CORPORATE PAEDOPHILIA

The Role of South African Organisations in the Fight Against Child Pornography

November, 2008

The Internet is one of the major channels through which child pornography is viewed, downloaded and distributed. In South Africa, the workplace provides the widest access to the Internet and email and as part of its efforts to prevent and control the prevalence of child pornography, the Film and Publication Board (FPB) needed to understand what organisations are doing to prevent the viewing, downloading, or distribution of child pornography at the workplace.

The survey was conducted amongst management and employees of organisations (private and government) from many different sectors, by province.

Conducted on behalf of FPB by
Plus 94 Research

Table of Contents

Section 1: Executive Summary

Section 2: Study Background

Section 3: Findings Phase I

Section 4: Findings Phase II

Section 5: Conclusions and Recommendations

Executive Summary

1.1 Research Background

During the 6 month period (April-September 2008), the Film and Publication Board (FPB) conducted an extensive research study that sought to provide insight into the level of understanding and engagement organisations within South Africa and their employees had on the subject of child pornography in a workplace setting. The research study was in two main phases, namely an initial qualitative/quantitative phase targeted at organisations, followed by a purely quantitative phase targeted at organisation employees.

Respondents were asked various questions on policy (computer use, email, Internet, etc.), the methods used in informing employees on how to conduct themselves in their IT correspondence with colleagues, and recalled cases of fellow employees being caught either viewing, downloading or distributing child pornographic material in the workplace. Also respondents were questioned about the likelihood of them reporting incidents of child pornography viewing, downloading or distribution in their workplaces.

1.2 Findings

- Most organisation policies on computer use frown on the use of workplace computers for personal purposes, but still employees stated that most of their Internet activity was for personal reasons and the second most common type of emails sent/received were from personal contacts.
- Employees are placing restrictions on themselves in terms of the amount of time they spend surfing the Internet. Organisations seem to be placing a greater amount of importance on the content that employees are able to view on the Internet.
- Around 65% of all respondents knew that they were being regularly monitored and being kept in check by their It departments and IT software.
- 22% of respondents had received pornographic emails in the past. And 6% had passed on pornographic emails to colleagues.

- There were not many reported incidents of child pornography viewing, downloading or distribution in the organisations surveyed.
- There was insufficient awareness and understanding of the subject of child pornography in the corporate environment. There was a greater amount of understanding on the subject of child pornography demonstrated by employees than organisations.
- Around 70% of all employees had a good enough understanding that 'child' pornography was distinguishable from 'adult' pornography. Also 95% of all respondents agreed, when prompted, that child pornography was the sexual exploitation of children.
- About 80% of all respondents thought that child pornography was a real problem in South Africa.
- Only 1% of all organisation employees have ever participated in workshops and training on the subject of child pornography.
- A majority of respondents felt that there was both a moral and legal responsibility for organisations to prevent and report instances of child pornography in the workplace.
- Close to a third of organisations said that their organisation had no policy regulating the viewing, downloading or distribution of child pornography. A little over half of those respondents indicated that policies on the regulation of child pornographic material had either never been considered or were not seen as being an important priority.
- For the most part, existing policies did not include explicit reference to the accessing/viewing, downloading or distribution of child pornography.
- The existence of policy did not have a direct correlation, on the whole, to the enactment and proper enforcement of the policy specifications and legal obligation.
- Rates of awareness and understanding between organisations and employees are not synchronised. 71% of organisations in South Africa have an existing anti-child pornography policy, however only 40% of all employees know of such a policy. This is despite such policy documents and specifications being distributed in a wide range of ways including; being included in their employment contracts, management holding regular briefings and verbally explaining policy.

- The most distinct action taken by a very limited number of organisations was to insist on people involved in cases of child pornography attending counselling sessions.
- Around two thirds of all respondents included in the study were very interested in attending workshops and seminars educating them on the anti-child pornography campaign.

1.3 Recommendations

The research study outcomes present an organisational landscape that is not uniform in the way it perceives the prevalence and extent of the problem of child pornography in South Africa. Organisational behaviour, in terms of the manner in which child pornography offenders are dealt with is at best marginally successful at dealing with the problem within the workplace, and at worst it undermines the legislation put in place to regulate and monitor child pornographic material.

Strong motivational tactics need to be adopted by government and specifically the Film and Publication Board, in drawing policy makers within organisations into the fight against child pornography.

- A more visible anti-child pornography fight needs to be adopted. This would apply strongly to anti-child pornography legislation becoming better known in the general public and specifically in workplaces around South Africa.
- Education on the link between child abuse and child pornography need to reiterate amongst employees and in the organisations they are employed.
- Frequent workshops, that involve the active participation of organisation senior management, are a necessity in informing current and future anti-child pornography policies with organisations.

