implied by, the person who submitted the report. This is prior to any Hotline determination. It shows that with the exception of a few anomalous months (e.g. June 2002), a relatively consistent proportion of reports submitted per month are suspected child pornography. Over the two-year period, an average 70% of all reports, was suspected child pornography or related material (including 30 reports citing child-erotica as the suspicion).

**TABLE 4 GROUPING OF REPORT CATEGORIES FOR ANALYSIS**

CP Related Illegal	Other Illegal	AP Related Not Illegal	Computer Related	Other Not Illegal	Outside Remit
Child Pornography	Financial Scam	Adult Pornography	Virus Attack	Nudism	Outside Hotline Remit
CP Jump Site	Racist Material	Extreme Adult	Spam Email	Insufficient Detail	Complaint
Child Abuse	Illegal Material	Adult Jump Site	Hacking Site	Query	
Child Trafficking			IPR Alleged Violation	Other	
Child Erotica *					

\* Note: Child Erotica images, while not actually illegal under Irish law, have been categorised here for completeness (see Appendix 4).

**FIGURE 3 Suspicion described in report**



**HOTLINE DETERMINATIONS**

Every report submitted to the Hotline is investigated. A member of the Hotline staff will attempt to find the reported content for assessment. However, the content may not be found due to:

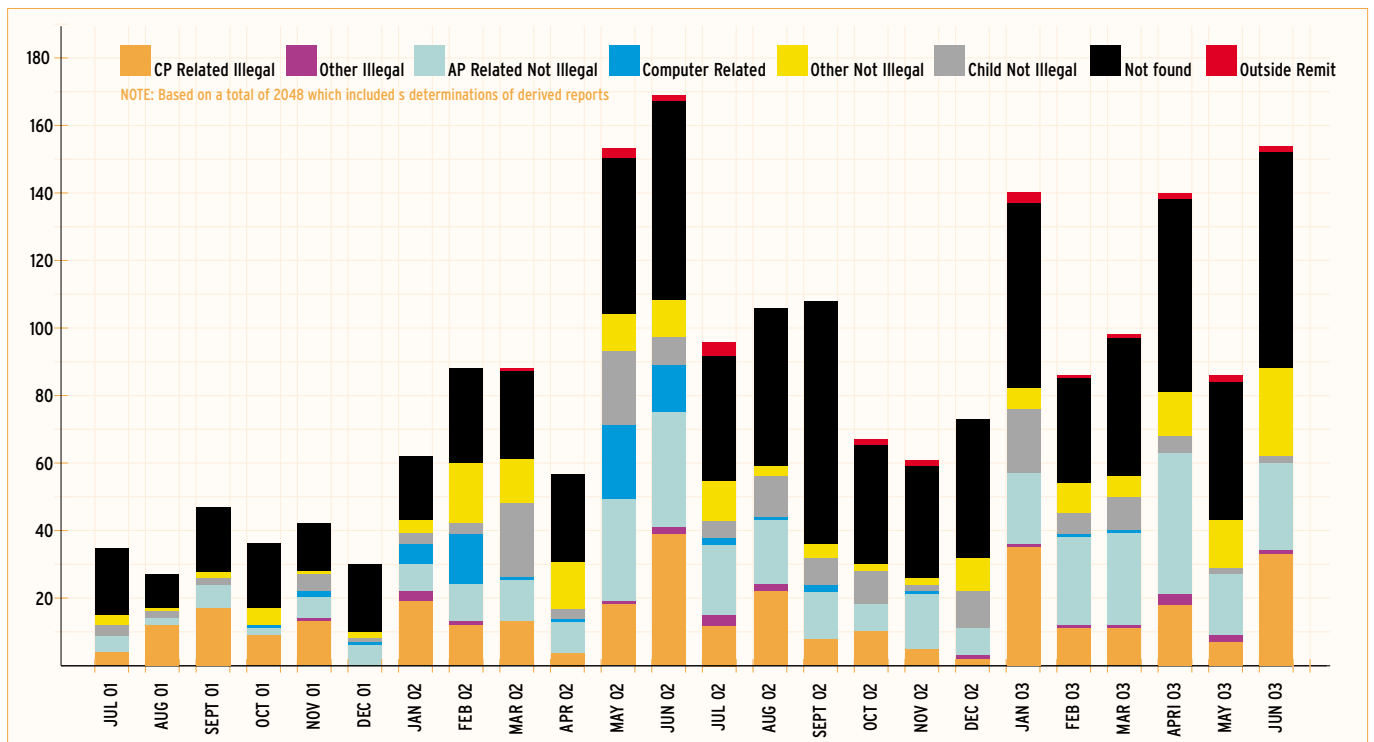
- The reporter has given insufficient information to allow the Hotline find the particular web page. Often sites do not have navigation to lower directories and having the root domain name is insufficient. This is particularly the case for free web space on hosting sites like "geocities.com" or "terra.com.br". The Hotline requests everyone to provide as full a page address (URL) as possible.
- The site has already been taken down by the hosting ISP as the undesirability of the content has already been brought to their attention. Often, this is because they have been informed that spam has been used to advertise the site, this is a breach of their usage terms and so the ISP removes the site irrespective of the content.
- The site has deliberately been moved to a different server by the owners to avoid detection. This is becoming an increasingly common practice. The Hotline has observed some sites being moved four times and more within 24 hours. Also, this principle applies to peer to peer file-sharing systems where users with illegal files may make them available for a short time only.
- The actual URL is found by the Hotline but the material described has been changed by the site owners and the particular image referred to in the submission can not be located.

In this reporting period, the content referred to in 42% of all reports was not found by the Hotline. This is discussed further in "Quality of Reports" in the "Issues Arising" section.

If the reported content is found, the Hotline staff member uses their expertise to assess, whether in their opinion, the content would probably be illegal in this jurisdiction.

In a considerable number of reports, the Hotline finds that the reported page actually links to other sites and, if these also contain

**FIGURE 4 Hotline determination of reported material**



illegal material, they must not be ignored. For example, this often occurs when the reported page turns out to be a single advertisement page which contains images of child pornography. The images are actually advertising three other sites all apparently offering child pornography and are hyperlinked to those sites. The Hotline will verify if these target sites in fact contain child pornography. For each one that does, a new activity is recorded - effectively this is a Hotline generated report. The Hotline refers to these as "derived" reports.

Derived reports always refer to illegal material and therefore increase the proportion of illegal content found relative to reports originating from the public. This is not pre-emptive searching, the Hotline is only reacting to reports from

the public in the first instance but finding that additional report records are necessary to capture and take action against what has been found.

Over the two-year period, "derived" reports increased the total number of reports processed from the 1792 reports received from the public, up to a total of 2048. In analysing the determinations this larger number has been used.

Figure 4 shows the assessment of the target content as determined by the Hotline and is based on a total of 2048 reports which includes "derived reports".

