

# Three Hazards Child Protection in the Electronic Age

A study carried out by Pat McKenna, Childwatch.ie,  
for Barnardos

2009



  
Barnardos



## OVERVIEW

This study was commissioned by Barnardos, and undertaken between April and September of 2008 by 2SAPlus Limited on their behalf.

The research focuses on three primary hazard areas for children:

- **Children's Personal Privacy:** the policy and means through which children are individually identified, and can maintain selective data privacy.
- **Children's Data Protection:** the security and administration of stored data about children, and the policy and physical means through which that data is accessed, and transported physically or through electronic networks.
- **Child Sex Abuse Imagery (CSAI):** restricting access to the means through which such unlawful media is available to consumers.

Contributions were sought and obtained for the study from a wide range of people (76 in all) in positions of governance and management in the information technology domain of organisations operating in child related sectors, including: Healthcare Agencies, Education, Government Departments, Telecommunications Companies, Child Service Organisations, IT Security Companies and Software Manufacturers etc.



## BACKGROUND

People appreciate the need to protect children in the physical world. There is an even greater requirement – but perhaps less well appreciated - to correctly estimate the needs of protecting children in the world of computerisation.

Data about children is created and processed from the time of birth. The creation of such data is usually not voluntary, and often no notification is given to parents or guardians as to the extent of that capture, its purpose, use and possible future distribution.

What organisations store that data? Who has front and back office (including maintenance), access to it? Is it securely stored? Is it securely transported over networks or physical media? What is it used for? Who decides on the required level of security and accountability for the correct administration and safety of this data?

As children grow, their access to computers and the internet grows with them. And in the process, children enter a world of opportunity and risk. A person of any age can join an internet social site and create a profile that is real, or a complete fabrication. A child online has no guarantee that a person with whom they are communicating is nine or fifty nine, is male or female.

In some circles a child over the age of fourteen is deemed to be of sufficient intelligence to correctly make judgment as to the nature of the data they may release about themselves on social sites. What is the status of such disclosure where the child is actually five years of age? What if they are eight years of age and purporting to be fourteen? Equally, what is the status of this disclosure where the child in question has diminished responsibility through illness or otherwise?

There is a great deal of debate about what is and is not child pornography, and what may or may not be legal. However there is absolutely no issue that movies and images displaying children being sexually abused are illegal. Such imagery corrupts the people, both adults and children, who view it. It should not be forgotten that for this imagery to be produced at all, a child somewhere in the world has been brutalized sexually, through terror, or torture. The recording of this act is the production of a physical crime scene. The people who produce it are criminals. The people who watch it are criminals.

So if it is illegal to display such material on a computer screen, or store it on media, does it not follow that it might be illegal to knowingly facilitate the means to access and transport such material to the computer in the first place?

The three elements of Data Privacy, Personal Protection, and access to CSAI are important because they are interrelated.

A person seeking and viewing CSAI or CEM (Child Exploitation Material), is feeding an unhealthy and unlawful interest in children. If that person should gain access to a child's legally stored data (e.g. PPS Number, full name, DOB, Address etc), and can query internet social sites to match up a profile (photos, friends, habits, likes and dislikes etc), then a clearly defined risk to the well being of that child is obvious. Such data harvesting will equally pose risks to the child in adulthood also.

This study is designed to get the individual views to key questions of IT professionals to establish their thinking on addressing such issues that affect the security of children in computerisation today.



## CHILDREN'S PRIVACY ON THE INTERNET

Social networking is a new and fantastic phenomenon. It enables and promotes all sort of relationships that weren't possible before. It encourages the making of new friendships and the restoration of old ones, and enables people to keep track of their friends in "real time".

However some key questions regarding the privacy of children and the data and imagery that they volunteer must be realistically addressed. Laws exist relating to the use of data on computer systems located in Ireland, but where this data is located on an internet site such as a social network (Bebo or MySpace are popular examples), the rules of data protection do not appear to apply in the same manner.

### Pseudo Profiling and Age Verification

This is the single greatest issue that arises when addressing personal privacy issues on Social Network (SN) sites.

In the United States, the law dictates that a teenager above the age of thirteen may join a social networking site and share their personal data and images. In Ireland the age of understanding is assumed to be fourteen. However, this age is nowhere written in law, so it tends to operate as no more than a guideline.

A SN is open for business and anyone can join. A fifty year old can pose as a teenager and set up a comprehensive profile to support that claim, and a nine year old child can equally pose as a teenager also.


Children will also tell you that they have facilities within the SN software to fine-tune the levels of access that are allowed to their profiles. For instance a person may need to login to view some profiles, and some children restrict access to their information to only their closest friends. This is very responsible networking and SNs are to be congratulated for providing such controls.

The key difficulties for SNs:

- Anyone can pose as anyone else. For instance there is little to prevent anyone from creating a profile complete with photos and pose as a fourteen year old boy.
- A profile can be created to purport to being someone else: anyone can create a profile claiming anything and insert another person's photo thus claiming that person's identity.
- Although the SN is governed by US law to only allow children above the age of thirteen to have access, in reality they have absolutely no way of knowing that this is the case, so in practice this law is meaningless.
- A SN cannot determine if a person (or in the case of this study: a child) joining suffers diminished responsibility through illness.

With regard to the age and identity issues above, the Data Protection Commissioner in Ireland outlines that they are not aware of the existence of any requirements/guidance on how age is predetermined by social networking sites.

This is a key statement. Let us illustrate the dangers here using Bebo as the SN example. Bebo is statistically the largest SN used by children in Ireland. In the course of this study, research demonstrated that it is extremely easy to find children on Bebo – where they live, their ages, their likes and dislikes, the school they attend, etc. Without even meaning to, children frequently give overt clues to all these things.



And it is very easy too to find examples of children, often very young, behaving in ways that would not be out of place on adult sites, presumably in the belief that they are safe and secure. (Examples of all these things can be supplied separately.)

Data of this kind, and behaviour on site that is inappropriate to the age of the child, makes children very vulnerable. Predators frequently create profiles that are not truly real, and lace those profiles with features designed to attract and manipulate the personalities of vulnerable young people.

The absence of any age limit is a crucial issue. Again, in the course of this study, we came across one Bebo home page of an Irish child of five. He says in his profile that he is five and it appears from his photo that he is five, and he is on Bebo? At least someone had the sense to switch off his brother's profile from public scrutiny.

Is there anything in Irish law that addresses any of the obvious child data and personal protection issues that arise?

### **Harvesting Personal Data**

Another key difficulty that arises in the context of SNs is data harvesting. Data harvesting is defined as the ability for individuals and companies to trawl the internet for data in a manner not unlike that of search engines, and then organise that data into highly structured frameworks that facilitate advanced searching in the future.

For instance, a job seeker being interviewed for a job might find that the employer has had access to information from their profile home page, and comments exchanged between friends, and other material such as photographs of holidays, nights out etc.

Clearly the potential for researchers to get access to internet based data from organisations that scan the internet and other information mediums is considerable.

Using a piece of software like Paros, for example, it is possible to "spider" a Bebo home page. A spider program will gather all the links available and in turn index all the links on each discovered page thereafter. Using this method in conjunction with a parser it is possible to cross link discovered keywords and nicknames to build a comprehensive profile of an individual and store that data for later retrieval.


Using other utility programs it is possible to download the content of pages to a user's personal computer.

The lesson here is that anyone with the knowledge to download particular programs from the net has the ability to complete their own data mining. In the hands of a predator with technical skills this is worrying.

### **Contributor Responses**

#### Ability of a person to assume or alter their true identity on a computer:

Of our 76 contributors from IT Management and Corporate Governance who were asked if there was a need to engage a method of credentialing that clearly establishes the real identity of a user to combat pseudo-profiling, all 76 agreed without exception that there was no need for any user in commercial or social internet software to create and use an identity



other than their own, and that there should be legislation to introduce a system of credentialing that ensures that a person using a computer system is who they say they are.

This is not strictly just a judgement of Bebo or any other SN. Contributors universally agree that pseudo profiling practices should not be allowed in any circumstances where personal data is available.

One contributor managing a site to which children connect (an educational facility), was very clear: “It should be illegal for an adult to impersonate a child”.

