White Paper

Thinking Outside the "Porn" Box

…separating the sexual content debate from issues relating to marketing, commercial practices and child exploitation

Finding a Workable Solution to Privacy, Security, Consumer Fraud and Child-Exploitation Issues Relating to Adult Websites

Presented by:
WiredSafety.org and its WiredKids division
The World's Largest Online Safety and Help Group
(A 501c-3 corporation, operating through unpaid volunteers worldwide)

Prepared with the assistance of global child advocacy groups and experts, some of whom are identified at the WiredSafety.org website. Given the nature of the topics covered herein, and restrictions on certain groups being able to recommend non-criminal approaches to the online adult sexual content issue, not all groups or experts contributing to the preparation of this White Paper and to the conclusions reached herein are identified.

Contents

Introduction

The Internet has changed the way most of us interface with and think about pornography.[1] It has made it much easier to find when you are seeking it and harder to avoid it when you are not. Before the Internet, people had to reach out to find it, now it reaches out to find you (and your children).

This fact has reinvigorated the debate about access to pornography, especially online. But this debate, like the offline debate before it, is caught in the endless loop of defining the problem, the content and whether, by whom and how it should be accessed. The global nature of the Internet, and the worldwide panoply of laws and jurisdictions, however, unlike the offline one before it, further complicates this debate.

While these debates air important considerations, every day it becomes more essential that something be done – now. It's time to put the endless debates aside to find a solution. More than a million pornographic websites exist today. This is likely only to increase. In addition, many commercially-irresponsible pornography sites are exploiting the absence of effective global regulations to take advantage of their customers and innocent Internet users, including children. While we wait until the overarching debate about pornography itself is resolved, our children remain the targets of unscrupulous pornographic marketing practices. Unless we "think outside of the box" in crafting innovative and immediate solutions, these abuses will continue and escalate.

Many online industries operate under applicable "best practice guidelines" and commercially responsible standards. The online pornography industry has, largely, avoided adopting commercially responsible standards. The credit card companies have long recognized this, and labeled the online pornography industry "high risk" for the amount of fraud and e-commerce abuses existing within that industry.

[1] Recognizing that "pornography" has no clear definition, and, in some variations has been described as something "[you] know when [you] see it", this White Paper will use "pornography" and "adult content" and "sexually explicit content" interchangeably. Rather than attempt to define the term for legal purposes, the authors of this White Paper hope that the readers will "know it when they see it" without the need for further definition. Since the discussion herein avoids the nature of the content itself, the perceived differences in the terms and the political correctness of these terms is irrelevant. When a legal meaning is required, that term will be clearly defined under applicable law. Defining "pornography" and the other terms referenced herein, except when they have specified legal significance, defeats the intent of this White Paper to avoid the traditional debates over sexual content (other than for child pornography (actual and virtual) and sexual exploitation of children).

By encouraging the pornography websites and services to adopt a set of responsible "Best Practices Guidelines" and shun the marketing, privacy and security abuses of others within that industry, everyone benefits. These guidelines would prohibit unscrupulous and abusive marketing practices while requiring better privacy and security practices. This could reduce the amount of unintended exposure to online pornography for those not seeking it (especially our children) at the same time customers of online pornography are protected. Further, some areas of child sexual exploitation (most notably virtual child pornography[2]) can be addressed through contractual and voluntary guidelines when the law alone is often insufficient or nonexistent.[3]

The success of the solutions proposed is premised upon the assumption that the voluntary adoption of best practice guidelines by adult websites is good for business.[4] A unique set of factors makes this an especially good time to promote the adoption of best practice guidelines. The voluntary adoption is fueled by a combination of carrots and sticks, and the application for an .xxx TLD by a company willing to adopt best practice standards.[5] Many jurisdictions are stepping up the enforcement of existing laws and adopting new ones to deal with the perceived problems. Credit card chargebacks, penalties and high fees associated with "high risk" online industries are exacting their toll on the pornographic site operators. Some governmental authorities block, filter and otherwise prevent access to pornographic websites. At the same time, the competition among

[2] Certain jurisdictions have different legal treatment of images which have been virtually compiled or entirely computer-generated differently from those where an actual child is being sexually-molested (even if they appear to be actual images of children being sexually-abused). The images that do not portray an actual child, in a recognizable way, are frequently referred to as "virtual child pornography." Recently, a federal child pornography law was held unconstitutional by the U.S. Supreme Court using this reasoning.

[3] Many believe that the United States still has serious gaps in the laws governing child-exploitation and "virtual" child pornography. The guidelines proposed in this White Paper exceed the legal requirements of most countries, worldwide.