Section Two: Study Background

2.1 Introduction

According to *Internet World Stats*[1], Internet usage in South Africa grew by 112.5% between 2000 and 2008. South Africa had an estimated 2.4 million users in 2000. As of March 2008, the number of Internet users has risen to 5.1 million – and rising. It would probably be difficult to find a single company or business in South Africa that operates without at least one computer. Research in the United States and the United Kingdom with regard to corporate computers has, however, revealed disturbing trends.

Statistics compiled by Web watchers, for instance, provide clear evidence that employees with Internet access spend a great deal of company time accessing, viewing and downloading pornography, including child pornography. According to SexTracker.com[2], "*.....approximately 70% of all Web traffic to Internet pornography sites occurs between the traditional work hours of 9 a.m. and 5 p.m.*" Family Safe Media reported in 2003 that more than 2.5 billion e-mails per day are pornographic in nature.[3]

Twenty five percent of all search engine requests, according to Dr David Bissette, are *"pornography-related"* and *"more than 75 percent of people at work report having accidentally visited a pornographic Web site, while 15 percent of workers report having 'accidentally' visited such sites more than 10 times".* [4]

According to law enforcement officials in the United States and Canada, 19 000 computer hard drives in Virginia, USA contain child pornography,[5] while about 45 000 computers across Canada are involved in trading child pornography.[6] The majority of these are corporate computers.

[1] www.internetworldstats.com
[2] *Workplace Web Use: Give 'em an inch....*, Douglas Schweitzer, SearchSecurity.com, 2004
[3] *Pornography Statistics 2003*, www.familysafemedia.com, 2003
[4] *Internet Pornography Statistics: 2003*, www.healthymind.com, 2004
[5] www.inrich.com/cva/ric/news/politics.apx
[6] CTV.news, *Star*, Toronto, Canada

Security experts are convinced that child pornography is hidden on “virtually every large corporate network”.[7]

“While it's common to hear stories of workers being fired for downloading pornographic images onto their systems, and it's even more common to hear people complain of pornographic spam, industry watchers say the problem goes even further. Child pornography -- explicit images and text dealing with underage children -- can be easily found on nearly every large network -- be it corporate, academic or government.

"If you've got a big company system, I can almost guarantee that you have child pornography on it," says Kenneth Citarella, deputy chief of investigations with the Westchester County District Attorney's Office. "It's there somewhere."

“And analysts and law enforcement say it's not simply a case of someone accidentally opening an offensive spam message. "We're not talking about that one click to open and then 'Oh, my God' and delete," says William Eyres, chief executive officer of the Joint Council on Information Age Crime. "That's not the problem. It's a different level. Someone downloading thousands of pictures is a different story."

“Edward Appel, chief operating officer of the Joint Council, agrees with his colleague, adding that there's 'almost a 100%' probability of finding child porn on corporate networks”[8].

According to David T Cox,[9] *“.....corporate employees with Internet access at the office spend about one-quarter of their time online, accessing sites unrelated to their duties.*

Many of these employees are visiting sexually explicit sites with a regularity preceded in traffic only by news sites. Moreover, seventy percent of workers who use email admit they received adult-oriented email on the job. The result of all this cyber-philandering is that one in four corporate computers contains pornographic files.”

A survey of 200 IT companies in the United Kingdom by the Internet Watch Foundation, found that 75% of the companies would not report employees caught downloading child pornography

[7] Reported in *Business*, 14 February 2003

[8] ibid

[9] *Litigating Child Pornography and Obscenity Cases in the Internet Age,* JTLP Summer 1999 Edition

in the workplace to the police, and 38% would not even discipline or sack an employee for downloading illegal pornography.[10]

Web watchers and law enforcement officials are not surprised at the number of employees who access, view and download pornography, including child pornography. Corporate computers are, generally, more sophisticated than home computers. Using workplace-computers allows employees to hide such perversions from their spouses and other members of the family. Additionally, many employers do not monitor the use of corporate computers for illegal activities and some even seem to be unaware of the potential liability[11] of employers for the illegal conduct of their employees with respect to the viewing and downloading of child pornography. Many employers also hide behind the principle of an employee's right to privacy, thus allowing employees unfettered freedom to abuse corporate computers.

These disturbing trends triggered concern about the situation in corporate South Africa, and led to the Board's commissioning of this research into the attitude and response of South African companies and government departments to the increasing global trade in child pornography.