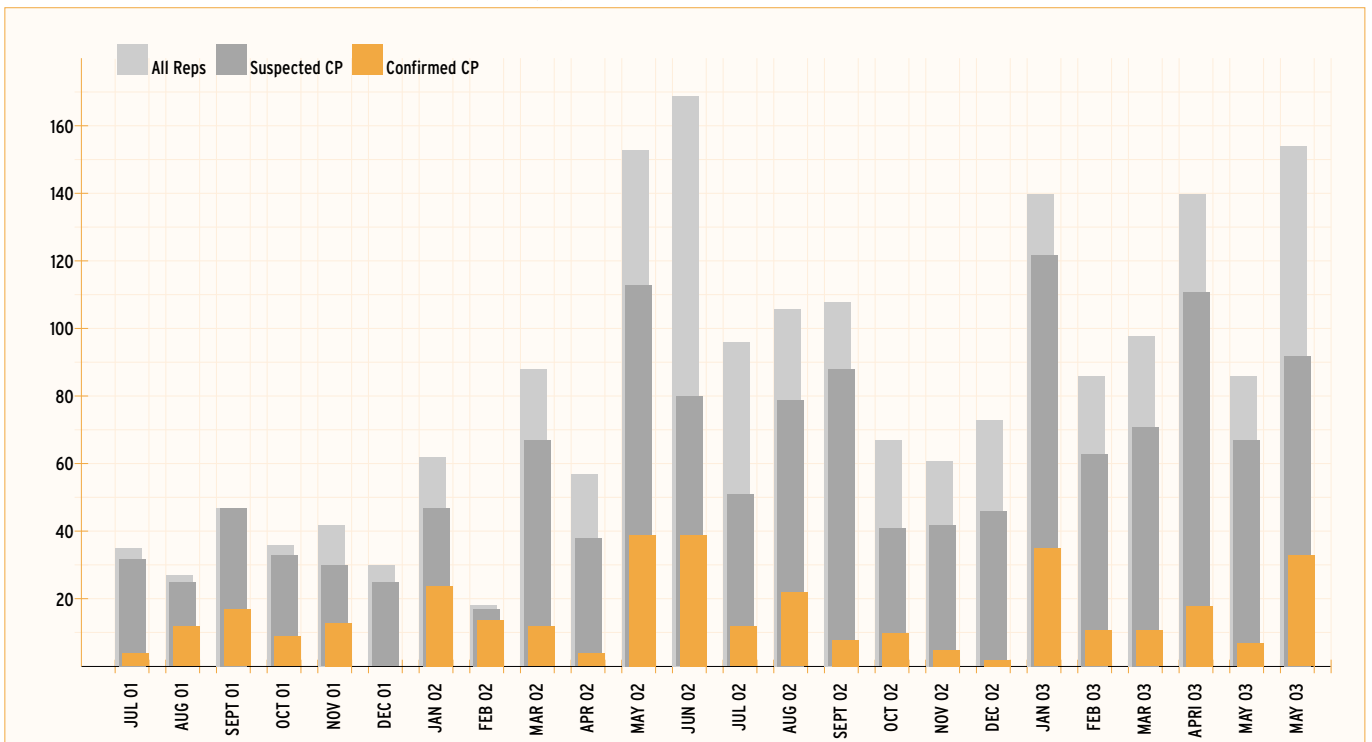
Two outstanding features can immediately be seen:

- The large proportion of reports where the target content simply can not be found, and
- The significant reduction in the number of reports that prove to be child related.

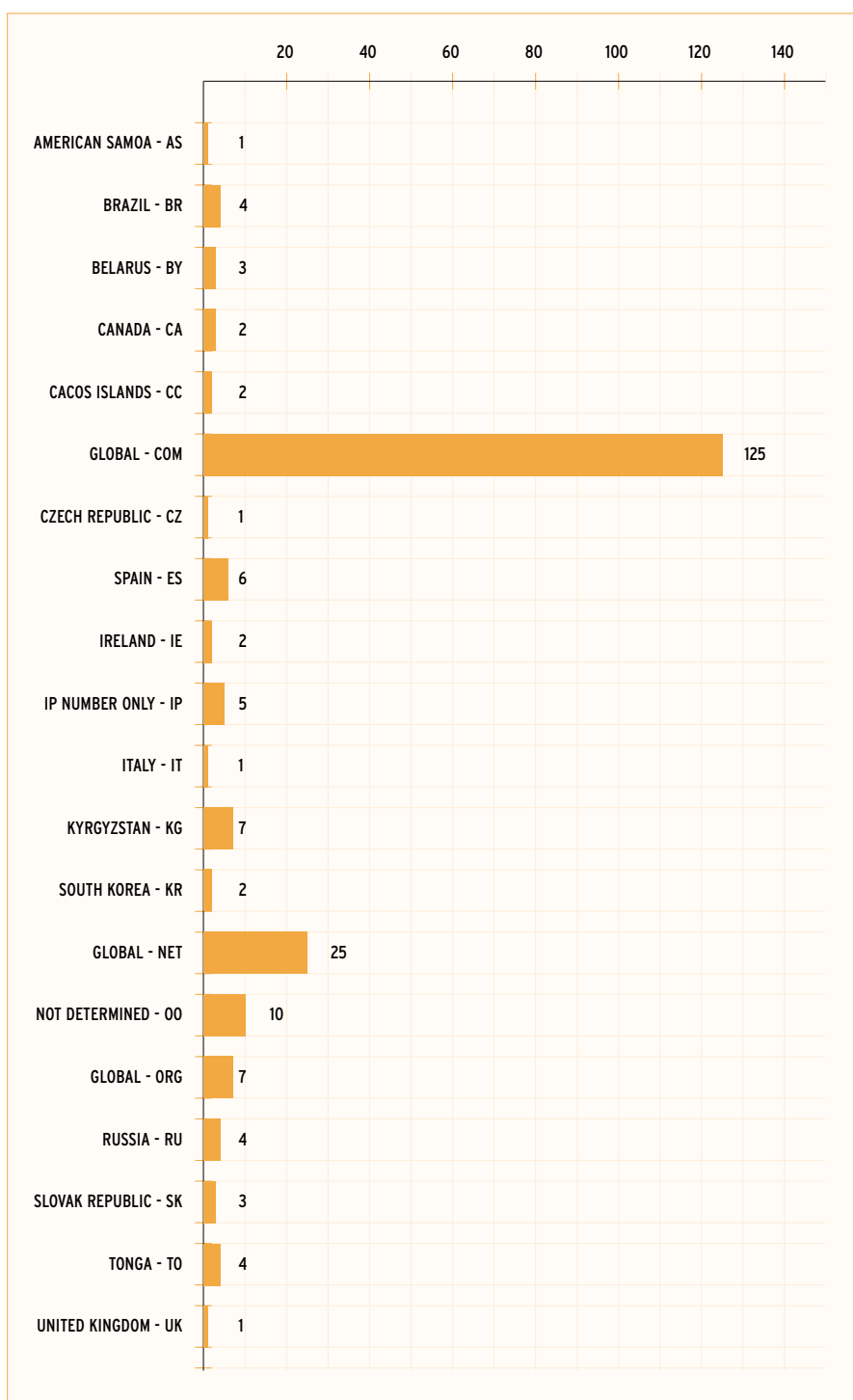
In the majority of cases where child pornography was suspected and the Hotline succeeded in locating the reported content, the material was determined to be actually adult pornography.

This is shown strikingly in Figure 5 where the child pornography related suspicions and actual determinations are compared to the total number of reports.

**FIGURE 5 Comparison of Suspected to Determined Child Pornography Reports**



**FIGURE 6 Top level domain of reported illegal material**



It must also be remembered that the Hotline derived reports actually inflate the number of CP determinations, as these are only added when a reported site points to other illegal content. Despite the growth in reporting, the number of determinations of illegal content remains a relatively small proportion of all reports.

It must be emphasised again, that the Hotline does not engage in any pre-emptive searching. All reports are generated by the public or out of investigation of those reports by the Hotline.

It is worth adding that it is not possible for the Hotline to follow up every link presented on index sites as these can point to many hundreds of web pages. With the increasing number of automated index sites, this can lead to circles of links to mainly adult pornography sites that yield nothing illegal. In these cases, adhering to INHOPE practice, the Hotline investigates five links which are randomly selected. If any of these prove to contain probably illegal content a derived report is recorded for each that does.

Over the reporting period there were a total of 357 reports, including derived reports, where the target content was assessed as probably illegal under the laws of the Republic of Ireland and further action was required.

334 were child related and 23 related to other illegal activities. It is of note that there were an additional 192 reports of child related images which were determined as “child erotica”, which are probably not illegal under Irish law. These are not included in the confirmed CP numbers.

### LOCATION OF SITES

Where a determination is made that content is probably illegal, the next step is to find the source country. When the target of the report is a web page, chat room, discussion group, etc., the Hotline tries to find the country and organisation that is hosting the content.

Alternatively, if the material is e-mail or a Usenet posting, the Hotline tries to trace the server from which it was originally sent. If there are references to web addresses in the e-mail or posting, the location of these will also be traced.

This process is time consuming as often the actual content is at the end of a chain of sites. It is also a common practice for the images to be held in a different location to the framework of the site. The Hotline has a suite of tracing tools at its disposal and it is generally possible to find the organisation that provides network access to the server on which the content resides. After removal of reports referring to the same content (duplicates), there were 215 unique cases determined as probably having illegal content under Irish law.