What logical reason would there be for an adult to impersonate a child and conceal the fact that they were doing it? This is a very singular context that cannot be confused with other matters such as an adult acting the part of a child for a play or TV programme. This is about adults creating identities (particularly as children, or the peers of children e.g. a school principal), other than their own and connecting to children on the internet with that identity.

### **Addressing Arguments for Change**

There is at the moment no basis for the Data Protection Commissioner, or anyone else, to take action against the issues that arise here – which could include taking action against specific SN sites – because there is no requirement or guidance on how age is predetermined by social networking sites.

So barring informal acceptance that a child of fourteen is of the age of understanding to make judgement regarding the personal information that they display online, there is actually nothing in law to stop a five year old, or an eight year old child with diminished responsibility sharing images of themselves through a webcam to the members of a SN or chat room.


In fairness to SNs, how are they supposed to police this to any degree if the state in which the children are resident does not provide a method of credentialing. This is a key issue. Also Bebo itself, for instance, provides its users with many tools to restrict access to their homepages, and many children use these tools.

However, the key issue is the age at which it becomes appropriate to allow personal data sharing, and the ability of people both very young and old to become members of these sites, and to create false profiles for themselves.

According to the Office for Internet Security and others, one answer for many issues related to children on the internet is parental responsibility. A child should not be allowed to access the internet except under strict parental supervision. Where such supervision is not available then the computer should either be located in the middle of the house directly within view of parents or other adults, or the child should not be allowed to access the internet at all.

This is of course good advice. Anyone who has studied what children actually do on the internet can quickly establish that their behaviour is not monitored by anyone, with the exception sometimes of people who wish to make them vulnerable.

Important as it is, the concept that parental responsibility will solve this problem is flawed for many reasons, most of them obvious. Young people are frequently far more computer literate than their parents are. The logistics of sitting on a child’s shoulder for hours at a time will often not be realistic. Many teenagers will not tolerate parental “interference” as they would see it, and can in any event find ways around parental restrictions.



Of course a wide range of internet security options exists. Is it realistic to expect that the vast majority of parents will be able to access/use them?

On the other hand one would think that parents would make a huge effort to protect their children online. Some statistics suggest that up to one child in four does receive inappropriate advances but 95% in that category never report the incident. If those advances lead to damage to the child, many parents will be haunted by guilt – and by the thought that if the advances had been “nipped in the bud” the damage could have been prevented.

But what happens if a child is approached online and neither the parent, child nor anyone else for that matter ever realizes it; possibly watched while playing, or going to school, or the local shop, or swimming and showering at the local community swimming pool, by someone who on the internet poses as another young school child of a similar age, and chats to the child regularly?

Against that background, we strongly recommend that consideration be given to the development of a commercially viable Age Verification and Identity Management (AV/IDM) program for children. There are moves in the US to examine the viability of such solutions between law makers, SNs and commercial vendors. Ultimately, the development of such a system is the only way to guarantee that everyone on a SN site is who they say they are, and therefore the only ultimate protection for children.



## CHILDREN'S DATA PROTECTION

The Data Protection Act does not specify any difference in risk terms between information belonging to adults and children. It does specify the need for appropriate security of data being held by an organisation, and the requirement to take the appropriate steps necessary to ensure that people with access to that data are entitled to view it.

In a case where private data including Name, Date of Birth, PPS Number, Address could be matched with a person's Bebo profile, the photos posted, and the comments made by friends and family, this would result in a comprehensive identity profile being available to persons or organisations unknown. This is sometimes referred to as 'Connecting the Dots' in the hacking world.

Section 2 of the Data Protection Act requires that a data controller complies with a number of provisions:

- Restricting unauthorised access to data
- Restricting unauthorised alteration of data
- Restricting unauthorised disclosure of data
- Secure transmission and transport of data over network or other means
- Protect against all other forms of unlawful processing

This section derives from recital 46 of the Data Protection Directive which states that: 'Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorised processing'.

There is no specific technical security requirement set out in the Directive given that these are subject to frequent change, and so it is frequently a judgement call for the data controller to make in relation to the type of personal data which they process.

The Data Protection Act has no industry standard or guidelines included in the legislation but the Commissioner has cited IS 17799 information security standard (which is the focus of the data protection requirements) on their website.

However, crucially there is no notification requirement on behalf of a data controller under the Data Protection Act to prove that their systems are compliant with the "safe and secure" provisions of the Act. That said, data controllers constantly submit requests for advice from the Commissioner.

The Commissioner investigates the security standards of organisations where complaints about alleged breaches of the Act are brought to their attention. When this occurs the Commissioner has a strong power of audit when they enter an organisation and examine their technical and physical security arrangements.

Another area of security that is covered by the Act is people's access to data. The following case study covers the points in question.

## **A Case Study reproduced from the DPC Web Site**

The following text is taken from the Data Protection Commissioner's own web site. It illustrates well some of the issues addressed in this report.

*A large organisation, whose staff are employed at several locations throughout the country, used a central database to record information relating to its employees and their work. The complainant questioned the security arrangements in respect of his personal data, and the extent of access to such data throughout the organisation.*

*The organisation's computer system comprised about a hundred personal computers nationwide connected to a central computer in the Dublin head office. Some sixty laptop computers were also provided for use by employees when away from their offices. These laptops contained a version of the organisation's main database which was downloaded from the main computer and updated periodically. Accordingly, data kept by the organisation on its main database was available to staff in the head office, in the local offices, and at off-site locations.*

*The complainant, an employee, made his complaint while the computer system was still being developed and implemented by the organisation. He made the following points: first; he alleged there had been a breach of security because the laptops were without any password protection for a period during the development of the system. Second; the complainant objected to certain of his personnel data and details of his work activity being generally available to staff, and argued that such data should only be available to those who needed them to perform their managerial functions.*

*Section 2: (1)(d) of the Data Protection Act states that "appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction." The question of the security of access to the laptop computers was considered in the light of this provision.*

*My investigation established that each laptop required use of a password for access to the local version of the database. Where a laptop was establishing a connection to the main computer, another password was needed, and access to the main database itself required the use of a third password. In principle this approach appeared to conform well with the requirements of section 2 : (1)(d) above. However, the apparent effectiveness of this approach had been compromised. In the interests of simplicity of operation the organisation issued a unique centrally-generated password to each member of staff (so that each staff member would only need to remember one password) thus reducing the effectiveness of the password system as a whole. Furthermore, in the course of training staff on an upgraded version of the software, the password security system was modified to allow trainees ease of access to the system. This modification gave open access to the main database from a number of laptops.*

*As soon as this fact was discovered, the data controller took steps to rectify the matter. It is not appropriate for a data controller to allow his standards of security to slip, so that personal data becomes more widely accessible than is necessary. However, I noted the prompt action taken by the data controller to put matters right, and - given that my investigation did not discover any evidence of unauthorised access or use of the data during the period when the passwords were not in operation - I did not uphold this part of the complaint.*

The second ground for complaint put forward was the alleged wide availability throughout the organisation of details relating to the complainant's work activities including particulars of annual and sick leave. This raised two separate but related issues: first, whether this wide availability constituted "disclosure" for the purposes of the Data Protection Act; and second, whether the wide availability of data was consistent with the organisation's duty to take "appropriate security measures ... against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction."


On the first question, I noted that the only people with access to the main database were the staff of the data controller. The definition of "disclosure" given in section 1 :( 1) of the Act, specifically states that disclosure "does not include a disclosure made ... to an employee ... for the purpose of enabling the employee ... to carry out his duties". In my opinion, these words require a data controller to make an assessment, in respect of particular employees, as to whether such employees need to have access to particular holdings of personal data, and to provide accordingly. Thus, one would expect a Human Resources Manager to have access to personal data not necessarily available to the manager of a client database, and vice versa. Data controllers should, in my view, take reasonable steps to prevent personal data from being made available to employees who may have no work-related interest in the data.

On the second question, I consider that sensible restriction of the availability of personal data is one of the "appropriate security measures" that data controllers must consider. The more people who have access to personal data, the greater is the risk of unauthorised access or disclosure. These issues were discussed with the data controller in detail. The organisation explained that the wide availability of personnel information and staff operational details was due in part to business requirements, and in part to the culture and tradition of the organisation. Following discussions, the data controller made a number of significant changes to the computer system, at some expense, in order to restrict access to the personal data of employees. It is my view that, in a case such as this, an appropriate balance must be struck between the concerns of the employee as data subject, the real operational requirements of the organisation and the costs to the organisation. I took the view that, following the changes referred to above, the data controller was compliant with the Act.