Iyavar Chetty
Antoinette Basson
Film and Publication Board

[10] Reported in *Breaking Business and Technology News* @ silicon_com.mht (2005)

[11] In the case of *Doe v XYC Corp (887 A.2d 1156 N J Superior Court App. Div. 2005)*, a New Jersey, USA, appellate court held that an employer could be held liable to a victim of child pornography based on the actions of one of its employees. In that case, the employee's wife and mother of his 10-year-old stepdaughter filed a negligence claim against the employer after learning that her husband had been using his workplace computer to view and distribute nude photographs of his stepdaughter. The mother's claim was based on the employer's failure to detect and stop her husband from using his workplace computer to interact with child pornography web sites, thereby allowing him to "*continue clandestinely photographing and molesting"* his stepdaughter. The court held that the facts presented a compelling case for liability on the part of the employer

2.2 Brief Overview of the Study

The findings from Phase I indicated that the level of awareness and understanding of the fight against child pornography, amongst organisations in South Africa, was somewhat lacking. Further inquiry needed to be made in order to weigh organisation awareness and understanding (with influenced organisation policy) against employee awareness and understanding. The employee sample was drawn from a broad spectrum of organisations in the private sector as well as from government departments.

For the purposes of this report the generic term ‘organisation’ will be used to refer to both government departments and private sector enterprises (the two main segments in the study). There will be occasion where specific mention is made to ‘government departments’ and ‘private sector’. This will be in the case where particular aspects of the findings concern only one of the two segments.

2.3 Study Objectives

2.3.1 Phase I

The main objectives of Phase I were as follows:

- To test awareness and understanding by organisations of what constitutes child pornography
- To determine the existence and nature of policies and measures that organisations have in place to prevent the viewing, downloading or distribution of child pornography at the workplace
- To assess the prevalence of child pornography within the workplace as reported by organisations and determine what measures are taken against the offending employees
- To test awareness and understanding of anti-child pornography laws in South Africa, such as the Sexual Offences Act and the Films and Publications Act, No 65 of 1996 (and its amendments)
- To assess the level of motivation within organisations to fight child abuse and child pornography.

2.3.2 Phase II

Phase II was directly aimed at evaluating the levels of awareness and understanding of individual employees on the subject of child pornography, as opposed to the organisation as a whole. Respondents, during the interviews, therefore based their answers on their personal perspective and were not speaking on behalf of the organisation with which they were employed. The main objectives were as follows:

- The awareness and understanding employees have of child pornography; the definition of child pornography, the incidence of child pornography in their workplace
- The awareness and understanding of anti-child pornography policies that may or may not exist in their workplace aimed at addressing issues pertaining to the viewing, downloading and distribution of child pornography by employees.
- The effectiveness of anti-child pornography policies in curbing the viewing, downloading and distribution of child pornography by employees.
- The awareness and understanding of laws in South Africa, such as the Sexual Offences Act and the Films and Publications Act, No 65 of 1996 (and its amendments)

2.4 Methodology and Sample

It was a basic requirement that all respondents who participated in the study should have access to email and/or the Internet. This applied to both phases.

2.4.1 Phase I

In the initial Phase I, 270 respondents were interviewed, in face-to-face in-depth interviews (20 respondents) and in the web-survey (250 respondents). The in-depth part of this phase focused on senior management of large companies within South Africa in diverse business sectors. Of the types of management representatives included in the survey, there were management from Information Technology (IT), Corporate and Government Affairs, Legal Affairs and Human Resource (HR) departments.

Included, in the web-survey interviews, were human resource managers of small and medium companies (SMME's) and government departments. Specifically, within the private sector, organisations were involved in a range of industries with the most number of organisations falling into the manufacturing, construction and financial services fields and the least falling into the sanitation and engineering fields.

2.4.2 Phase II

In Phase II, 750 computer aided telephonic interviews (CATI) were conducted. The use of the CATI methodology was very helpful and best suited to this phase of the study as it allowed interviewers relatively easy access to employees of different designations within organisations in diverse industries from around the country.

Of the total sample size, 450 interviews were conducted with employees in private sector organisations and 300 with government department employees. Employees were divided into four main, namely: top management, middle management, skilled operational and junior staff.

The sample distribution (by province) was based on available employment percentages and financial activity recorded in AMPS 2007 (b)[12]. Most respondents were employed in organisations in the Gauteng province, while the least represented province was the Northern Cape. The business sector distribution gathered from the findings covered many different sectors, the most represented in the private sector being; construction, professional and business services, financial services, manufacturing and retail

[12] SAARF: http://www.saarf.co.za

Section Three: Research Findings Phase I

3.1 Understanding and Prevalence of Child Pornography

3.1.1 Awareness and Understanding

One of the most striking aspects of the findings was the confusion that persists amongst individuals and within organisations as to what constitutes child pornography. Respondents, for the most part, did not make immediate links between child abuse and child pornography.