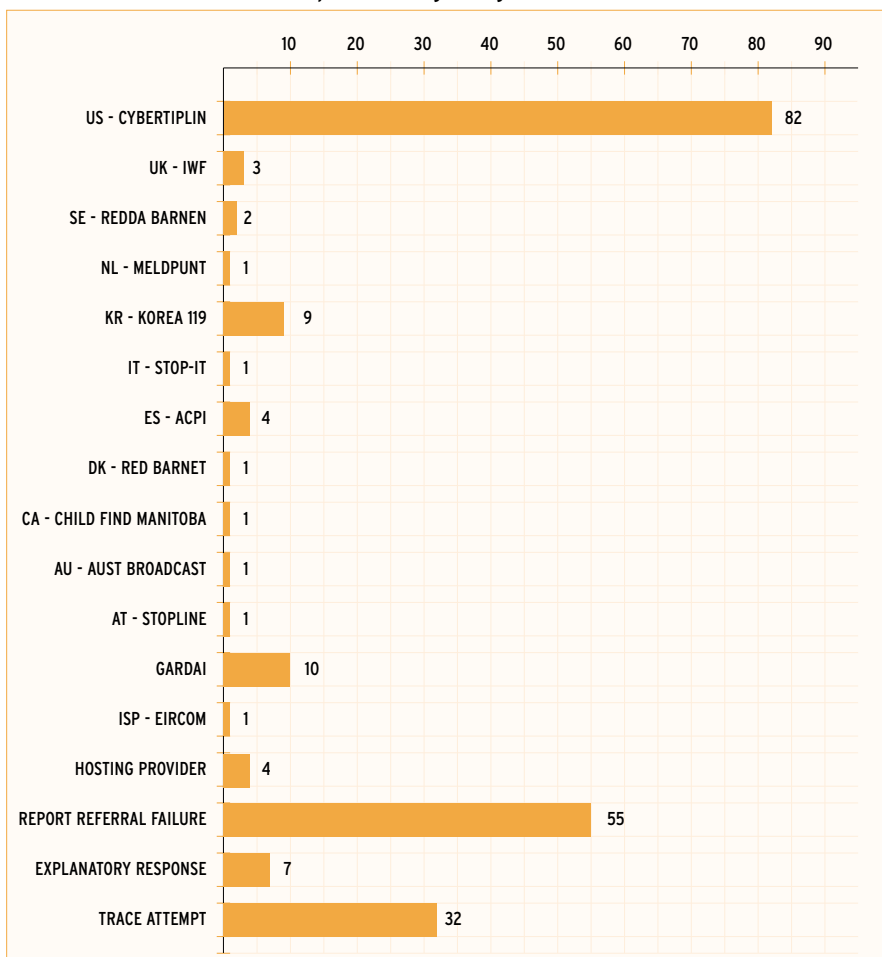
The bar chart (figure 6) shows the incidence (number of reports over the two year period) of top level domain (TLD) names among these 215 reports. Obviously global TLDs can be located on servers in any country. However, it is important to realise that even where a country name is the TLD, this is not necessarily the country in which the server is actually located. This occurred in the case of two .IE reports, both of which referred to the same content, which was actually hosted outside Ireland. In the two year period there has not been a single valid report where the content turned out to be

hosted in Ireland. The 00 designation is used where a domain name or IP address could not be ascertained. Usually these are spams where the content of the spam itself was actually illegal but the reporter did not provide sufficient information to allow the source to be traced.

This chart (Figure 6) should be compared to Figure 7, which shows the country where the content was apparently hosted when actually traced by the Hotline. Unfortunately, the traced apparent origins of countries were not readily extractable from the Hotline database where a

report was forwarded through an Garda Síochána or where there was a "Report Referral Failure". This facility is being added to the database and will be available for analysis in future Hotline reports.

**FIGURE 7 Actions undertaken for reports referring to illegal content**





### **ACTIONS ON ILLEGAL MATERIAL: SOURCE DETERMINED TO BE WITHIN IRELAND**

In the two year period there were no valid reports of content hosted or originating inside Ireland, therefore the national procedure was never invoked. The Hotline has however informally advised site owners based in Ireland whose content, while hosted abroad, had been compromised (generally due to hijacked domain names provided on links) without their knowledge. For examples, see section "[Samples Cases](#)".

### **ACTIONS ON ILLEGAL MATERIAL: SOURCE DETERMINED TO BE OUTSIDE IRELAND**

Where possible, the Hotline co-operates with its INHOPE partners and other organisations in the International effort to combat child pornography on the Internet. This is achieved by rapidly forwarding to partner Hotlines, detailed information of potentially illegal content appearing to be hosted in their countries, so they can take appropriate action.

As can be seen from figure 7, 105 reports were forwarded to INHOPE member Hotlines and one to an established Hotline service in Canada. One report was made to Eircom.net about a newsgroup. (This referred to a sub-group, far down the group hierarchy, which was maintained in another jurisdiction and was being replicated in the Eircom newsgroup listings. When some of the message postings in the group were brought to Eircom's attention by the Hotline, they immediately removed the offending subgroup from newsgroups they list.)

Where there is no INHOPE hotline in the source

country and the reported material is assessed as illegal in Ireland, the report is forwarded to An Garda Síochána. They then pass the information through international police channels to the appropriate authorities in the source country. All ten reports passed to the Gardaí in the two year period fell into this category.

32 of the reports could not be traced to completion (called "trace attempt" on the chart). The usual reason for the failure that the report refers to spam which contains illegal text or images. However, as delivery headers are not included in the report, the Hotline can not trace the source. Other causes of trace failure are forged or incomplete domain registrations and indeterminate IP Network Information Centre registrations.

On some occasions the Hotline provides "explanatory responses" to reporters of content that is determined as being probably illegal in this jurisdiction but there is no other course available to the Hotline. There were 7 such cases in the two years. A typical example would be a report of known site where the contents would probably be regarded as illegal in the Republic of Ireland but the Hotline knows it is not illegal in the source country due to some technicality. This can arise when the legal age definition of a child or, where the definition of what constitutes an illegal image of a child, varies between jurisdictions.

Where there is no hotline in a country, www.hotline may occasionally make a report to the abuse desk of the ISP in that country (4 cases in the period). This is usually in circumstances where spam is being relayed

through a reputable ISP in one country but is offering illegal material by way of a contact e-mail address in another country. While the e-mail is regarded as illegal in Ireland (because it advertises child pornography), it may not be so regarded in other countries, because the law in those jurisdictions require an image to be present. Nevertheless, the Hotline can take action as the ISP in question regards sending spam from their servers as a breach of their terms of usage and often they will close the account. Alternatively, if the spammer is exploiting an accidentally "open relay" resulting from a poorly configured mail server, the ISP will often close this, as it has a negative impact on their resources. For examples, see section "[Hotline Report Case Samples](#)".

Unfortunately the Hotline has to report that it continues to have report referral failures in about 25% of cases. Many of these cases involve material that is very probably illegal in the Republic of Ireland and other INHOPE member countries but the Hotline knows it is not regarded as illegal in the source country and there is no point in forwarding it through police channels. The reality is that a proportion is hosted in countries where there is no method of having action taken. Telecommunications to these countries have typically been poor and so they are not often encountered. However, as links improve in such countries, international political pressure will have to be brought to bear to prevent the criminals who supply illegal material, including child pornography, from using these countries as safe havens.

- *Keep one e-mail address for private use to trusted friends and online transactions with reputable companies then use another for chat rooms, bulletin boards, etc.*
- *Never reply to a spam, even to the "unsubscribe reply" address, this just confirms to the spammers that a valid and active e-mail address exists and will result in yet more spam.*
- *Use spam filtering software or services, or set up rules in the e-mail package used to sort e-mail into different folders and automatically delete e-mail received from known spam accounts.*

## ISSUES ARISING

The following paragraphs examine some of the issues which follow from the analysis of the Hotline's core work.

### INCREASING INCIDENCE OF SPAM

"Spam" is the colloquial term used for unsolicited commercial e-mail. It is a large and growing problem on the Internet. Both ISPs and legislators are making serious efforts to eliminate it without infringing privacy of individuals or the right to advertise products. Until such time as these become effective in most countries, spam will be inevitable. At present, Irish ISPs estimate that approximately half of their e-mail resources are utilised in delivering spam over their networks.

As discussed earlier in this report, submissions

to the Hotline resulting from spam have grown from 2 (period Nov. 99 to June 01), to 864 in the period (Jul. 01 to Jun 03). This growth is even more pronounced when it is graphed as the percentage of reports received in each month over the current reporting period (figure 8).