[4] This White Paper does not propose or support mandatory guidelines. Nor does it support a mandatory adult TLD. The success of this model rests on the willingness of an industry that is very difficult to practically control, to control itself and others within that industry. Attempts to make the best practice standards or any TLD mandatory would have the exact opposite of the intended effect. Market influences (which include existing regulatory schemes), not new legal requirements, must guide the migration to any TLD or best practice identifiers. This White Paper proposes that the Internet pornography industry should be self-defining for the purposes discussed herein. If a site or service wants to define itself as a member of the adult industry and reap the benefits of being considered a member of that industry adopting more responsible standards, endless arguments over who and what qualifies are avoided.

[5] ICANN (the entity controlling the creation of "top level domains" (such as .com, .net, .org and in this case .xxx)) has solicited applications for new TLDs. An application has been made by ICM Registry and IFOR (a Canadian non-profit corporation) for the creation of, and right to control, an .xxx top level domain on the Internet for sexually explicit websites and online services. (The application can be viewed at ICANN's website, www.icann.org.)

pornographic websites has increased substantially. The time is ripe for innovation and adoption of industry-wide codes of conduct.

Understanding that they can choose between sites that will protect their privacy and financial information and those that do not, it is assumed that customers will demand better commercial practices from sites they frequent. Therefore, the sites adhering to more responsible standards should succeed in this competitive market, and perhaps also avoid the law enforcement scrutiny given to the sites that engage in consumer fraud, child exploitation and privacy and security abuses. Certain consumer marketing safe harbors may also be available to the sites that avoid targeting children.[6]

Both those who oppose all forms of pornography and those who believe pornography should not ever be regulated will likely find fault in this approach. But much can be gained if we put these traditional stances aside to deal with a growing problem that requires our immediate attention. While the debates continue, our children are bombarded with graphic sexual images while they surf, search and even use offline computer applications with "ever-on" connections.[7]

Thinking "outside the box" requires that we face existing facts and try to tackle the issues that can be dealt with now. Hopefully we can provide an additional margin of protection for those affected by the abuses, at least in the short-term. This White Paper does not propose a final answer or a silver bullet. But it does identify and recommend an important piece of the overall puzzle. When combined with appropriate laws, enforcement of those laws, consumer awareness, education and technology tools, this piece will help enable a meaningful solution.

To work towards a solution to these abuses, we will have to avoid the heated debates centering on pornography itself. But if this can be accomplished, without giving the impression that pornography itself is acceptable (to those who oppose it under all circumstances), or can or should be restricted or criminalized (to those who oppose restrictions on consenting adults' ability to access pornography), everyone wins. It is the intent of this White Paper and those who have joined in its preparation that we do just that. Adopting the measures proposed in

[6] These are not safe harbors from obscenity and similar laws. They are safe harbors under existing laws that shield sites if they can prove they are not marketing to children, by attempting to masquerade as a children's sites, for instance. This is further discussed later in this White Paper.
[7] Pornographic pop-ups can appear when our children are not actively using the Internet as long as the DSL or cable connection is open (which is how most broadband connections are configured).

this White Paper should have no effect on the core debate occurring inside the "box", nor should it give comfort to any side in the debate.[8]

Solutions must be varied, creative and broad to be effective. It will take a combination of law and regulatory enforcement, ISP and hosting company cooperation and the strict oversight of the merchant and financial services to make a difference. It will also take the voluntary adoption of best practice guidelines from the online pornography industry.

Many of these fraudulent and questionable practices are already regulated by governmental agencies around the world. Stepping up enforcement of these existing regulations would help stem their growth. Some of these practices also violate the terms of service of most hosting companies and ISPs. Policing their terms of service and shutting off service to those violating them can be helpful as well. Several of these practices also breach the terms of merchant accounts with credit card and online payment service providers. Closing the merchant accounts of offenders and carefully enforcing the chargeback rules can be very effective. But none of these, even collectively, has had a major impact on these abuses and questionable practices.

But when combined with self-regulation by the more responsible members of the online pornography industry and the adoption of a set of best practice guidelines that ensure commercially responsible marketing practices and privacy and security standards, these other methods become far more effective. And further regulations become less necessary.

If this can be accomplished, "something significant has been done." It's not the silver bullet, but a serious step in the right direction. Market influences, competition and criminal prosecutions of those engaged in fraud and commercial criminal conduct should do the rest. Those willing to adopt responsible commercial practices will survive; the rest, hopefully, will not.