When asked to provide a prompted definition as to what the term 'child pornography' means, the majority of respondents (99%) did in fact know that it was the sexual exploitation or abuse of children. However this correct reply by respondents might be a little misleading, as unprompted responses to the same question, revealed that respondents had mixed notions about child pornography that were mostly incorrect.

Respondents saw the issue of child pornography in heavily gendered terms, as they implied that what constituted child pornography was the sexual exploitation of *girl* children by adult men. No mention of boy children was ever provided. Also there was slight confusion as to who, legally, was a child. Respondents were not aware that anti-child pornography legislation defined the 'child' in child pornography as any person who was depicted in sexual material as a child, and not necessarily a child in any age specific manner.

3.1.2 Corporate Values, Ethics and Child Pornography

Respondents perceived pornography – in its many manifestations – as violating their personal values and ethics. They also saw pornography and specifically child pornography as something that not only violated but could cause irreparable damage to their organisation's public image.

The obsession around public image and perception was particularly evident in the responses by those respondents from the private sector, especially within the financial services.

Consequently, even though there was confusion and misunderstanding as to what child pornography was, respondents said that it was important to regulate the type of information and content entering and leaving organisations through organisation resources such as computers and email/Internet facilities. 14% called for tougher discipline and action in protecting the workplace from child pornography. While 6% stated that organisations should do more in terms of email and Internet monitoring to ensure child pornography is not disseminated through the workplace.

3.1.3 Legal Obligation in Reporting Child Pornography

There was the feeling that organisations had both a moral and legal responsibility to prevent and report instances or cases of child pornography. There was a high proportion (76%) of respondents that said their organisations were aware of the legal obligation to report knowledge of child pornography. A lower, proportion (63%) of respondents said that the Film and Publications Act, with respect to child pornography was known to their organisation.

Even with this generally high level of perceived responsibility and awareness, a small number of respondents could recall that they had had cases of child pornography in the past. There were 3 and 5 reported instances of the viewing, downloading or distribution of child pornography in government departments and the private sector respectively.

Most respondents confidently said that a possible reason for organisations not having many cases of child pornography was that employees were generally quite *busy with their work* and therefore did not concern themselves with viewing, downloading or distributing child pornography.

There were a minority (2 organisations) of respondents who mentioned that their organisation had noticed the potential – and secret – abuse of organisation IT facilities such as computers, email, Internet and portable devices (USB drives and cellular phones) in encouraging the viewing, downloading and especially the distributing of child pornography.

3.2 Policies and Measures to Control Child Pornography

3.2.1 Presence of Policies and Monitoring

76% of all organisations had a general computer usage policy in place. There were more government departments with general computer usage policies organisations within the private sector that had such a policy (94% and 70% respectively). Significantly, 31% of private sector organisations did not have a policy. Nevertheless, overall, a majority of organisations had a policy on the monitoring and regulation of general computer use by employees.

71% of organisations had specific policy on the viewing, downloading or distribution of child pornography. There was no significant difference between the proportion of government departments and private sector organisations that had a specific anti-child pornography policy.

Of the organisations that did not have such a policy, organisation perceptions of the degree of importance of the issue of child pornography in the workplace was relatively low. These organisations saw child pornography as being somewhat irrelevant in their business objectives and operations, as a third of these organisations had never even considered introducing a specific anti-child pornography policy. 12% saw no need for its introduction.

Yet within this bleak outlook at how organisations are perceiving the problem of child pornography at the workplace, there is some hope as almost 20% of organisations were either in the process of introducing anti-child pornography policy or had not as yet decided whether to introduce it or not.

3.2.2 Liberal Usage and Monitored Usage

From the policy landscape described above two distinct types of organisation behaviour are common in the South African workplace, in terms of the manner in which policy is enacted. Presently organisations can be described as falling into either the Liberal Usage or Monitored Usage categories, and each category shall be outlined briefly:

- Liberal Usage organisations would typically have minor measures in place to track Internet traffic and also the size of inbound and outbound emails. No monitoring of the content of emails would be conducted. The measures used could include the outsourcing of IT services to an external company or having infrequently updated Internet website filtering software. *This approach was very reactive and employees were charged with keeping checks on themselves and in effect police themselves.* Liberal usage organisations only dealt with the issue of the viewing, downloading or distribution of child pornography (or any other material that could be classified as indecent or offensive) when an employee was caught abusing the rules and regulations.