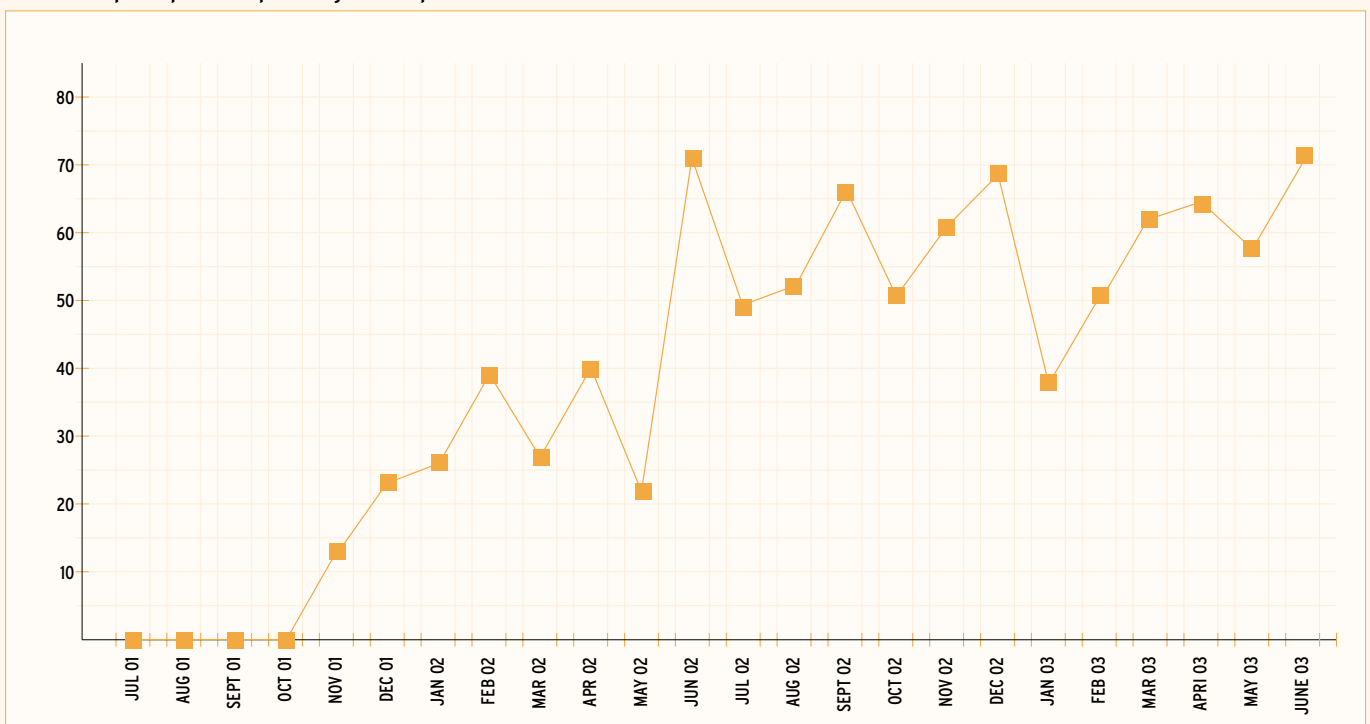
There is no doubt that spam triggers a large number of reports. Often the text is sexually explicit and the spam may shock the recipient into making a report. Generally these spams do not refer to content that is actually illegal. This aspect is discussed further in the next section.

Despite the media attention that Chat has received due to a few high profile cases of children being lured into meetings with paedophiles, the number of reports about chat

incidents is minuscule in comparison to spam. The greatest irritant to the public of UCE (spam) is its nuisance factor. However, the number of complaints received by the Hotline over the two year period complaining about UCEs in general is very small. This shows that by and large, the public is discerning and only report UCEs which they believe refer to illegal content. So it is pertinent to examine what has caused so many UCE related reports.

The primary cause of reports about spam is advertising of adult pornography. Firstly, there is increasing use of spam for this purpose. Secondly, there is a worrying trend where the language used in the spam can be interpreted as referring to paedophilic activities. This shocks people into making a report who, wisely,

**FIGURE 8** Spam reports as a percentage of all reports



do not attempt to click on the links provided, for fear that it may bring them to a site containing illegal content that could download on to their computer.

Another explanation for the increased reports of spam (and Web sites) is that there has been a massive increase in Internet usage. Simply there are more people available to spammers. First time users quite often use the Internet many months before their address finds its way on to a spammers list. From descriptions provided to the Hotline in reports, we have found that new users suddenly receive such spam and have no idea why this has occurred. It shocks them and often causes fear as there is a tendency to believe that they have been specifically targeted for what they believe

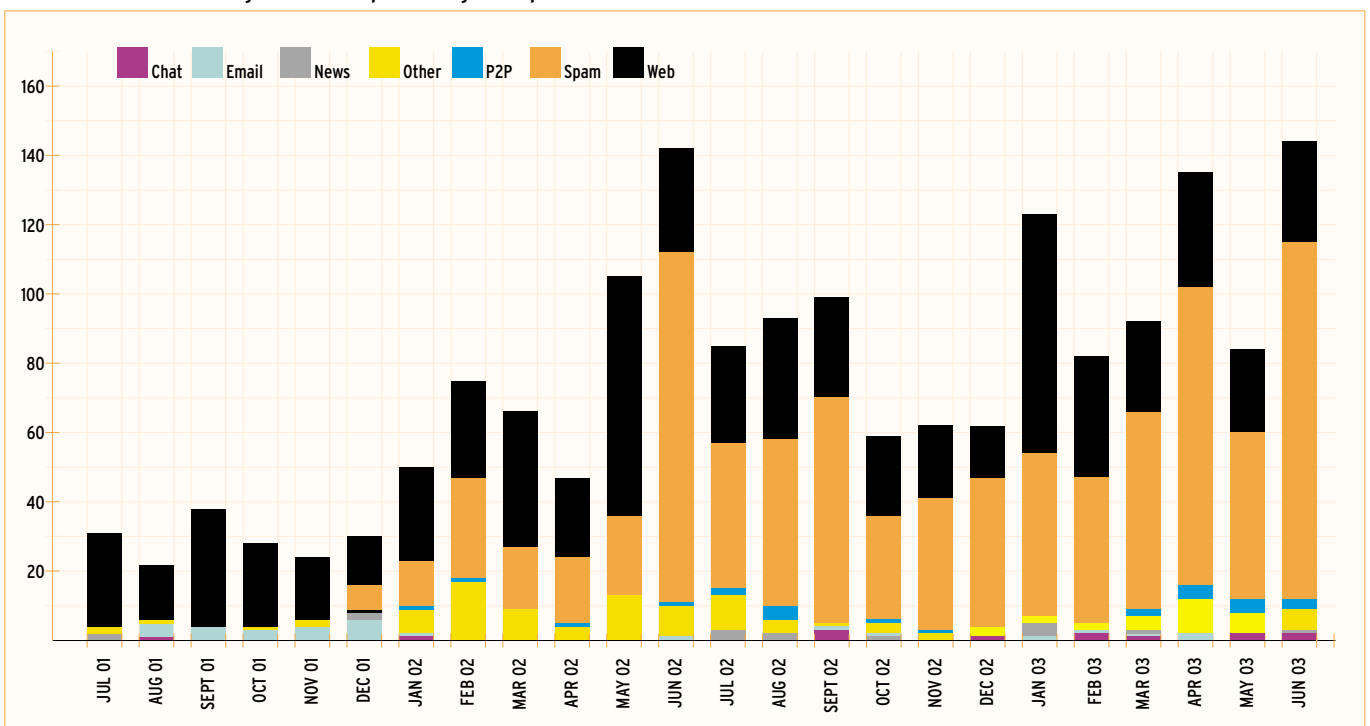
to be an invitation to illegal material. It is worth emphasising here that:

- These spams are not specifically targeted, they are mass-mailed throughout the world, often in batches of tens and even hundreds of thousands.
- They very rarely actually refer to illegal content. Mostly it is advertising adult pornography pay-sites or, to a lesser degree, defamation attacks (see next section).
- A new user's e-mail address will not at first be known to the spammers, so no spam is received.
- After some time the new user's e-mail address finds its way on to a spammer's list. This is due to any of a number of methods:
  - The user has placed their e-mail address

on an open web-site where "crawlers" automatically gather addresses found ("harvesting") and add them to the spammer's list.