[8] This White Paper is in no way an endorsement of sexually explicit or adult sexual online content. It merely sets the issue aside for the purpose of reaching an agreement on privacy, security, consumer fraud and child exploitation issues which are or should be acceptable to responsible adult site webmasters and website operators. The views of any identified group on sexually explicit content itself must be obtained from them directly, and not assumed from this paper. Many groups that adamantly oppose all pornography, in any form, see a benefit to identifying and encouraging better commercial standards. But they will also continue to fight against pornography itself.

Summary of Conclusions

While we await the "silver bullet" that will allow everyone to control content they view and communications from others online, solutions need to be drawn from existing legal frameworks and innovative approaches. Criminal laws and consumer protection regulations play an important part in any solution to unintended exposure to pornography and to child pornography and other illegal content. Awareness campaigns and educational programs directed at parents and children can be a significant factor in preventing unintended exposure, privacy intrusions and fraud, as well. Parental controls, filtered search engine options and filtering technology to reduce exposure to pornographic sites and SPAM, pop-ups and other unsolicited communications, marketing and advertisements can also be an important tool.

But self-regulation of the adult online industry by the voluntary adoption of a commercially-responsible set of best practice guidelines is a key component of an overall solution to the problems described herein. Most other industries are governed by a self-regulatory or established set of best practice guidelines or codes of conduct. Given how it operates and the animosity many members of the industry feel for others within the industry, it isn't surprising that the Internet pornography industry has so far avoided any self-regulation or industry-accepted codes of conduct.

But, the adoption of best practice guidelines by responsible adult webmasters can provide substantial protections for all stakeholders, especially in the area of privacy, security, crime prevention and fraud. These guidelines should include protections against unsolicited graphic communications, unintended exposure to graphic sexual content, child exploitation and child molestation, financial fraud, and privacy and security violations. Self-regulation can also help prevent and facilitate the reporting of fraud and criminal behavior, such as child pornography and exploitation, re-dialers, phishing and identity theft.

As people learn to demand better choices about if, when and how they access sexually-explicit content or allow unintended pornographic intrusions into their or their child's online activities, the market will select the more responsible sites. Those who adopt the best practices may also be able to benefit from potential safe harbors under certain laws.

Best practice guidelines or industry-adopted codes of conduct are usually adopted with governmental encouragement or when a leader in the industry spearheads the initiative. Unfortunately, there is currently no one leader within the adult industry capable of forming a responsible industry group.[9] This has been one of the obstacles in trying to convince the adult industry to adopt best practices. Yet many within the industry are seeking ways of being identified as safer, more secure and more private than their competitors.[10]

Now is a particularly good time to convince the pornographers of the value of adopting best practices. Stepped up criminal investigations and global prosecutions, the pressure of religious leaders, community groups and parents to enforce existing and adopt new laws, onerous credit card rules that target the online adult industry, and increased competition among online pornography sites and services create serious incentives for change.

At the same time, a leader of sorts has recently emerged. An applicant for the creation of an .xxx space on the Internet and the right to control that space has agreed, in principal, to the adoption of basic best practice guidelines for all .xxx websites. This applicant, created and headed by people not associated with the adult industry, which will run under the oversight of a Canadian non-profit, could be the one entity able to forge a consensus among the members of the adult community. (See Annex B for a statement by this applicant about its intentions.)

This White Paper intentionally does not set out the particular best practice guidelines. This would require negotiation with members of the online pornography industry itself, and with leading stakeholder groups. Rather, the issues which must be addressed, why they must be addressed, and the benefits of addressing them are outlined in detail. The .xxx TLD registry, if approved, or any group willing to spearhead best practices for the online adult industry can use this White Paper as a basis for creation of a code of conduct. The draftsmen of this White Paper wish to point out, however, that "the devil is in the details."

[9] While several attempts have been made by some within that industry to set industry guidelines, none have succeeded. If one particular group is involved, others will not be and vice versa. So, without one trusted leader to make this happen, nothing is accomplished.
[10] Many adult websites have qualified for the privacy seal programs of TRUSTe and BBBOnline. Apparently the seal programs provide a significant value to the adult sites.

Identifying the Problem

For all Internet users:

Open your e-mail box or conduct a search for anything online and you are likely to run into graphic sexual images or content whether you like it or not. And our children are often more likely to be targeted by pornographic images or messages than we are, because of how they communicate online and how easy they are for the marketers to find.