- Monitored Usage organisations usually would have in place a highly skilled forensics unit that kept an eye on all Internet traffic. Through random or systematic quotas this unit would select emails that would be inspected for a wide variety of sensitive or undesirable material, including pornography that was outlined in the organisations policy document.

  Nevertheless, even though these organisations had stringent measures in place, there still persisted a perception by IT personnel that employees who wanted to cheat the system, and download and distribute sensitive material such as pornography, were increasingly relying on smarter ways in which to store large files and data on organisation computers and intranet/central systems/networks. *The device most mentioned in this underhanded behaviour was the USB drive/memory stick*. IT personnel explained that the device's relative affordability and ease to use assisted the user in distributing content quickly from computer to computer in the workplace and without too much detection.

A majority of organisations would have to be placed into the Monitored usage category. However, the level of monitoring varied as policies amongst organisations with anti-child pornography policy was different. The difference can be noted, not only in the manner in which email and Internet activity is regulated and monitored, but also in the policy specifications.

For instance, if an employee was found to have viewed, downloaded or distributed child pornography, organisations could choose to do one of the following things; initiate internal disciplinary action, report offending employees to law enforcement agencies or terminate an offender's employment contract.

3.2.3 Existing Anti-Child Pornography Policies

The following is an excerpt from one of the organisations that were willing to show interviewers their organisation policy:

> *"We as the company provide the employee with computer equipment and online access to internal and external networks between the Internet so that they may communicate more effectively, serve clients better and achieve the company's business goals…*
> *Our company prohibits the use of Web or any other Electronic Communication Services or equipment to access or transmit pornography and or indecent material, promote online gambling or transmitting hate mail…*
> *By signature of his document, I as the employee acknowledge that I have understood and agreed to the contents of this policy and is therefore permitted access to the Internet and other resources provided by the company"*

The majority of the organisations with a general computer usage policy did make specific reference to the viewing and distribution of pornography in the workplace. No organisation included in this phase of the study made mention of an explicit mention to child pornography in their organisation policy document. It was simply assumed, by senior management, that employees would know that 'pornography' included the viewing and distribution of child pornography and that this was included in the 'indecent material' mentioned above.

3.2.4 Policy Specification and Employee Access to Information

Of the organisations that had both general computer usage and anti-child pornography policy, what emerged was a mixed bag of specifications and ways in which the policies were enforced.

To best look at these varied policies it is better to describe the natures of the policies. Firstly these organisations, for the most part, did make mention of the types of employees allowed access to using particular programmes. 38% of organisations allowed their whole workforce access to email and the Internet. Mostly management staff was allowed the most amount of freedom as to which programmes they could use and also the most amount of flexibility of use.

A small number of organisations did restrict the time employees could spend on the Internet and the type of email accounts that could be accessed using organisation Internet. With these organisations, an in-house email account was created for each employee so that IT monitoring could be more efficient. In terms of keeping a check on individual inbound and outbound emails, mailbox space allowed was relatively smaller than that made available in external email accounts. A few organisations included restrictions on the length of time spent on the Internet as it was assumed that far too much time spent on the Internet may influence employees to view or download pornographic material and affect work productivity.

Specifically on Internet use, organisations tended to place great importance on the types of websites visited by employees rather than the length of time. Most organisations (69%) had filters or firewalls in place that hopefully would restrict employees accessing undesirable or indecent material such as pornography. However there was a spotty approach to the quality and effectiveness of these Internet barriers as some organisations did not bother too much in ensuring that the filter specifications were regularly updated.

3.2.5 Communication of Policy

The effectiveness of the messages contained within policies in reaching employees and also the level of enthusiasm and respect employees treat the policies is important in being able to gauge how successful current measures by organisations are in fighting child pornography.

There are, broadly, five common means of organisations communicating the policy to employees, namely through:

- The employment contract
- The Intranet/Central network

- Email
- Induction process/continuous briefing sessions
- During the logging-on process (to the Internet)

The burden of ensuring proper communication lay with HR managers and officers as they were either meant to include policy specifications in employees' employment contracts or initiate and conduct induction or briefing sessions that would help in verbally communication. IT managers and officers were largely responsible for sending out emails that reiterated the policy to employees, but this was largely done on an adhoc basis. IT personnel were also responsible for the posting of policy reminders on the Intranet and also into the logging-on processes, and this it was hoped, could give employees a quick reminder before they accessed information on the Internet.