### **Contributor Responses**

The questions presented here focus on the 'business end' of why things generally go wrong with people's data, and questions asked are specifically in context of a child's data. It should be noted that there has been a number of high profile incidents in Ireland and the UK where data belonging to adults and children has been compromised, and in some cases years lapsed before correct reporting of the issues involved. The degree to which this publicity might influence the opinions of contributors is tempered by the fact that the contributors themselves are knowledgeable and responsible for IT matters within their organisations.

Data is most often stored in databases in clear form (with no obfuscation). There are many computer languages and technological means through which a database, and the server(s) upon which it runs can be accessed. Where data belonging to a child is stored, how should that storage be protected?



Storage of data belonging to children:

- Of our 76 contributors from IT Management and Corporate Governance who were asked how data should be stored, nine responded that it should be in clear text form, 60 that it should be stored in obfuscated (encrypted) text form, and eight were unsure. Of the above 67 indicated that any requirement should be clearly defined in legislation.
- Contributors from smaller organisations have little idea of how they could accomplish a legal compliance and would fear the impact on their business if they had to comply.
- Contributors addressing the concerns of the smaller organisations suggest that common entities such as schools and crèches should be provided with a secure commercial 'out of the box' package that can be installed and following setup is compliant with any legislation.

Data belonging to children in transport: Of our 76 contributors from IT Management and Corporate Governance who were asked about the security of data in transport, through networks or on physical media, all 76 responded that in no case should data belonging to anyone, children or otherwise, be transported in clear unencrypted form. All 76 agree that this should be legislated for and tightly controlled.

Some contributors have raised questions regarding the manner that data is shared through email as that medium is unsafe and insecure from access by persons other than those who should have access to personal data. Email content and attachments that are not encrypted can be accessed by persons other than the sender and intended recipient within the email transport mechanism.


Perpetually encrypting data belonging to children: Of our 76 contributors from IT Management and Corporate Governance who were asked if where data belonging to children is processed, should this data be perpetually encrypted at the time that it arrives in a system, and then perpetually for the lifetime of its use?

70 contributors agree that it should be kept in perpetual obfuscation for its lifetime in use and indicated that legislation should be in place to ensure that this is the case; 2 felt that there was no requirement for this; and 4 others were unsure.

Control of backups containing data belonging to children: Of our 76 contributors from IT Management and Corporate Governance who were asked if it is a requirement to encrypt backups and separately store encryption keys where data belonging to children is held, 33 felt that it is necessary to ensure that algorithm and keys are NOT contained in backups along with obfuscated/encrypted data; 15 said that it is not necessary; and 28 had other suggestions or were unsure.

Of the latter 28 some felt that backups should be locked away in a safe (or equivalent) so the question of controlling encryption keys is not an issue, and 22 of that group felt that they could not answer the question correctly as they did not completely understand the issue. From an industry perspective this was surprising.

Control of data belonging to children in Developer and Testing Databases: It is regularly the case that organisations use a copy of their live databases for the purposes of development and testing. Such databases and the servers upon which they run are most often not maintained to the same level of security and access control as a live database.



Of our 76 contributors from IT Management and Corporate Governance who were asked if data should be scrambled immediately upon migration to a test or development database: 75 felt that it should, and there should be legislation to govern this practice. One contributor felt that this was an unnecessary overhead.

Many contributors are at pains to stress that they do actually scramble data that is placed in test and developer databases, but equally have knowledge of many organisations that do not.

Security of architecture where data belonging to children is processed and/or stored: The servers, network and other common elements such as content switches and firewalls etc. Each collaborate to make up the 'architecture' upon which data is stored, transported and processed.

Of our 76 contributors from IT Management and Corporate Governance who were asked if it is necessary to certify an architecture with an annual/bi-annual security assessment: 74 felt that it was, and that this should be put into legislation; and 2 felt that this was unnecessary. Although the vast majority of contributors feel that this is a necessary requirement, they equally raise fears regarding the financing and extent to which such audits might take place. Many contributors, particularly IT Managers assert that legislation would give them the necessary leverage to ask their financial controllers for budget to get system audits done. Where auditing is mandatory, the majority of contributors feel that it should be carried out by an agency of the Data Protection Commissioner and charged at rates that make such activity accessible to all type and sizes of organisations involved in handling children's data. There is scepticism that this requirement would become a cash cow of IT Security companies charging +/- €1000 per day.

The primary concerns of contributors relate to audit cost and frequency.

People with access to data belonging to children: This almost more than any other question raised an emotional response from contributors, particularly those who are parents. In many organisations access to application forms containing data is restricted in some fashion, usually through the use of a username and password. Within the application the user is typically only allowed to view data that is relevant to their job description. When dealing with 'back office' software, or during development or testing, very often the people involved are consultants and contractors, not necessarily employed directly by the organisation owning the application and data.

Of our 76 contributors from IT Management and Corporate Governance who were asked that where the data is belonging to children, should people with any such access be subject to vetting: 55 said yes; there were zero responses against; and 21 had other responses and ideas including:

- “Vetting should be a condition of contract”.
- “Vetting of overseas call centre and support staff would be impossible”.
- “Vetting is in itself not enough – the question should relate to a framework of checks of which vetting is one element, and checking references and other public information (including Bebo and other SN profile pages) is also required”.
- “Need exists but the service does not”.
- “Vetting and people checking is critical. It is a huge issue”.

- “The Garda Vetting Office would likely not have the means to cope if all employees with access to children’s data needed checking, and then the small matter of IT Sector consultants, contractors, support staff, developers, analysts all looking for vetting? The need is there but the infrastructure to get it done is not”.
- “This requires an independent body that will service the IT and Mobile Operator industry”.
- “In the absence of a means to achieve this, there would be a significant impact on organisations that need to work with electronic data belonging to children”.
- “Need does not arise if core personal data is already encrypted – then it is down to employees of the organisation that have proper access to data through the software provided”.
- “Organisations that use children’s data should be willing to pay to have their employees vetted. The IT Services Sector is no different”.
- “Vetting. This will not happen because it is hard to prove that an incident involving a child’s safety was directly attributable to a vetting failure. Until we (the contributor) have the equivalent of an Ian Huntley tracking kids through our (the contributors organisation) software and committing crimes against them, then it will never happen”.
- You ask questions in your study about profiling on Bebo. Are we (the contributor) any different?

One further personal comment from a contributor, which raises additional issues, is reproduced here as it was written (with the permission of the contributor):

“When a programmer walks in and works on our system, I personally have no real idea of what he does outside of work, if he looks at porn, if he does this or that. Even better, I have no idea who the next consultant is who will walk through that door and work on the data in my system, which incidentally is maintained by a large multinational managed services company. In that context I know that it has lots of people working in its data centres but I have only met two, and as before I don’t really know these people at all. We (the contributor) speak on the phone for ten minutes every other day.

If anyone works on this system and commits a crime against a child, or a domestic incident for instance, who is going to call me? So in truth I have records on thousands upon thousands of children but if you asked me to put my hand on a stack of bibles and swear that I can assure the individual safety of each child’s personal data from interference by someone who has worked on the system, then I couldn’t do it.

You don’t need to be on Bebo to be a pseudo profiler. This would be funny if it wasn’t actually real.

The Data Protection Act is meaningless when you get to this level regarding security and access to records.”

All respondents indicated that there should be legislation to govern this requirement.

Establishing the credentials of a user accessing data belonging to children: In high security environments such as online banking, the use of a simple username and password is steadily being replaced as a means of user credentialing in the computer world given the nature and frequency of attacks mounted against that method of authentication. There is favour among many organisations toward stronger methods of authentication such as “2 Factor Authentication” as a more secure method of credentialing.

Of our 76 contributors from IT Management and Corporate Governance who were asked that where the data is belonging to children, is a need to use stronger methods of

credentialing as a minimum requirement: 59 said yes; 17 said no; and the same numbers were for and against legislation.

### **Addressing Arguments for Change**

The Data Protection Act does not specify any difference in risk terms between information belonging to adults and children. Information Technology is one of the very few areas of life where distinctions between the security of children and adults are not addressed separately. It is clear that there is a divergence of thinking between IT Managers and Governors and the Data Protection Act in terms of what should apply when data is belonging to children.