- The user has posted comments to an open bulletin board or discussion forum where their address is similarly "harvested".
- There are many viruses which, having infected a persons computer, send the contents of the address book back to spammers. If the computer of some body the user has e-mailed becomes infected, the spammers get the user's address.
- Spammers use random common name generators and apply these to harvested company and ISP e-mail service domain

**FIGURE 9** Bar chart showing incidence of spam as target of reports relative to other services



names. They generate combinations, e.g. jones+a @companyname.com, to give ajones@gmtengines.ie, bjones@gmtengines.ie, cjones@gmtengines.ie. Spam costs very little, so they spam to all and hope for a reply that shows it's a valid address.

- The user has provided their e-mail address to a company but have omitted to tick a box to "opt-out" of product information proposals. Some less reputable companies will sell their client lists. It must be emphasised that reputable, particularly European Union based, companies do not engage in this practice.

Education about keeping ones e-mail address safe and using multiple e-mail addresses is really the only way to overcome this. Simple approaches are recommended by the Hotline:

- Keep one e-mail address for private use to trusted friends and online transactions with reputable companies then use another for chat rooms, bulletin boards, etc.
- Never reply to a spam, even to the "unsubscribe reply" address, this just confirms to the spammers that a valid and active e-mail address exists and will result in yet more spam.
- Use spam filtering software or services, or set up rules in the e-mail package used to sort e-mail into different folders and automatically delete e-mail received from known spam accounts.

### DEFAMATION ATTACK UCES

There is a genre of dubious UCES that appear to advertise a particular web-site by making exaggerated or defamatory claims about the products or services offered by the web-site owners and by providing a hyperlinked URL or contact e-mail address. Despite denying any involvement, the target organisations are often suspected of being behind the UCES and send them to generate traffic to their sites. The exaggerated or mildly defamatory remarks provide "plausible deniability" to the web-site owners! (These are often colloquially termed "Joe Job" spams.)

A very alarming trend emerged in early 2003 when UCES of this type appeared which blatantly advertised illegal drugs, armaments and child pornography for sale. These had the appearance of "Joe Jobs", however, they had such a devastating affect that many of the target sites had to close down. It is very unlikely that organisations would bring this upon themselves. It appears that the perpetrators are people who bare a grudge against an individual or organisation owning the target web-site. The Hotline received 120 reports of these apparent defamatory attack UCES which recipients believed were really providing a sales channel to the illegal material advertised. Unfortunately this practice has been copied and there has been a rapidly increasing incidence of these defamatory attack UCES towards the end of the reporting period.

Defamatory UCES are of concern to the Hotline as these e-mails have been very widely distributed and can find their way into children's e-mail accounts. The text is highly offensive and

there is a trend towards inclusion of greater description of paedophile material supposedly available at the target site. The Hotline is participating in International efforts to close the e-mail accounts that are being used to send the UCES. Where appropriate law enforcement have been involved. Targets of the defamatory attacks have also instigated law enforcement investigations.

These defamatory UCES also generate a considerable workload for the Hotline. It was a single UCE of this type that caused the largest number of duplicate reports in the two year period. During the reporting period, none of the defamatory UCES, which contained references to paedophilic content, were targeted at Irish web-sites. In the Hotline's experience, and from our examination of headers received in reports, none of these UCES were sent from e-mail servers in Ireland.

## INVESTIGATION OF REPORTS

This is an ongoing issue highlighted in the 1st Hotline Report. The situation has been accentuated by the rapid growth in reports. Because of the phenomenal growth of Internet usage, the majority of reports come from people who have never used the Hotline previously.

Understandably, reports received by the [www.hotline.ie](http://www.hotline.ie) service often lack necessary detail. These reports are still investigated. The Hotline staff will take informed action in an attempt to find the material. This is very time consuming and nevertheless, in the majority of cases results in a "not found" or "insufficient detail" being recorded.

Many sites attempt to restrict access using different methods such as password control, hidden links or even password controlled compressed archive files. In addition, many sites carry advertising banners or "pop-up windows" which are time consuming to download and can interfere with the safe operation of hotline's systems. Where files that must be downloaded to view the contents are involved, the download time can be considerable. Viewing of videos in an attempt to ascertain if the suspected sequences contain any illegal content increases investigation times greatly. With higher bandwidths being available to the public the incidence of video and live "webcam" reports is increasing. There is also a heightened risk of viruses being implanted on the Hotline computers with downloaded content.

Due to these developments, investigation of reports received by the Hotline has continued to take significantly more time than anticipated.

The quality of reports and whether the person reporting has used the web forms or not, has a considerable impact on the time taken to process reports. To improve the quality of reporting, the [www.hotline.ie](http://www.hotline.ie) web-site was redesigned and went live in mid-2002. The amount of user safety information and advice was increased. The reporting forms were improved and some explanatory sequences added. The forms, if completed properly, assist the hotline staff by providing a structured report which can be partly processed in an automated manner. As was shown on Table 2, just under 52% of all reports continue to be sent as free form e-mails.

Especially in the case of UCE's, the Hotline recognises that it is easier for the reporter to simply forward the e-mail. Unfortunately, this loses the vital delivery header information and in many cases it is not possible to process the reports to a conclusion. The Hotline therefore requests all reporters to use the web forms and, in the case of UCEs, include the headers by copying and pasting them into the dialog box provided.

The hotline treats all reports received in the utmost confidentiality and reports may be made anonymously. However, the fact of having made a report to the Hotline is not a defence in court if for any reason a Garda investigation results in charges being brought against an individual under the Child Trafficking and Pornography Act 1998.

Responses sent out by the Hotline and all promotional activities continue to request the public to report using the web forms. It had been hoped that the proportion of free-form

reports would have decreased. Regrettably this has not been the case. Some hotlines in other countries will only accept reports sent using web forms. However, every report is valued and the Hotline has decided to continue to accept free-form e-mail reports.

## TRACKING AND MANAGING REPORTS

The Hotline tracks and manages reports using an in-house Microsoft Access database. During the reporting period this was improved with refinements being added to tracking categories, queries and reports. The database contains essential details of Hotline actions taken on reports received since the establishment of the Hotline. This system is isolated from the Hotline web-site which is a considerable advantage in terms of security. This system is complemented by Microsoft Excel spreadsheets which are used to analyse and graph the data. This was the mechanism used to produce the statistics and charts contained in this report.

### ARCHIVING REPORTS AND MATERIAL

It is the policy of the Hotline not to archive content that it finds during investigations. With the exception of files that must be downloaded in order to view them, it is the policy of the Hotline (in line with INHOPE best practice) not to store any material reported to it. Procedures ensure that such material is only downloaded when the Hotline assessment is to be undertaken and when a determination has been recorded, the file is immediately and securely erased. It is also policy that following assessment and determination activities relating to web-sites, cached temporary files created by the browser are securely erased at regular intervals. The Hotline does not maintain a database of child pornography for research purposes.

### PROTOCOL WITH AN GARDA SÍOCHÁNA AND WITH INTERNET SERVICE PROVIDERS

Clearly, if the Hotline is to be successful in combating illegal content it requires the full cooperation of the Internet Service Provider Industry who are uncompromisingly opposed to such misuse of their Internet services. However, having the material removed from the Internet is only the first step. If criminal investigation was not to follow, the perpetrators would simply reappear under another account name or on another server.

The Hotline has developed vitally important working relationship with An Garda Síochána. This is the second link in the process that allows the findings of the Hotline to be passed to An Garda Síochána who may then initiate criminal investigations. Under the auspices of the Internet Advisory Board, the Hotline has worked with An Garda Síochána, the Data

Protection Commissioner and the Internet Service Providers to develop a protocol for controlled exchange of information required in the process of a Garda Síochána investigation of criminal activity.

Under this protocol, the www.hotline service is enabled to issue a "Notice and Take Down" instruction, if and when required, to the specific Internet Service Provider. This process was not brought into action in the reporting period, as no illegal content was reported to the Hotline where the source was within the jurisdiction. However, the good working relationship established has allowed the smooth operation of reporting content where the source was outside the country. The Hotline and An Garda Síochána meet regularly to exchange expertise and knowledge of the evolving technologies being employed on the Internet.