Most of the communication methods in use were voluntary in nature and depended on employees taking the initiative to either attend briefing sessions, open emails or open documents put onto the Intranet, as shown in the following table:

Communication method	Total (n=177)	Government (n=39)	Private Sector (n=138)
Management verbally explains the policy to employees	50%	51%	47%
Written and included in their employment contract	48%	44%	52%
Written and available to them on the intranet	29%	62%	21%
Written and sent to them via email	20%	33%	16%
Written and distributed in pamphlets	10%	21%	7%
Written and posted on notice boards	10%	13%	10%
Host awareness workshops	2%	8%	1%
Document signed by employees	2%	-	3%

Looking at how employees may perceive the anti-child pornography policy, respondents were asked to what extent employees in their organisations followed or respected the policy.

The majority of respondents said that employees followed or respected the policy entirely. However it must be mentioned that about a quarter of government department respondents said that employees only partly followed or respected the policy.

3.2.6 How Violations Are Handled

It has been mentioned that a very small number of organisations had revealed any cases of the viewing, downloading or distribution of child pornography. In terms of how offenders were dealt with, only government departments were said to have ever reported an offender for criminal prosecution.

The private sector tended to not report offenders for criminal prosecution, even though a high proportion (75%) of private sector respondents said that their organisations were aware of the legal obligation to report offenders to law enforcement agencies. The private sector preferred to make use of internal mechanisms for dealing with employees who viewed, downloaded or distributed child pornography.

External mechanisms for dealing with child pornography offenders, such as reporting offenders for criminal prosecution, were not accessed at all. The trend was for these organisations simply terminate the employment contract of offenders and not to contact the relevant authorities.

The most common specification in all organisations was that of issuing employees with written warnings. This occurred in 3 government departments and 1 private sector organisation. Government departments (3 departments) were alone in reporting cases of child pornography in the workplace for criminal prosecution. Only the private sector respondents, made mention of a policy specification on offending employees being giving psychological counselling/assistance (2 departments).

Section Four: Research Findings Phase II

4.1 Overview

The relationship that organisations imagined existed between the organisation policies and employee behaviour was tested. As the findings indicate, there are a few gaps in the manner in which organisation policy reaches employees and how employees themselves relate to it.

4.2 Employee Profile

The organisation profile, where respondents were employed, varied. Most respondents (78%) were employed in small to medium organisations, and 22% in larger organisations. Two items of interest should be noted that are relevant in the findings of this phase: firstly, the private sector tended to employ far fewer employees than government departments (in a single branch) and the proportions in this phase mimicked the size distribution in the previous phase.

In terms of employee designation, access to top management respondents was somewhat difficult, especially in government departments. However 14% of the complete sample comprised of top level management. Middle management and skilled operational employees were the most represented.

The strong presence of these employees in the survey provides a good base for a better understanding of the workplace environment and how employees conduct themselves, as typically these sets of employees would have had the greatest amount of interaction with other employees within the organisation and perhaps have worked in that organisation for some time.

4.3 General Computer Usage Policies

Overall 54% of respondents stated that they definitely knew of a general policy regulating employees on the use of computers created by their employers. The proportions of respondents who knew of such a policy were higher amongst government employees (69%) than private sector employees (44%). It is not too surprising that more government employees knew of such a policy, as more respondents within this employee segment reported that they knew of this policy as it had been included in the employment contract.

Generally the communication lines in government departments as opposed to the private sector, appeared to be more open, the only exception being in the level of verbal communication. Only 44% of government department employees, compared to the 52% of private sector employees, said that senior management had verbally explained policies to them.

Of the respondents who said they knew of such a policy, the most common features of policy mentioned were:

- Company computers are not to be used for personal reasons
- Pornographic websites should not be accessed/viewed with company computers
- Certain websites are blocked/restricted
- Employees are allowed access to the Internet during specific times only
- Employees are prohibited from downloading illegal information from the Internet

As can be seen in the above mentioned, organisations had a keen interest in guarding employees from perceived threats from the Internet.

4.3.1 Email and Internet Usage by Employees

Some respondents contradicted themselves when outlining policy specifications and then mentioning the types of computer or Internet activities they engaged. Regardless of the policy specifications, a substantial amount of respondents reported that they engaged accessed personal information and content using workplace computers, email and Internet. A quarter of all respondents reported that they mostly accessed their personal email, surfed the Internet, read news updates, sought new employment opportunities, visited social networking websites, and the like.

Specifically on email accessibility, government and private sector respondents stated that they sent and received 93% and 83% work related emails, respectively. What is bothersome, in terms of restricting unwanted external content from the secure workplace environment, is that 8% of respondents reported that they regularly receive unsolicited emails.

The picture of the work environment that respondents further painted was quite interesting. More than three quarters (78%) of all surveyed employees do not share the use of the workplace computer with any other employee, as illustrated in the table below.