The organisation holding data belonging to a person, let alone a child, is responsible through its data controller for the protection of that data. An adult can make representation to the Data Protection Commissioner where a concern exists regarding the security of such data. But what does a child do, assuming that the issue of security would occur to them in the first place?

There is acceptance that a parent or guardian would act on a child's behalf in any query of data being held by an organisation. This makes some assumptions not unlike the case highlighted previously in the section on parental responsibility for children's actions on the internet.

Given these factors, who looks after the child's interests under the Data Protection Act? These are reasons why children are a special case in many other spheres of life, and their protection under the Act should arguably be no different.

IT people have major concerns with the Data Protection Act as a tool that ensures data security. Those concerns are:

- No mandatory security audits and incident reporting.
- No clear definition of the term 'appropriate' measures for data security.
- No framework of reference and vetting for employees and external support people.

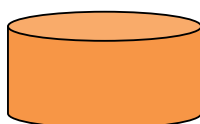
If these elements were clearly defined in legislation and were a legal requirement backed up by penalty then an IT Manager would be confident of approaching a Board or Financial Controller to make provision to ensure the necessary compliance. In the absence of such a requirement it is simply a fact that many organisations will not provide for data security to the degree necessary, as is borne out by reported incidents of data loss over the years.

To correctly frame the issues let us outline what a commercial computer system might look like, and then address the issues from the questionnaire.

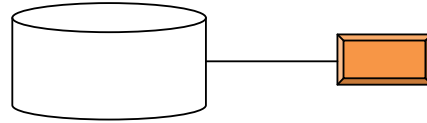
A university for example would hold records on staff, students, faculty specific data, email system etc. Data maintained would relate to anything from student personal data, to credit card processing, to staff administration, pay and allowances to name but a few.

To achieve such functionality the organisation would purchase commercial off the shelf software that is tailored to their needs for the purposes required.

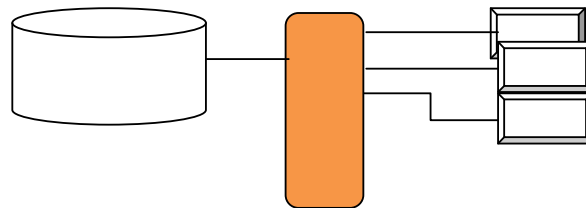
The storage of this data would likely be contained in a Relational Database:



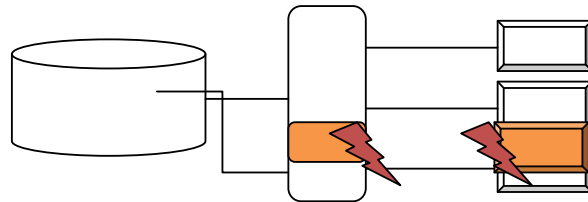
Associated with the data storage would be a means to display that data to users. One method is through Client/Server where this software is typically resident on a user's computer and connects directly to the database through means of a network cable connection:



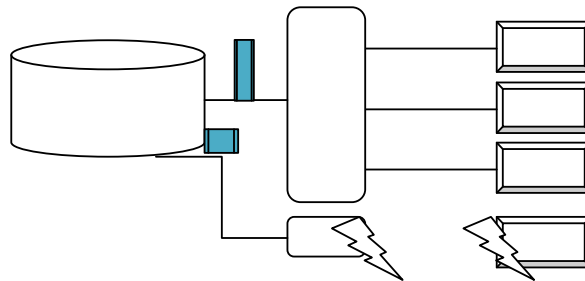
In this case many computers would be connected to the database, one for each user. This would require a series of networking hardware items such as hubs and switches to interconnect many user computers to the database.



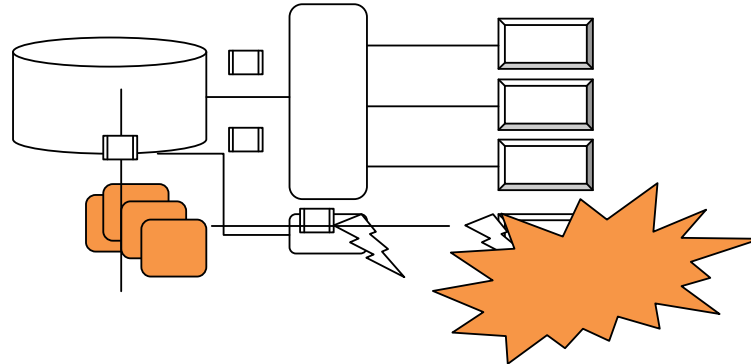
Many organisations allow wireless access from laptops within their organisations.



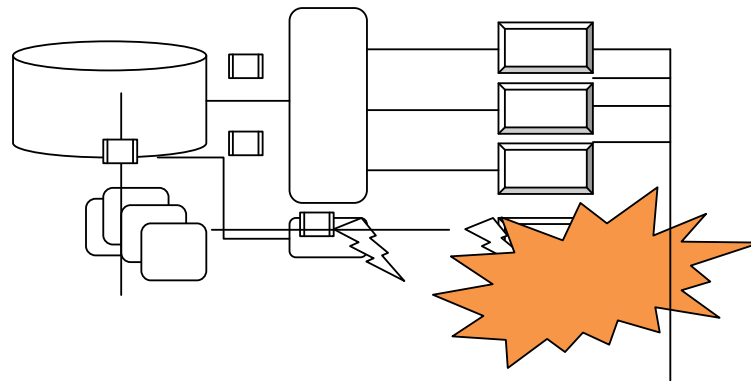
A firewall may be incorporated at a variety of strategic points to control who and what type of traffic is going where on the network.



Many systems incorporate access to and from the internet. In this case the software that manages the user's interactivity with the data will reside on Web Application Server(s) and the users will gain access through a browser or applet application.



Lastly one must consider that individual user's computers are also connected to the internet.




From the above simplistic diagram one can deduce that large computer systems are difficult to secure and administer with so many access points both locally and through the internet. The act of securing Web Application Servers is not trivial, and the requirement to have software that is robust is very important.

When one mentions elements such as applications and systems security and database administration, the first item on the IT managers agenda is cost and resources: what needs to be done and how much cash is available to do it.

IT Managers in organisations with such systems spend a lot of cash each year training and retaining in-house resources to manage systems, or buy in consultants with specific expertise in these areas. However, often there is a gap between what they would like to do, and what they actually can do. And then there is the reality of the smaller organisation with critical data to protect, but with far less resources to work with.

The stored data is kept on the database, or simply in an Excel spreadsheet in a small organisation. The responsibilities of the data controller under the Data Protection Act are the same whether the system is big or small. Large platforms such as Oracle require a lot of knowledge to correctly administer and secure. Malicious persons can draw on a wealth of information outlining flaws with large platforms and the administrator must have the time and



expertise to ensure that Data Protection Act compliance is maintained. Often organisations will employ the services of consultants to assist their in-house staff.

A database can be accessed through the software that is created to provide a user interface to its content or utilities to manage and maintain it.

The development and maintenance of software means that it is necessary to create a copy of the live database so that queries can be verified as being correctly constructed. Many organisations scramble this data as a matter of form. However many others do not and where developers and contractors are working on the database they would have open access to all the data contained therein.

An aspect requiring attention is the management of backups that are snapshots of all the database content held on a permanent media such as a tape. Access to backups is a crucial and often neglected aspect of systems security. It is not unusual to see lockers containing backup tapes remaining open and accessible to staff and others in the area.

User interface software normally comes in two forms: Client/Server and Internet. These are very different in the manner that they work and have very different security concerns associated with them. Client/Server software runs on the users own computer and connects directly to the database. The software runs on the operating system (usually Windows) and is normally fast and highly functional.


User interface software designed to work on the internet normally resides on a Web Server to which the user connects through their browser. Some software such as that written in applets can be feature rich and behave in a manner not unlike that of Client /Server. More likely to be used on the internet is browser hosted material delivered through HTML, PHP, PERL, JAVA and other platforms designed for the purpose of creating lightweight though functional software.

The risks to security and inadvertent access to data is far more serious when using web based software. The software needs to be written with great care and designed and tested by people with knowledge of the risks which are numerous. Elements like session handling and fine graining access for users with differing responsibilities is more complex to secure in web based software, as is ensuring user credentialing which is often maintained through username and password combinations, a form of security that is basic and easily attacked through conventional hacking and social engineering techniques.