### OFFERS OF ASSISTANCE

The Hotline service continues to receive offers of support and direct assistance from members of the public and some organisations. These offers were evaluated and, where necessary, with assistance from the Internet Advisory Board and in reference to INHOPE best practice recommendations. While the Hotline recognises the good intentions of these offers, the nature of the task and the legal implications involved, dictate that the work should be carried out solely by Hotline employees. Due to growing numbers of reports the Hotline has initiated recruitment of additional staff.

### HOTLINE VISIBILITY AND PROMOTIONAL ACTIVITIES

The Hotline's primary focus is on maintaining a service to accept reports from members of the public on illegal child pornography and other specified illegal content. As testified by the growing numbers of reports and from feedback the Hotline has received from reporters, the response to the service has been very positive. Nevertheless, it is desirable that visibility of Hotline should be improved so all Internet users know where to turn should they encounter suspected illegal content.

During the reporting period, the Hotline undertook a number of visibility-raising events and initiatives.

The presence of the www.hotline logo on the web-sites of ISPAI members is mandatory under the Code of Practice and Ethics to which they have signed up. Hence ISPAI members have ensured that the Hotline service is made known to their customers.

Eircom.net included a profile of the Hotline and safety tips on Internet use in a news leaflet enclosed in every Eircom telephone bill sent to all residential customer. Hotline personnel have regularly been interviewed for TV and radio programmes and newspaper articles.

The Hotline has produced DL sized leaflets that provide Internet safety tips aimed at adults, especially parents and those responsible for children. It describes very briefly and simply what steps can be taken to improve safety and provides the Hotline's contact details. These are provided to members of the public requesting information and have been distributed to libraries and at events at which Hotline staff speak.

The work of the Hotline has also been highlighted in the awareness activities of the IAB. Callers to their advice line are informed of the Hotlines function as required.

The Hotline has co-operated with the National Centre for Technology in Education (NCTE) who prepared a series of publications aimed at teachers and pupils in secondary schools entitled "Be Wise On The Net!". These publications have been distributed to every secondary school in the country and included the Hotline contact details.

### **QUALITY OF REPORTS**

The effectiveness of the Hotline depends on the quality of the external reports on which it relies to initiate its actions. The large numbers of reports containing insufficient detail to initiate a case, or where the content simply cannot be found at the location reported, is worryingly high. The Hotline employees, IAB members and ISPs have attempted to identify the reasons and to address the problem.

Anecdotal evidence from examination of the Hotline reports and calls to ISP desks on support issues has provided some suggestions. The Internet and computer technology is a relatively new to most users. As a result many people do not understand what is going on "under the covers". When they encounter what they suspect is illegal information they simply are often unable to describe where or how this occurred. They may be unaware that some of the solutions are very simple, such as, switching on an option to reveal the current URL. A common problem is that the web address of the search engine (i.e. Google) rather than the URL of the search result is reported. Failure to cite the search engine name and the specific search criteria used renders it largely impossible to pursue the report.

Education (such as ECDL) to raise users' knowledge of what they are doing on their Computer is the best solution. However, as more children and young people receive training on computer usage at school and college, we will see this problem decline. However, for the time being, this continues to be a problem for the Hotline.





*The fact that none of the reports that have been determined as illegal content, referred to material hosted or distributed from Internet facilities in Ireland, must indicate that self-regulation is working in the Irish jurisdiction.*

## CONCLUSIONS

The Hotline is now well established and is a cornerstone in the fight against illegal material on the Internet at home and abroad through membership of the INHOPE network.

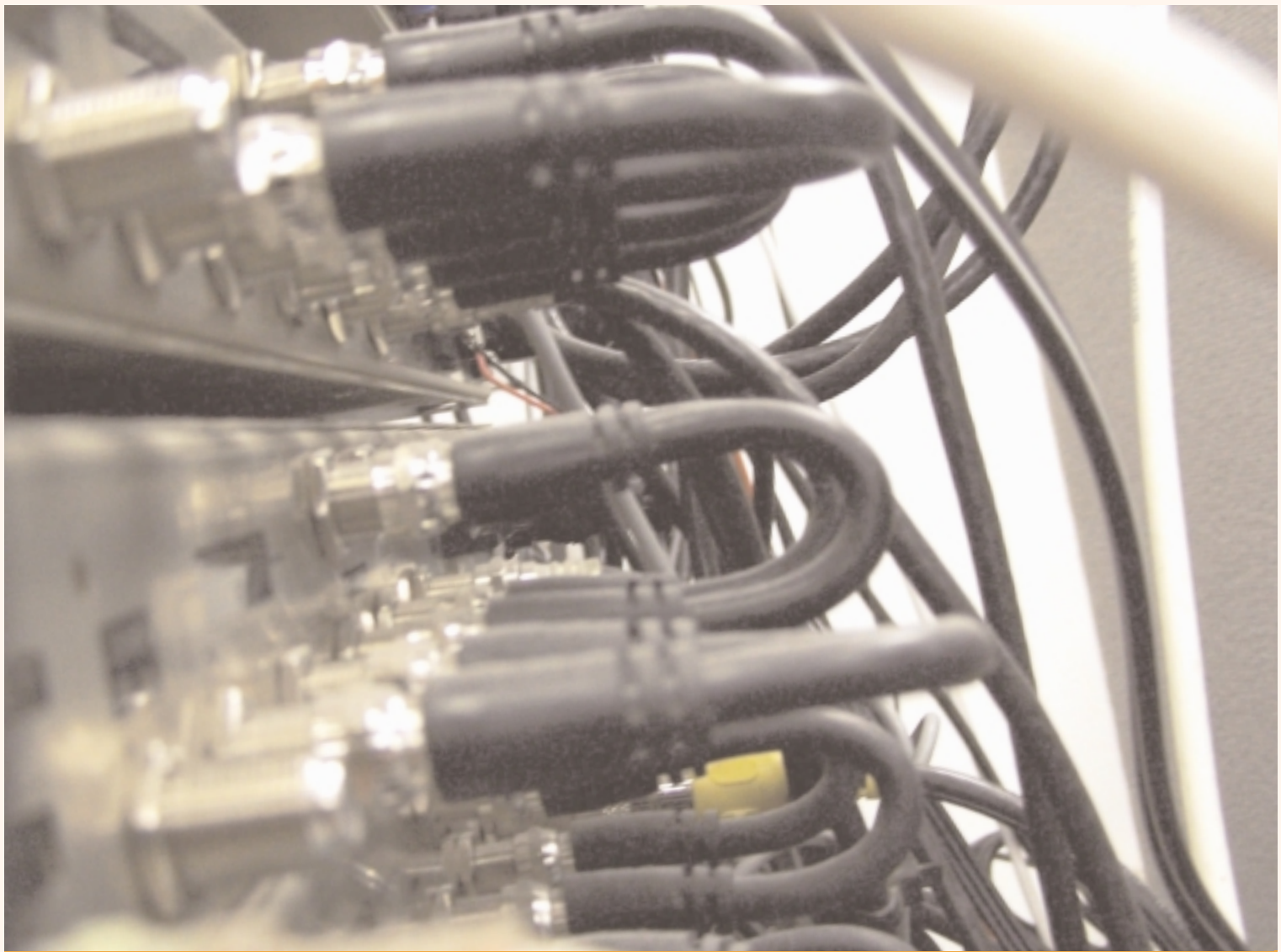
The public is using the Hotline and the number of reports received is growing continually.

The fact that none of the reports that have been determined as illegal content, referred to material hosted or distributed from Internet facilities in Ireland, must indicate that self-regulation is working in the Irish jurisdiction.

The Hotline can not work alone. It is only through the support of the IAB, An Garda Síochána, Government, and the ISP industry that it can provide its contribution to the collective fight against illegal use of the Internet.

Undoubtedly the Hotline faces enormous challenges in the time ahead but based on our knowledge and experience, we are confident that we can meet these challenges and continue in the objective of contributing to make the Internet a safer environment for all users.





*The Hotline traced the home page and found that it was hosted by a member of the ISPAI. However, it was then found that the guest book was on an external link as it used a third party guest book service. This was then traced and it was found that the guest book was hosted in the USA.*

## SAMPLE CASES.

### SAMPLE 1

**REPORT:** A report was received citing a web-site on the private pages of an Italian ISP. A complete URL was provided. It claimed that there was a series of related web pages that was advertising videos for sale. The site included many still shots of the video which the reporter suspected were child pornography.