Number of employees sharing computer	Total (n=163)	Government (n=61)	Private Sector (n=102)
Zero	1%	2%	-
1-2 employees	45%	43%	46%
3-4 employees	26%	26%	25%
5-6 employees	13%	11%	15%
7-8 employees	2%	2%	2%
9-10 employees	5%	7%	4%
11-20 employees	7%	8%	7%
20 employees or more	1%	2%	1%

Theoretically, the proportions of employees not sharing the use of a computer makes the probability of using these computers for illegal purposes high since the chances of being found out by fellow employees would be small.

Counter to this, however, is the 22% of respondents (from government and the private sector) who share their computer with at least one other employee. These respondents would have a greater chance of coming across unwanted information from fellow colleagues.

An interesting feature of employee behaviour, in relation to the manner in which they access information in the workplace, is the self policing or regulation that occurs. 73% of all respondents spend less than 2 hours accessing their email and/or the Internet. However a substantial 15% of respondents spend more than 6 hours – almost the entire 8 hour working day – on the same activity. Obviously the degree with which organisation policy is stringent and is implemented has great effect on computer behaviour.

4.4 Prevalence of Pornography in the Workplace

Prior to asking respondents about their perceptions of child pornography and the possible presence of it in their workplaces, it was useful to enquire about their perceptions on 'adult' pornography and its possible presence in their workplaces.

A minority (5%) of all respondents thought pornography to be freely available in their workplace. These respondents sighted lax control, monitoring and restrictions on the part of the organisation and its IT measures as the prime reason for the availability of pornography at their workplace. It is interesting to note that most of the respondents who complained about pornography in the workplace were in middle management positions and skilled operational.

22% of respondents (government and private) had in the past received emails of a pornographic nature. A smaller proportion (13%) reported awareness of incidents of colleagues receiving emails containing pornography. Of the employees receiving pornographic emails, (85%) said they had deleted the offensive email and another 7% reported the matter to senior management. While a disturbing 6% passed the email on.

4.5 Understanding and Prevalence of Child Pornography

In looking at the perceptions of respondents to the issue of child pornography, it must be outlined that for a substantial number respondents, it was the first time they had been asked to engage in such a topic. For this reason, most of their responses tended to have very strong emotional colouring and emanated from their personal values and moral codes.

Levels of general awareness and understanding of the issue of child pornography were not wholly consistent. Only 35% of all respondents were aware of the provisions of the Film and Publication Act of 1996. Most respondents (75%) stated that they were aware of their legal obligation to report incidents of child pornography to the South African Police Service (SAPS), yet as shown below, far fewer respondents were aware of their own organisation's anti-child pornography policy.

Around two thirds (65%-72%) of all respondents could define the concept of child pornography. Nevertheless, the third of respondents that could not define the concept, present a danger to the workplace, as it can be assumed that they would not be able to properly identify child pornographic material if they were to come across it.

4.5.1 Awareness of Anti-Child Pornography Policy at Workplace

40% of all respondents were aware of the existence of an anti-child pornography policy at their workplace. The levels of awareness for government and private sector employees mimicked each other. Junior staff was the least aware of the presence of an anti-child pornography policy – much like their low levels of awareness of general computer usage policies.

As was shown with the general computer use policies, the communication of these policies to employees was pivotal in informing their levels of understanding of how to conduct themselves in the workplace and with organisation resources. 50% of private sector respondents, as opposed to 39% of government department respondents, could recall mention of an anti-child pornography policy in their employment contract.

Levels of verbal communication of anti-child pornography policy in government departments (34%) were also shown to be lower than in the private sector (49%).

Of the respondents who were aware of such a policy, the most commonly identified specification stipulated that any employee found to be viewing, downloading or distributing child pornography would face internal disciplinary action. Employees in the private sector were shown once again to more likely to be immediately dismissed from their jobs than their counterparts in government. Interestingly, from respondents' recollection of policy specification, the reporting for criminal prosecution was the third most mentioned specification by government respondents.

4.5.2 Reported Cases of Child Pornography and Action Taken

Only 3% of all respondents could recall a case of viewing child pornography. Also, only 2% of respondents recalled a case of downloading child pornography.

The recalled incidents of the distribution of child pornography were even lower, at 1%. Also, 1% of respondents could recall an incident that they personally viewed as child pornography – these were mostly the respondents who did not have a handle on the concept of child pornography.

There were no major differences in the number of incidents of child pornography in the workplace mentioned by government department and the private sector respondents. The only difference concerned the manner in which these incidents were dealt with by senior management.