Web based software is served from an organisation's web servers which themselves are part of an architecture that can include firewalls, content switches, load balancers etc. Each of these elements has its own administration and security concerns, and all need to be addressed to ensure that a system is safe.

As can be seen the primary areas of concern are architecture, software and people.

Organisations retaining credit card data are required to be licensed to do so, and must comply with industry standards in order to retain this facility. One of the difficulties with this is the fact that there is an element of ad hoc in the manner that it is being implemented. A similar situation arose in the implementation of 3D-Secure, a system to heighten the security of credit card *not present* transactions over the internet.



These examples are outlined in this report as they are pressing protocols that are being implemented as industry standards. However individual organisations to a greater or lesser degree implement or flaunt these standards as they see fit.

This is even truer where data protection is concerned. Data controllers and security officers have their own interpretations of what the Data Protection Act should mean to their organisation. And the fact that they have an interpretation doesn't guarantee that their concerns will be met in the current fiscal year.

A simple way of circumventing responsibilities under the Data Protection Act is to create a policy that looks watertight, but implement the minimum necessary to realise that policy.

Another important consideration is the belief among some IT Managers that you cannot implement too much security if it impairs the ability of the business to function. This is a crucial observation particularly applying to consumer facing organisations and government departments.

The one point that came back over and over again from respondents to this study is the requirement for legislation to compel organisations to fulfil their responsibilities under the Data Protection Act. Some argue that the Act already does this, but it has little real effect in reality.

The IT Manager needs to be able to approach the Board or CFO and state that they need X amount of allotment to enable them to comply with the law. Even more effective is to tell the Board that they need this allotment in order to pass their annual Data Protection Act 'NCT Test'.


Otherwise the reality of life in IT is that the manager will get a percentage of the resources required and not be fully compliant with the DPA.

So the message is clear. An industry standard is nothing if not backed up by a requirement in law. The DPA is watered down if compliance is not established and maintained through audit.

Where children are concerned, the majority of contributors agree that personal information should be stored in encrypted form. There is a concern that small organisations would not have the expertise to enact such a policy. In these cases it is suggested that a software solution could be supplied across the board to (e.g.) schools that would assist them in this regard.

All contributors agree without qualification that children's data in transit though any form of media should be encrypted. But what was most surprising was the adoption of the 'Hot Data' question. All but two contributors feel that data belonging to a child should be perpetually encrypted from the moment that it is captured, through its storage, and only be unencrypted when accessed through user interface software. Where this data is accessed through the internet then contributors say that this 'Hot Data' should be a requirement under law. This is also the case where this data is managed by a third party hosting and managing data on behalf of an organisation.

This is an excellent practice if adopted and solves many of the issues currently causing concern. For instance employees or contractors of a company simply could not access



children's data except through a user interface designed to present the material because it would be encrypted for its lifetime of its existence on the database.

In keeping with the previous responses contributors agree that developers and testers should have no access to the personal data of children. Such data should be scrambled in cases where it is not already encrypted as per the previous responses above.

A big issue is architecture security. This is an essential component of the safety of personal data and can cost a lot of money to properly setup, subsequently secure and then maintain that security. Many contributors feel that an annual audit is required but the costs associated with this are considerable.

Biggest among the concerns of contributors from a professional and personal perspective is the management of people with access to data belonging to children. And the key word on everyone's lips is vetting. However a better term would be Background Framework Check which would include vetting as a component, but would also include other means such as reference checks etc. This is a huge concern to people at any level and invokes strong emotions among contributors.

It is difficult to estimate the number of employees who have access to children's data and would require checking including vetting. It is far more difficult to estimate the number of programmers, analysts and designers, support and maintenance staff, consultants and contractors that have access to children's data.

As just highlighted contributors have issues with developer, system maintenance and contractor or consultant access to children's data. These groups of people would not have normal user login rights to the application as their job description has nothing to do with the administration or maintenance of the data. Yet they have access to this data in the back end through maintenance utilities.

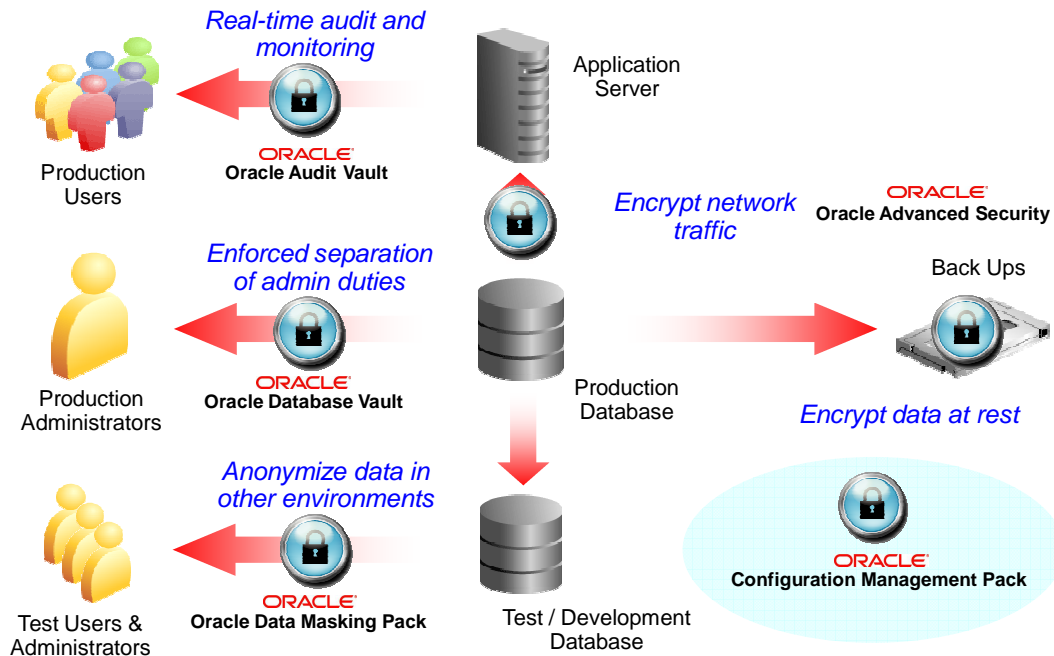
It is not difficult to understand why contributors favour the use of encryption, including perpetual encryption of data for the lifetime of its retention in the database as it solves so many person and electronic access issues.

Contributors are split on the method of credentialing used to authorise entry of that individual into the application. It is felt that security in the Client/Server software model is sufficient with username and password because for a user to gain access to the login application software, they would first need to login to the computer itself with a possible second login required to a network.

However where access is allowed through internet software where the only authorisation control is the login box, then a superior form of credentialing is favoured by contributors. An example of this is 2 Factor Authentication of which there are a number of credible Open Source solutions available for free downloading.

The next diagram shows how one industry leader addresses these issues in its products. Oracle has provided this slide from its consumer security presentation for the benefit of this study to outline an example of a major software vendor providing a range of integrated solutions to key points raised in this section of the study: data security, user access security, administrator and developer/contractor access security, backup's security, test and developer database security.

## Database Security



ORACLE

The slide above shows that the core issues being addressed in this section of the study are known and addressed.

One really interesting point worth mentioning from the study is the amount of people who are data controllers, and don't actually realise that they are data controllers. This is not as strange as it sounds.

The Chief Information Office sometimes thinks it's the Database Administrator, who thinks that it is the IT Director. More confusing is the data controller who outsources the operation to a management company, or buys in a product that is maintained (security and administration) by the supplier. Even more obscure is the Managing Director of the three person crèche who has never given a thought to their role under the Data Protection Act at all.

It is clear that where children's data is a factor, the Data Protection Act requires strengthening to adequately empower the Data Protection Commissioner to provide better Child Protection in Computerisation in Ireland.

## CHILD SEXUAL ABUSE IMAGERY (CSAI) ON THE INTERNET

(The facts and assertions in this section are known to relevant officers of the Garda Siochana and Europol, with whom correspondence has taken place in the course of this research. It would be possible to illustrate some of the assertions made here with easily accessible and shocking graphical material. For obvious reasons they have not been included.)

This section deals with what are known as Child Sexual Abuse Imagery and Child Exploitation Material. Child Sexual Abuse Imaging occurs when abusive or sexual acts involving a child are recorded. The effects of the abuse on the child (and continuing into maturity) are compounded by the wide distribution and lasting availability of the photographs and other images of the abuse.