**HOTLINE ACTIVITY:** The details of the report content were transferred into the database. Hotline staff then attempted to find if the site was active. The site was found. The content was verified as advertising videos which were for sale by credit card purchase. Still images purporting to represent examples of the video content were used on the site. These showed a girl estimated to be about 10 years old in explicit poses and engaging in sexual activity with an adult male. The Hotline verified these as being probably illegal under the Child Trafficking and Pornography Act 1998.

The Hotline traced the site to a private web space supplied by a major ISP in Italy. The IP addresses found by the trace were verified to ensure the server was in fact located within the Italian jurisdiction.

As there is an INHOPE hotline in Italy a standard forwarding report was prepared. This was then sent to Stop-IT (the hotline) in Italy.

Details of the activity were completed in the Hotline database and the case was closed in [www.hotline.ie](http://www.hotline.ie).

It is interesting to note that Stop-IT pursued the matter in conjunction with Italian law enforcement and the site was taken down in Italy. Within a few weeks the identical material was again reported to [www.hotline.ie](http://www.hotline.ie) but it had now

moved to servers which were apparently located in South Korea. A similar process occurred when the Hotline reported it to Internet119, the Korean INHOPE member, which resulted in the site being removed in that jurisdiction. It has come to the attention of other Hotlines in a number of other countries around the world since that time.

### SAMPLE 2

**REPORT:** A www.hotline received an anonymous report that the "guest book" of the web-site of a member of the Irish hospitality industry contained references to child pornography. The site domain name was given and it had a .ie domain registration. The dates on which the entries were made in the Guest Book were also given.

**HOTLINE ACTIVITY:** The Hotline first recorded the details into the database and then confirmed the existence of the web-site. The guest book was not immediately apparent on the home page. The Hotline then examined the six links to pages within the site. One of these pages was found to have a link to a guest book. This link was taken and the reported entries were found in the guest book. These had been placed there by third parties. These entries implied sexual acts with children that could be interpreted as probably illegal content under Irish law. Others provided links that implied that child pornography may exist in other locations. The links proved to be broken and the target sites could not be found.

The Hotline traced the home page and found that it was hosted by a member of the ISPAI. However, it was then found that the guest book was on an external link as it used a third party guest book service. This was then traced and it was found that the guest book was hosted in the USA. Due to the terminology used the Hotline knew there was little possibility that the reported guest book entries would be regarded as illegal in the USA.

It was obvious to the Hotline that these guest book entries had probably been placed there by persons unrelated to the Irish establishment. The Hotline contacted the

establishment in question and explained the situation. They were quite shocked that the site had been misused in this way and highly embarrassed that visitors may have seen this. Due to changes in personnel, administrative passwords to the guest book service were lost. The Hotline provided advice that they should have their web design company remove the link and so make the guest book inaccessible and if required establish a new guest book. It was also explained that open forums like guest books are regularly misused in this way. The report was then closed. (The establishment implemented the advice given and the site no longer has access to the offending USA based guest book service).

### **SAMPLE 3.**

**REPORT:** The hotline received a report that a spam e-mail advertising child pornographic images was received at the information desk of a Dublin based company. The staff had been quite disturbed on receiving it and the manager made a report to the Hotline. They provided the textual content of the spam and the delivery headers.

**HOTLINE ACTIVITY:** The hotline logged the details into the database and initiated its investigations. The URL contained within the spam led to a web-site that contained images as described in the spam and was offering membership of the site by way of a credit card payment. The site had a preview section allegedly providing sample images of what was in the password protected members area. The Hotline determined that the images of young girls estimated at around 11 to 13 years of age were posing in a manner that they were probably illegal under Irish law.

A derived report was created as it was the spam not the web-site that was originally reported.

The web-site was traced and appeared to be hosted in Russia. A standard forwarding report was completed and sent to An Garda Síochána for forwarding through police channels. Details of the activity were recorded in the Hotline database and the derived report was closed as "Report to Gardaí".

The Hotline then attempted to trace the source of the spam using the headers. The spam headers were faked and it was not possible to determine with any accuracy where the spam had

originated. The details of the activity were recorded in the database and the case was closed as a "Trace Attempt".

**SAMPLE 4:**

**REPORT:** A spam e-mail was reported to the Hotline which had been received on a standard private e-mail account offered by one of the major Irish ISPs. The reporter provided the plain text of the spam and the headers.

**HOTLINE ACTIVITY:** After logging the details of the report, the spam text was examined. It was advertising video tapes of child pornography for sale. There were no images or URLs embedded in the spam. The text describing the content of the various videos was explicit enough to be probably illegal in its own right under Irish law. The only method of response provided in the spam was to contact an e-mail address which had a .RU domain. This was the public e-mail service of a large ISP in Russia (which offers free e-mail accounts similar to those provided by ISPs in all countries).

The Hotline then examined the headers. Much of these were forged but it was possible to determine that it did not appear to have been sent from the Russian ISPs servers. Examination of the various headers confirmed the first genuine header IP and this showed that the spammer had injected the e-mail through an e-mail server that was provided by a major ISP in Sweden.

There is an INHOPE member hotline in Sweden run by Radda Barnen (Save the Children-Sweden) and the Hotline forwarded details. The Swedish hotline verified that the e-mail appeared to have been distributed from an e-mail server of a broadband customer of the ISP. The Hotline closed the case as "Forwarded to SE - Radda Barnen".

Subsequently the Radda Barnen Hotline fed back that the ISP found the customer's server was poorly configured and this had allowed it to be exploited by the spammers. The ISP instructed the customer on how to rectify the configuration. The "hole" through which the spammers were advertising the illegal material was therefore successfully closed down.

## APPENDICES

### APPENDIX 1 - WWW.HOTLINE SERVICE: TERMS OF REFERENCE

Terms of Reference of the www.hotline service (as agreed by the Committee on the Illegal and Harmful use of the Internet).

- The investigation of complaints from Internet users about illegal material on the Internet.
- The taking of appropriate measures to address identified illegal material hosted, posted or provided within the Irish jurisdiction on the Internet, in collaboration with all the relevant national players, including An Garda Síochána.
- illegal material is identified but is outside the jurisdiction, to follow agreed local blocking procedures where feasible, and to liaise with the appropriate national jurisdiction.
- In relation to harmful material on the Internet, to encourage, promote and assist in the development of rating systems for Irish sites in the context of emerging international developments in this area.
- To disseminate information about the hotline service to the Internet user community and to develop user friendly and effective methods for notifying complaints.
- To actively co-operate with similar complaint bodies outside the jurisdiction in the area of exchanging information and experience in all matters relating to its functions.
- To document and implement transparent standards and procedures for its complete range of functions.
- To publicly report on its activities at regular intervals.

To report to a new Advisory Board on the Internet (see Section 5.4) on all matters which require advice, discussions or decision by the Board, including new Internet developments which the Director feels should be brought to the Board's attention.

### APPENDIX 2 - ISPAI MEMBERSHIP

The members of the Internet Service Provider Association of Ireland (ISPAI) were the following as of June 2003:

MEMBER NAME	WEB ADDRESS	BUSINESSES INCLUDED
EircomNet	www.eircom.net	Indigo Services
EsatBT	www.esat.net	IOL and Oceanfree
HEAnet	www.heanet.ie	
Irish Domains	www.irishdomains.com	
Novara IT	www.novara.ie	
O2	www.o2.ie	
UTV Internet	www.u.tv	
Vodafone	www.vodafone.ie	

### APPENDIX 3 - INHOPE ASSOCIATION MEMBERS

The members of the INHOPE Association as of June 2003

COUNTRY NAME	MEMBERSHIP STATUS	ORGANIZATION	WEB ADDRESS	MEMBERSHIP DATE
Australia	Associate	ABA	www.aba.gov.au	Nov-99
Austria	Full	Stopleveline	www.stopleveline.at	Nov-99
Belgium	Full	Child Focus	www.childfocus.org	Sep-01
Denmark	Full	Red Barnet	www.redbarnet.dk	Mar-01
Finland	Provisional	Save the Children FI	www.pela.fi	Sep-02
France	Full	AFA	www.pointdecontact.org	Nov-99
Germany	Full	ElectronicCommerce Forum	www.eco.de	Nov-99
Germany	Full	FSM	www.fsm.de	Nov-99
Germany	Full	Jugendschutz	www.jugendschutz.de	Nov-99
Greece	Applicant			
Iceland	Full	Barnaheill	www.barnaheill.is	Sep-01
Ireland	Full	ISPAI	www.hotline.ie	Nov-99
Italy	Provisional	Save the Children IT	www.stop-it.org	Jan-03
Korea	Associate	Internet	www.internet119.or.kr	May-03
Netherlands	Full	Meldpunt	www.meldpunt.org	Nov-99
Spain	Full	Protegeles	www.protegeles.es	Mar-01
Sweden	Full	Rädda Barnen	www.rb.se/hotline	Nov-00
United Kingdom	Full	Internet Watch Foundation	www.iwf.org.uk	Nov-99
U.S.A	Associate	Cybertipline (NCMEC)	www.ncmec.org	Nov-99



#### APPENDIX 4 - EXPLANATION OF CATEGORIES FOR CLASSIFICATION OF CONTENT

The following is an explanation of the categories used by the Hotline in classifying reported content. It is emphasised that these are not legal definitions and are provided purely to give the reader an indication of the type of material that is being discussed in the analysis.