Below is a table showing the varied recalled actions taken against employees who had viewed child pornography at the workplace:

Situation (Viewing)	Total (n=20)	Government (n=13)	Private Sector (n=7)
The person(s) involved were discharged from employment	30%	23%	43%
The person(s) involved were reported for criminal prosecution	25%	31%	14%
The person(s) involved were given a written warning	20%	8%	43%
The person(s) involved were handed some form of punishment but were not discharged	15%	15%	14%
No action was taken against the person(s) involved	15%	23%	-
The person(s) involved were given a verbal warning	10%	15%	-
Not sure/Don't know what action was taken	10%	8%	14%

Government departments appeared to be more proactive and following legislation on child pornography a little better than the private sector. As can be seen government departments tended to use a dual approach to dealing with cases of child pornography by initiating internal disciplinary hearing while also informing external authorities.

4.6 Policies and Measures to Control Child Pornography

4.6.1 Mechanisms to Enforce Policy

The types of mechanisms were very similar in both government departments and the private sector. The most popularly used mechanisms to enforce computer (including email and the Internet) access policy were: installation and maintenance of firewalls/filters, the IT department and personnel monitoring use and selected websites being blocked.

A high proportion (65%) of employees was aware of the fact that most of their electronic and digital correspondence and activity was being monitored. It is interesting to note that 17% of respondents reported that their organisations promoted peer monitoring as an additional safeguard to restrict unwanted information.

As reported by respondents, this method of policy enforcement was used more often by the private sector (21%) than government departments (11%).

As can be seen, a lot of emphasis in enforcing policy was placed on the perceived dangers of the Internet. There was recognition too in Phase I of the important and sometimes highly dangerous role the Internet plays in bringing unwanted content into the workplace.

4.7 Additional Respondent Comments on Child Pornography

Respondents mostly felt that more urgent and decisive action needed to happen in order for more children to be protected. They were vehement that more stringent legal action needed to be enforced. Respondents were very supportive of any legislation that sought to protect children, but also recognised that legislation alone could not fully achieve its intended purpose if not supported and upheld by communities, the media and the police. On the matter of the police, 87% of respondents said they were likely to report any knowledge of colleagues viewing, downloading or distributing child pornography to the SAPS.

Also, substantial proportions of respondents were interested in participating in anti-child pornography workshops and seminars. The most amount of interest was from government department respondents (69%) while 52% of respondents in the private sector were interested. Interest in receiving anti-child pornography information, was even higher, with 83% respondents from government and 70% from the private sector indicating interest. In terms of designations, junior staff showed the most amount of interest in participating in workshops and receiving information.

Section Five: Conclusions and Recommendations

5.1 Conclusions and Recommendations

Respondent answers and the general way in which organisations view child pornography would suggest that legislation does not impinge enough on organisations (particularly in the private sector) to take on the responsibility of creating any computer/Internet/email policy, let alone policy directly aimed at child pornography viewing, downloading and distribution. The following are the key conclusions and recommendations at addressing the issue of child pornography in the workplace.

- Communication between senior management and HR officers in particular was not strong in all organisations. The limited verbal communication of policies is problematic as it could, for those organisations that do have existing anti-child pornography policies, undermine their efficacy.
- In terms of the actual implementation, it appears that mostly it has been the trend that usually it is government departments that take instances of child pornography seriously enough as to involve external authorities by reporting employees involved for criminal prosecution.
- It was felt by respondents that workshops and seminars could be targeted at IT personnel and build on the sometimes limited knowledge employees have on child pornography in order to facilitate better identification of child pornographic content.
- Current legislation would need to be re-examined and amended slightly to pressure organisations (especially in the private sector and those employing large numbers of employees) to include anti-child pornography regulations in organisation policy.
- Policy makers, such as Human Resource (HR) directors/managers in the larger organisations and possible owners and Chief Executives of smaller operations, within the private sector need to be challenged on how their organisations currently and will in future deal with the problem of child pornography in the workplace.

- HR mechanisms and responsibility would also need to be challenged, as anti-child pornography rules and regulations could be encouraged to become a regular inclusion in employment contracts, with any transgressions resulting not only in the termination of employment but also in the reporting of offenders for criminal prosecution.
- A major positive from the survey is that the majority of respondents, especially employees in the private sector, did say that they would be highly likely to report incidents of the viewing, downloading or distribution of child pornography by colleagues.
- The most encouraging aspect of the findings is that of the employees who wish to participate in workshops and receive information that will inform on the anti-child pornography movement, most were junior staff members.
- Certainly, as an immediately feasible target for improvement by the FPB, more employees need to be briefed on child pornography policy.