The CSAI industry is now considered to be one of the fastest growing criminal activities on the internet today, a fact put forward by The National Centre for Missing and Exploited Children (NCMEC), the International Centre for Missing & Exploited Children (ICMEC) and other international sources.

According to the NCMEC, approximately one fifth of all Internet pornography is child pornography or CSAI. New technology such as inexpensive digital cameras and Internet distribution has made it easier than ever before to produce and distribute child pornography. The producers of child pornography try to avoid prosecution by distributing their material across national borders, though this issue is increasingly being addressed with regular arrests of suspects from a number of countries occurring over the last few years.


CSAI is viewed and collected by paedophiles for a variety of purposes, ranging from private sexual uses, trading with other paedophiles, preparing children for sexual abuse as part of the process known as "child grooming", or enticement leading to entrapment for sexual exploitation.

There is no doubt that an image or video of a child – many of them very young - engaged in a sexual act with an adult, or another child, or an animal, is illegal content. The use and distribution of this material is criminal. Viewing it is criminal. Neither of those facts appears to disrupt the growing market for such material.

The child filmed or photographed in the production of such imagery has no control over their destiny, and will be victims of the abuse, with its physical and mental after effects, and the knowledge that people throughout the world will have access to images of them being abused, for the duration of their lifetime, and probably longer than that again.

"The role of the camera should not be underestimated in the context of an assault, the presence of which enhances the powerlessness of the child in the abusive situation, diminishing the child's ability to interact or to say 'No' or 'Stop'. The child is performing for an audience, is given orders to smile etc., thus increasing the child's sense of complicity".  
(Anders Nyman, London, Dec 2001)

"Computer and digital technology has transformed the political economy of all pornography making it possible for almost anyone to be producer distributor and consumer simultaneously."  
(From "Rhetoric and Realities: Sexual Exploitation of children in Europe" by Professor Liz Kelly and Linda Regan, 2000)



This is not a new problem, but our inability as a society to protect children as victims, and adults who are exposed to such material and go on to break the law in pursuance of this material, is stark when the onset of mediums such as social networking and dual channel (mobile phone and internet) communications with children are commonplace.

When one describes that children as young as infants may be subject to rape, torture, murder (simulated or otherwise) and other types of physical and mental humiliation, it is difficult for people including those who at different levels are responsible for the care and protection of children to truly comprehend just how bad this market driven phenomenon actually is.

One such respected individual recently asked if there were boundaries of conduct in this regard, and used the term 'industry standard' when reaching to get the point of the question across. 'Industry Standard' is not something that applies to criminals who produce CSAI or CEM.

The evolution of digital media and its capability on the internet means that anyone with little resources can create CSAI imagery, some of which occurs behind closed doors of the home in which children live, perpetrated by family members.

The extent of depravity knows no bounds. Probably worst of all are instances of abuse involving torture, where children are bound, sexually abused and murdered (or murder is simulated) during the act. It is estimated that there is in excess of 800 gig's of CSAI material across the internet and is accessed through web pages, Usenet's and Peer-to-Peer networks. With the above in mind it is important to put a context on the distribution methods of providers of CSAI on the internet.


## **Usenets**

The early days of the internet were defined by the ability to download material in binary files. This facility is still available in the guise of Usenet. Many sites originally known as BBS or Bulletins Boards carried binary files depicted with names such as alt.binary.picture.\* These files are now generally found in Usenet's but some BBS still remain. Following is the policy of EPIX which has a strict policy regarding the availability of child pornography through its service.

### *Usenet Child Pornography Policy of "epix"*

*epix® Internet Services aspires to maintain a full Usenet service with no censorship for the purpose of restricting expression, yet recognizes that Internet Service Providers should maintain legitimate due care in adopting standards that reflect global societal legal consensus, which we recognize is difficult to define. It is reasonable to discern that child pornography laws have significant jurisdictional consensus. In addition, child pornography is a significantly different issue from obscenity. U.S. child pornography law is not targeted at restricting access to expression, it is written to prevent the sexual exploitation of minors in the process of producing the content.*

*Thus, epix® Internet Services reserves the right to not carry a newsgroup when its title clearly implies violations of child pornography laws. This policy specifically applies to newsgroups that are primarily used for transmitting binary/picture files containing child pornography. epix® Internet Services cannot guarantee effective filtering of all child pornography, as the technical nature of Usenet and the fact that epix® does not monitor content, makes this an impossible task.*



*Accordingly, epix® Internet Services will not carry the newsgroups listed below, under the guidance of this policy. This list may change from time to time, and every effort will be made to maintain a current list of blocked groups herein.*

Many other usenets exist, however, that employ no such policy. As a result, although there are many legitimate groups with all kinds of valid and valuable images and text, utilities and downloads, usenets have become a cesspit of CSAI where large downloads of thousands of images can occur on the click of a mouse.

## **Browser Content**

Paedophile sites are available and are often moved on to new servers following law enforcement activity. Some areas of the world are more helpful in site take down activity than others.

A number of years ago it was so simple to come across these sites which display paedophile images on the opening 'advertisement' pages that it was often the case that one could literally stumble on such a site by accident as a result of a Google or Alta Vista search. The search engines are now more particular about what they list and accidental encounters with paedophile sites is less of a problem.

However material is still getting through. Pay-per-view hardcore sites are constantly producing 'new' fresh material which means that another act of child abuse occurs to satisfy the market. There is a constant driver to produce ever new and more marketable (in paedophile terms) material for pay-per-view sites. Extensive video and images of infants engaged in all forms of sexual interaction are the norm, not the exception.


However Google among others do work with groups like the IWF (Internet Watch Foundation) and will remove listings of offensive sites when informed. Google is also using pattern recognition software analysis tools to determine CSAI carrying sites being accessed from its search pages.

A trend with paedophile sites is the creation of sites that display relatively harmless material on the front page, but the links from these images can quickly navigate to really dangerous abusive material. One occasional strategy is to dump images onto seemingly innocuous business, stamp collection or chess sites as examples.

Paedophiles are spending more time looking at 'alternative' image source sites from which to satisfy their needs. One such type is Lolikon, a Japanese Manga (comic) style artwork that portrays female children in paedophile like portraits, and Shotakon which is the male equivalent.

There is a dramatic increase in the use of computer technology to produce animated or avatar images of CSAI which is not illegal. The difficulty here is whether the image of the screaming child being abused is completely computer generated, or an image taken from an actual CSAI and programmatically rendered as the anime or avatar.

Criminal elements and paedophiles that organise sites distributing CSAI have a wealth of technology to avail of that makes law enforcement challenges very difficult. Aside from the use of proxy computers on the internet that reroute and mask connections to obscure CSAI servers, there is the ability to use hacking techniques such as XSS (Cross Site Scripting) that allow criminals to interfere with insecure genuine sites and use them to host or reroute



people to CSAI servers that they keep constantly on the move to avoid detection and eventual take down.

Some tools are available that will (allegedly) assist in stopping CSAI arriving on the home computer.

A browser safety tool such as McAfee Site Advisor will stop many, though not all, inadvertent strays into pornographic sites. It can be disabled by a user and will not stop someone who deliberately seeks to enter such sites.

Another aspect of browsing web content is the use of a variety of router networks and anonymous browsing tools. The use of some tools would allow a user to connect to the internet from a computer over an encrypted connection directly to a proxy situated somewhere in the world. This has the effect of effectively 'hiding' the content of material travelling along the internet connection to the user's computer. Using such software it is difficult for an organisation to sniff or trace the nature of the user's activity.

There is a very important distinction to be made at this point. Privacy tunnelling software is not the same as Secure Sockets Layer (SSL). SSL encrypts traffic passed between the browser and the server to which it is connected. When a user connects to their bank account it would be normal practice to protect communication between the user's browser and the banks server. Any software sniffing the network traffic would clearly see the address (<https://www.mybank.ie>) although the substance of the communication itself would be protected through encryption.

Privacy software like Net Shield operates by routing all browser traffic including SSL, into a virtual encrypted tunnel that has its gateway somewhere else in the world. The effect of having this encrypted tunnel running on the desktop computer is to render the organisation and ISP alike 'blind' to the address of sites that the user is connecting to, and the nature of the material being browsed or downloaded.