CATEGORY	DESCRIPTION
Child Pornography	Content that is assessed as falling under the terms of the 1998 Act and therefore would probably be found illegal if presented in a case before the Irish Courts.
CP Jump Site	Site which provides links or automated links (redirects) to a site that contains child pornography as described above. The site itself does not contain illegal images or descriptions but would probably be interpreted as advertising child pornography and therefore illegal under the 1998 Act.
Child Abuse	Sites providing assistance for persons to go to places where they can avail themselves of child prostitution and may otherwise abuse children. (Sex tourism).
Child Trafficking	Sites involved in the arranging the movement of children for illegal purposes.
Child Erotica	Content, particularly images but could be drawings or stories, which do not depict children in ways which are explicitly illegal under the 1998 act, but are nevertheless intended to be arousing to those with a sexual interest in children. This would be judged on the basis of the poses and settings, inappropriate clothing and make-up used. It must be emphasised that possession of such images in themselves would not be an offence. However, police investigations have shown that in the majority of cases, large collections of such images are found along with the child pornography on the paedophile's computer storage devices. Because such images may be viewed as being created to pander to paedophilic needs, it is categorised in the "child related illegal" group.
Financial scam	Usually spam e-mails and related web sites that are "confidence tricks" intended to defraud Internet users. (The Hotline does not accept complaints about goods or services not received following Internet based transactions. These are outside the Hotline remit.)
Racist material	Content which incites racism and hatred contrary to EU directives and Irish law.
Illegal material	Content which incites acts of violence or rape, is criminally defamatory, assists in trafficking of proscribed drugs and illegal immigrants, soliciting for prostitution, organisation of terrorism and other illegal activities.
Adult pornography	All forms of pornographic material which are not illegal under the 1998 act. That is, do not involve minors under the age of 17 years.
Extreme adult pornography	Content which is pornographic in nature that involves acts that if brought as an action in Ireland may be found to contravene obscenity laws. E.g. adults engaged in bestiality, fantasy rape, purported incest (between adults) and extreme sado-masochist sites. Unfortunately, the law is unclear in such matters and the Hotline would like to have clearer markers set down in law. At present if such material was found to be hosted in Ireland, we would report it to the member ISP who would take it down as a breach of its acceptable use terms.
Adult jump site	Index and similar sites that do not contain pornographic material themselves but provide links to such material. Often these contain descriptions and site names which cause people to report them.
Virus attack	Reports about viruses being received usually as spam.
Spam e-mail	Complaints about volume of spam being received but not reporting any potential illegality of the content.
Hacking site	Instruction on how to bypass security and illegally gain access to other peoples' machines. How to construct viruses, lists of stolen usernames and passwords, etc.
IPR alleged violation	Complaint that site is using or providing copyrighted material without permission of the owners of the intellectual property rights (IPR). Taking action on such complaints is outside the Hotline remit.
Nudism	Sites containing images of naked people that are not illegal. For example, these include naturist sites, or children in Africa who have photographed naked (because they have no clothes) but there is no sexual motivation to the images. These are reported very occasionally and usually out of context.
Insufficient detail	There are a surprising number of reports made, where simply not enough information is given to either understand or classify the complaint or even find the information to which the reporter is referring.
Complaint	Complaint about Internet service. Advice is given to contact the ISP customer or technical support unit. (Action is outside Hotline remit).
Other	Miscellaneous questions, etc., where action would be outside hotline remit.
Query	Questions from public and media on any aspect that is within the Hotline remit.
Outside Hotline Remit	Primarily allegations against individuals or other legal entities which should be made directly to An Garda Síochána. The Hotline only deals with reports about content on the Internet not the activities of people or organisations.

## APPENDIX 5 - EU INTERNET ACTION PROGRAMME

### AGREED OBJECTIVES OF THE WWW.HOTLINE.IE CONTRACT

To establish a hotline service in Ireland with extensive collaboration with a European Network of Hotlines. The Hotline will allow Internet Users and Internet Service Providers to report illegal content or use which they become aware of via their use of the Internet. The hotline will initially focus on illegal material involving children/minors and which is explicitly dealt with under the Irish Child Pornography Act 1998.

#### TASKS

##### Management

- Oversee the successful establishment of the hotline, and ensure accountability to funders and the public

##### Operations

- Receive reports of illegal or harmful material on the internet (esp relating to children)
- Track reports
- Investigate reports
- Respond to reports
- Gather Statistics to track performance and efficiency and for scientific research
- Liaise with Law enforcement agencies
- Liaise with Law enforcement agencies in relation to reports
- Contribute expertise to government departments, etc \ in relation to hotline activities
- Attend seminars, conferences to develop industry best practices

#### AWARENESS

- Establish web site for hotline and promote this through ISPs and by all other means
- Promote internet safety, where possible in conjunction with others
- Contribution to Network
- Sharing information with other hotlines,
- Sharing expertise about responding to illegal content
- Helping with training of new hotlines participating in INHOPE Association meetings and working groups

#### EXPECTED RESULTS

- Public Internet Hotline to accept reports on illegal child pornography in Ireland will be established
- Volume and results of reports to hotline will be regularly published
- Public awareness will be promoted via seminars and PR process
- 6 month report

## APPENDIX 6 - RATIFIED AIMS OF THE INTERNET SERVICE PROVIDER ASSOCIATION OF IRELAND

### THE OVERALL AIM OF THE ISPAI IS:

"To promote the interests of Internet Service Providers in Ireland."

#### PRINCIPAL OBJECTIVES

- The principal aims of the Association are:
- To promote accurate and un-biased media coverage of the Internet, Service Providers and Users.
- To provide a focal point for discussion with political groups and others likely to impact the industry.
- To establish a Code of Practice for service providers.
- To establish accepted standards of service and a uniform code of practice acceptable to members.
- To sponsor research into trends likely to affect Internet Service Providers.
- To communicate to members, issues and developments relevant to the industry, and to foster communications between members.
- To foster the industry's image.
- To encourage an open and competitive environment, and to resist anti-competitive policies and practices.
- To address any technical issues of specific relevance to the Irish Internet Community.
- To foster co-operation with related organisations world-wide.

Further information is available on [www.ispai.ie](http://www.ispai.ie)  
Further information on the Hotline is available on [www.hotline.ie](http://www.hotline.ie)

## APPENDIX 7 - REFERENCES

- a. "First Report of the Working Group on the Illegal and Harmful Use of the Internet", Government Stationery Office, 1998. <http://www.justice.ie>
- b. "Internet Advisory Board, Ireland, Report 2000 - 2002", Internet Advisory Board, 2003 <http://www.iab.ie>.
- c. "First Report of INHOPE, Association of Internet Hotline Providers in Europe", INHOPE, 2002
- d. "First Report [www.hotline.ie](http://www.hotline.ie) November 1999 - June 2001, Internet Service Providers' Association of Ireland, 2001. <http://www.hotline.ie>



[www.hotline.ie](http://www.hotline.ie)  
26 Upper Baggot Street  
Dublin 4



**Telephone:**  
1890 610 710  
**Facsimile:**  
1890 520 720  
**e-mail:**  
[report@hotline.ie](mailto:report@hotline.ie)  
**Web:**  
[www.hotline.ie](http://www.hotline.ie)