To catch a paedophile requires a lot of law enforcement man hours and is dependent on a measure of personal or technical stupidity by the paedophile. You often hear of paedophiles being tracked when they use credit cards to download material from paedophile pay sites, or being caught with images on computer hard disks, or their downloads being intercepted by the Service Providers.

In truth, the smart paedophile can avoid all of the above. The smart paedophile keeps two hard disks each with an operating system installed and each fully functional in its own right. When working he uses one disk, when roaming and stalking he uses the other. Swapping takes about five seconds on many laptops.

When using a tunnelling program as described above, where a law enforcement agency is monitoring a CSAI content site to which the paedophile is connected, they would trace a connection to the proxy gateway, and not back to the paedophiles own computer IP Address.

Paedophiles also use proxy services specifically designed and organised for their tasks. With end to end dual certificate based encryption anyone attempting to sniff and detect web activity is virtually powerless to unscramble the content.

Tracing paedophiles through their credit card payments is not straightforward. The credit card industry has been labouring over the introduction of 3D Secure, a protocol that would



ensure that online payments were made with the addition of a username and password to the normal card number and expiry date and CCV number.

In the absence of 3D Secure being implemented with 2 Factor Authentication, savvy paedophiles can generate or acquire credit card numbers belonging to others by downloading and running Luhn Reversal algorithms that create properly structured credit card number. It is possible to establish expiry dates for cards, and in many cases throughout the world, payments gateways request a security code and name/address, but never actually check it.

These are but a few of the headaches for the investigator who has to track a paedophile.

### **Peer 2 Peer Content**

Installing a Peer-2-Peer networking interface program such as LimeWire allows a user to connect to huge numbers of other computers across the internet, and thus exposes the user to whatever material may be on such computers. LimeWire is free for download from the internet.

For a young person in particular this is heaven: the ability to download complete works of a favourite artist (often illegally) without the need to get cash from mom or dad.

On searching for work from an artist a user can identify a computer hosting such content and elect to browse the host to see what else may be on this host. Now the user can list and download anything that may be shared on that host.

Equally a user may deliberately search for key search terms that will return thousands of listing for the target content.


In terms of CSAI content, absolutely nothing is off limits on P2P. Some commercial P2P software interface programs such as Kazaa restrict the content that can be viewed or downloaded. It has been shown that this is also true of Usenet. Browser content can also be restricted.

This is undertaken by many organisations, particularly government departments. It is also enabled for the general public in the UK where ISPs maintain an industry standard that is supported by the Home Office, and an independent organisation called the Internet Watch Foundation (IWF) maintains blacklisted sites where they have visually confirmed that CSAI exists on a site. Other blocking systems are functioning in places such as Norway.

No blocking exists to prevent the downloading of Child Sexual Abuse Imagery in Ireland.

### **Contributor Responses**

Blocking access to Child pornography, Child Sex Abuse Imagery and Child Exploitation Material: Of our 76 contributors from IT Management and Corporate Governance who were asked if a form of blocking/blacklisting should be used to restrict the availability of CSAI to their users and the public in general, 71 indicated such a system should be implemented,



and that same number indicated that there should be legislation with penalty to ensure that it is enforced. Five contributors indicated that they did not feel that this was necessary.

Most of the objections related to increasing restriction of digital rights from the point of view that if we block anything, CSAI or otherwise, then this becomes a thin end of a much bigger wedge. Reference was also made to scepticism regarding the workability of blacklisting/blocking, the potential for such a list to become public, and the potential for libel action by a site that is wrongfully blocked.

The overwhelming message from those in favour of blacklisting/blocking is straightforward: “This is illegal, why is it an issue at all?”

Many IT Managers argue that the absence of blocking within organisations leads to other issues such as harassment in the workplace as well as the cost and reputation damage involved with a discovery of CSAI on a computer connected to the network infrastructure of that organisation.

Use of anonymizer and encrypted tunnelling software: Of our 76 contributors from IT Management and Corporate Governance who were asked if the use of encrypted proxy tunnels (e.g. Anonymizer Total Net Shield) other than those used for legitimate commercial and personal use should be restricted, 55 indicated that there should be restrictions on such software and that there should be legislation governing the use of this software; two contributors indicating that there should be no restriction and that users should be free to use such software freely; and 13 contributors didn't have an opinion to express at all.

The latter group were defined by a surprising lack of awareness of the nature of tunnelling software and how it functions. Many contributors are unsure of how such software can be managed or blocked. Those from organisations with lesser IT spends and possibly not having a dedicated IT resource with security experience like schools, crèches etc do not appear to understand the issue at all.


### **Addressing Arguments for Change**

On the internet there are no real borders beyond language and time zone. However consumers connect to the internet through ISPs, or through organisations with their own access points directly to the net.

Ireland shares both language and time with the UK. However in the UK a system of blocking sites containing CSAI is implemented by the UK ISPs, supported by central government, and based on lists made available from the IWF (Internet Watch Foundation). The UK also has an organisation CEOP (Child Exploitation and Online Protection Centre) which actively tackles instances of paedophile activity.

We've already mentioned that Kazaa implements blocking on Peer-2-Peer and ePix does the same on Usenet's, and the UK uses a system for browser content. Implementing anything that would work on real time chat rooms would be difficult at best. However where a child is identified as being at risk, it is possible to place software on their computer that records all internet interactivity and including chat.

Ireland shares this notional internet border with the UK and does not have equivalent services with the profile and activity of CEOP, and ISPs in Ireland do not implement any type of blocking, or mandatory screening of consumer activity log files. The implication of this is a



cause for concern among many in the IT industry who see Ireland as an easy conduit for paedophiles both in Ireland and the UK.

The reasons for not blocking in Ireland as offered by contributors in that space are:

- The UK doesn't have a written constitution so has more legal flexibility to implement such initiatives.
- An ISP would be liable if it blocked content from a site in error.
- Blocking technology might not work.
- The black lists might be hacked and become available to the public.
- We (the contributor) can't see what travels on the network through an encrypted tunnel.
- Paedophiles will get their stuff from P2P or Usenet's, or another source.
- It is difficult to stumble on CSAI in the first place.
- Legislation is too cumbersome to keep up with technology innovation that might circumvent it.

Hotline, the organisation tasked with handling reports of CSAI in Ireland will tell you in their reports that no Irish sites have been discovered displaying CSAI. They will also tell you that there has been an increase in consumer reporting of sites in other jurisdictions displaying such content. They make reports through a common network of international hotlines and seek to have the offending sites taken down. This is not always successful and organisations like the IWF report significant difficulty in getting CSAI sites in certain jurisdictions taken down.


One question that remains particularly troubling: what of CSAI where Irish adults and children are involved in the production? This is a very specialist area and outside the scope of this study, but it highlights the potential that an abused Irish child may be viewed by people in Ireland. This is a relatively small country and the social implication of this point is worth mentioning in the context of the discussion on blocking content.

An initiative from international mobile operators will raise the bar regarding content blocking in Ireland. The GSMA (GSM Association) has agreed an initiative to prevent the display of CSAI on mobile networks. A timetable to implement NTD (Notice and Take Down) blocking technology to stop the appearance of CSAI on mobile phones will be in place by September 2009.

Interestingly the GSMA members accept that any system of blocking will never be 100% bulletproof, but agree that this is not a reason to do nothing at all. The initiative presents very real headaches for global players such as Vodafone. What flies in Vodafone UK may need to be tailored to be acceptable in the Vodafone Netherlands, and another variation required in Vodafone Spain. However, the central thrust of the policy is not lost within the Vodafone Group as a whole.

Possibly most important of notional barriers to adoption of blocking is the 'foot in the door' argument. If blocking is enabled for CSAI, then where will it end? Could the music industry argue that their 'illegal download' content should be blocked unless it comes from approved sites? Does it follow that sites containing 'Hate' material should also be blocked?

This really is not a serious argument in the context of CSAI blocking. People supporting digital rights and freedom of speech will assert that it is, but there simply is no comparison between illegal music downloads or proscribing the internet activities of an illegal



organisation, and blocking CSAI. Children who are participants in the production of CSAI suffer terribly, both physically and mentally. People who view this material are a potential risk within society, and the victims forever carry a burden that is virtually impossible to offload.

An image of a child being sexually abused is a crime scene. The basis of blocking is to restrict consumer access to CSAI, and to disrupt a lucrative market. Most of the cash being generated by the CSAI business is through conventional browser content, and this is where the 'fresh' content is available for purchase.

If countries or organisations take it upon themselves (e.g. the GSMA initiative) to implement blocking then this has the effect of severely restricting the market channels available to CSAI providers. Any act that strangles the ability to supply CSAI will ultimately serve the interests of children and society as a whole.

Blocking can work on a Notice and Take Down basis. Where a complaint is received about a site and a registered researcher investigates the report and confirms the existence of CSAI, the site is notified of the existence of the content and given an opportunity to reply prior to the site being blocked. This significantly reduces the opportunity for later libel complaints.

A strong argument being put forward against the use of blacklists is the fact that they may be reverse engineered and distributed in clear text. This argument is flawed for two reasons:


- There is a suggestion that not all of the individual mobile operators that are party to the GSMA want to maintain a perpetually encrypted list.
- Many CSAI sites come complete with a 'paedo' search engine and lists of bulletin boards with endless pages of links to sites that would be on that blacklist.

The argument that legislation would be too cumbersome to correctly manage technology innovation relating to CSAI in the future may well be valid. However it has been suggested by contributors with legal insight that such legislation would be enacted to manage the business case and relative industry standards adopted to adhere to that business case.

Will people determined to view such material use other means such as products that exist to encrypt content and break out to the net through proxies? Clearly the answer is yes. But where these proxy providers operate their software within Ireland or the greater EU then some contributors suggests that examination can be undertaken to determine the parameters through which they operate when they provide physical connections between their servers in places like the US, and computers located within our jurisdiction in Ireland.

There is a body of opinion within IT Management and Governance in Ireland that the term 'internet' is used as a get out clause for doing anything constructive to protect our citizens, and in their case, employees. Implementing solutions costs money and an IT Manager will not get the money required to implement content blocking unless there is an organisational reputation based reason to do it, an organisational ethos reason to do it, or it is written in law that it has to be done.

For instance Government Departments already implement content restrictions that are far in excess of just blocking CSAI, so much so that users of the system find it very restrictive. CSAI Blocking is very specific and does not filter content based on keywords and other such criteria that can result in genuine content being restricted where certain language is used in a document for instance.



The case for and against Application Providers of Tunnelling Software is another difficult matter. Many of our contributors were unsure of this question which account for the number that did not respond to it at all. Facilities such as The Onion Router and Anonymizer products to name but two allow for greater privacy when interacting on the internet. They effectively shield the source and routing of a user connected to the internet, and in the latter case can encrypt all traffic leaving a computer to a designated proxy server located somewhere in the world, usually the US.

There is nothing illegal about these techniques or programs. In fact they go a long way to guaranteeing privacy of the individual user when online. However there is concern that these mediums can also be used to allow persons browse and download CSAI from internet sites rendering the transaction completely private. This is a big issue for an organisation where that user is an employee, student, contractor, or other users of that organisation's facility. If this illegal material is being downloaded to a PC that is an asset owned and maintained by the organisation then there is an onus on that organisation upon discovery under the law. What if that user has a personal laptop and is downloading such material within that organisations network? Many contributors are unclear of the requirements under the law where anonymous networking software is used. Under the law an organisation is liable where it has knowledge that the material is being downloaded.

## CHILD PROTECTION IN THE ELECTRONIC AGE – RECOMMENDATIONS

- 1) Urgent consideration be given to the development of a commercially viable Age Verification and Identity Management (AV/IDM) program for children.

### 2) Data Protection Act:

The Data Protection Act be amended to:

- i) Ensure mandatory data breach reporting with significant penalties for organisations and government departments failing to comply.
- ii) Address the needs of children separately from adults under the act.
- iii) Create a criminal offence for persons who represent themselves as a child when contacting children through electronic means.
- iv) Amend the law to clearly state the age of understanding for the purposes of making ones personal data available on the internet.
- v) Create an offence for any organisation (domestic or international), to display personal data belonging to a child under the established age of understanding where it is determinable from the child's own input that they are in fact under that age, or where that organisation is made aware through a 'trusted' source such as a Hotline that this is the case. Note that this is a matter of subsequent user moderation, and does not require any Social Network to adopt an Age Verification/Identity Management solution.

### 3) Data Controls

In addition to the term 'appropriate' as used in the Data Protection Act, ensure the privacy of a child's personal data where an organisation or government department retains data belonging to children:

- i) That data used for testing and development is in scrambled form.
- ii) That data in any form of transport through network or other means is encrypted.
- iii) That data held on devices such as laptops which are located outside of the protected environment of the organisation are encrypted.
- iv) That where data is manipulated through means of the internet, or through a hosted or managed service, that it is perpetually encrypted at the point at which it is received, and its subsequent storage in the data store.
- v) Ensure that all user interface software correctly discriminates between application users depending on their area and level of responsibility with the data.
- vi) Ensure the privacy of data from persons other than those connecting through the user interface software with the options:
  - (1) Encrypt a child's personal data rendering it unusable by parties such as developers, maintenance and support staff, consultants and contractors etc.
  - (2) Deny access to persons unless they have had a Background Check including Garda Vetting.
  - (3) Ensure that all persons connecting to a user interface application displaying children's data have a suitable level of credentialing in Client/Server applications, and a minimum of a second factor when the user interface is accessible through the internet.

### 4) Licensing for Child Data Processing

Organisations seeking to process or store data belonging to children must:

- i) Register to do so.
- ii) Receive a license following an initial audit to determine the appropriateness of their policy, and actual implementation of data controls in conjunction with that policy.

- iii) Office of the Data Protection Commissioner to be augmented with a new self-funded commercially viable office with responsibility to:
  - (1) Initially certify and license organisations as per the amended act.
  - (2) Carry out an annual certification renewal audit to ensure that the organisation continues to maintain appropriate data protection compliance, particularly where the system or software is upgraded, or new additions have been developed or purchased off the shelf.

#### **5) Refine use of the term 'Child Pornography' in legislation**

This term is inappropriate to describe an act of child sexual abuse, the recorded imagery of such abuse, and other acts of exploitation against children in the context of the creation and distribution of such imagery. The report recommendation is to adopt the term Child Exploitation Material (CEM) as used by Interpol.

#### **6) Paedophile Investigation Unit**

This unit of the Garda Síochána should be enhanced and publicised in a similar manner to the level of visibility of the UK's CEOP to deter the operations of paedophiles operating through Ireland. In the absence of other practical controls on internet usage, raising the profile of this unit could be a significant deterrent to those who may wish to threaten the security of a child in our jurisdiction. The report acknowledges that CEOP and its operational context do not apply to An Garda Síochána, and this recommendation relates to the public face of the Paedophile Investigation Unit. Further, people in IT do not have a clear understanding of the techniques and mechanisms adopted by this Unit, and individuals can be reticent to make reports where they suspect (as against being completely sure) that a user of their system may be downloading or viewing.

#### **7) CEM Site Notice and Take Down (Blocking) Policy**

- i) Creation of legislation to require implementation of a system of protection for Irish consumers from CEM content by way of a Notice and Take Down methodology.
- ii) Statement within the legislation clearly ensuring the use of this in the context of CEM only.
- iii) Adoption of an industry standard compliant with the legislation for ISPs and all organisations providing direct access to the internet for consumers and employees respectively.
- iv) Mandatory inclusion of ISPs operating in Ireland irrespective of membership with established industry groups such as the ISAPI.
- v) Creation of a working group to establish recommendations of methods of control of CEM content coming from: Peer-2-Peer, Usenet's, Privacy channel such as TOR and anonymous networks, IRC Channels.

#### **8) Aggressive Media Campaign**

Creation of a series of advertisement videos to target parents and children separately outlining the real dangers in a manner not unlike AIDS and Alcohol & Driving campaigns.

#### **9) Mandatory Panic Facility**

The creation of a simple but effective 'Panic Button' on sites facilitating interactivity involving children that allows a child that is worried about a developing difficulty to get immediate support from an agency such as Child Line, Parent Line, Hotline, An Garda Síochána, or other organisations participating in this service. This exists in the UK and is highly successful as both an outlet for a concerned child, and a deterrent to a person behaving in a manner not appropriate to that child.



**10) Office of Internet Safety**

This office should be restructured to ensure that it is independent of all vested interests, and placed on a statutory footing.