Most Internet users are unhappy about the continued growth of marketing abuses and questionable advertising practices by many members of the pornography industry. What used to be just an annoyance and considered part of the price of using the Internet is now becoming a more serious problem. It is also becoming one that parents increasingly are insisting something be done to address.[11]

When anyone searches for information online, or mistypes or misspells a domain name ("typo-squatting"), they may find themselves at a pornography site.

When they open their e-mail boxes or instant messaging programs they may find themselves targeted by unscrupulous ads including those for "young teens," "preteens" and "little girls or boys" sex (often mere fraudulent advertising), or sites promising child pornography and "lolitas."

When they stumble upon a pornography site, they may find themselves locked in an avalanche of new pornography windows, unable to escape without having to shut down their computers ("mousetrapping").

And sometimes when they type in the URL of their favorite site, they

[11] The pornography marketing complaints received from parents and children themselves by WiredSafety.org and its family of sites has increased substantially over the last several months. From approximately 30 daily complaints from parents/grandparents and teachers about unintended exposure to online pornography, the number has increased to hundreds a day. Sixty-five percent of these same parents/grandparents have indicated that they either support an adult's right to access legal pornography or recognize their legal right to do so. They have also, until now, been unhappy with (but haven't lodged any formal complaints against) the onslaught of online marketing, misleading practices and sexually-graphic images they have encountered. They largely believed that nothing could be done to stop it. That has now changed. Now they are looking for ways to make it stop. More than mere technical tools, they want help, either from their ISPs or the government. They want someone to do something to help prevent their children from being confronted with pornography when searching for innocent sites, playing games and even using their computer in an "always on" environment, when pop-ups will appear on screen unexpectedly.

end up at a pornography site instead, either because traffic for that site had been redirected by a pornography site ("hijacking") or because the siteowner had forgotten to renew their domain name registration ("porn-napping").

As competition among the pornography sites increases, these marketing abuses increase. Unintended exposure is a serious and growing problem. These marketing abuses and questionable practices currently include:

- Child pornography (real and virtual)
- Sexual exploitation of children (including false advertising of child pornography and use of terms implying child pornography, such as "preteens," "little boys" and "lolitas")
- SPAM/SPIM[12]
- Fraudulent headers in promotional e-mails
- Fraudulent or misleading metatags, keywords, descriptions and listings with search engines
- Typo-squatting[13], particularly those intended to attract children
- Misleading domain names or keywords, particularly those intended to attract children
- The use of terms to attract those seeking child pornography
- Intellectual property violations, piracy and counterfeiting
- Browser hijacking/ Mousetrapping
- Slammed home page changes
- Spyware and adware, pop-ups and pop-unders[14]
- Graphic images on the non-subscriber front pages
- Graphic images in unsolicited e-mail and instant messaging links
- Spoofing and phishing practices[15]

[12] "SPIM" is the new name for unsolicited bulk instant messages. "Spam" is the e-mail equivalent (no relation to Hormel's luncheon meat).

[13] When someone, generally a pornographic website operator, registers the common misspellings of a popular site, especially one aimed at children.

[14]"'The websites that attract children and teens in droves are the ones most often targeted by some in the porn industry via pesky pop-up ads… A pop-up is an advertisement that comes up when you first click onto a website… Designed to draw your attention to an aspect of the site you're visiting or to sell you a product or service, most are harmless. But as many parents have discovered a large number of pop-ups include offensive photos of sex acts not suitable for young eyes. To see these hardcore pop-ups you usually have to come across a porn site, says Cathy Wing, director of community programming for Media Awareness Network. `Once you stumble on a porn site or go to one purposely it will trigger these,' she said from her office in Ottawa. Even worse is when sites aimed at teens _ skateboarding, music, video games _ trigger pop-ups with questionable content, Wing said. 'Tons of these sites that teens like to go to will eventually lead them to porn. That's the problem,' she said. 'It's the kind of sites that kids go to that they target.'" The-Cyberfile, Bgt , BY ANGELA PACIENZA, 25 February 2004, The Canadian Press.

[15] Pretending to be another website, often to trick people into providing their financial information and creditcard details for criminal purposes.

- Domain-napping/ Porn-napping[16]
- Criminal re-dialers and similar schemes[17]
- Page-jacking[18]
- Malicious code, criminal intrusions and Trojan horses

To quote so many parents, "something has to be done." And while some of them may support an eventual total ban on all pornography and some others support an unrestricted right for adults to view pornography, all of them support an immediate solution to the issue of unintended exposure.

[16] WiredKids.org's teen site, WiredTeens.com was recently grabbed by a pornographic website operator. It previously pointed to the WiredTeens.org main site. WiredSafety's executive director, cyberlawyer Parry Aftab, is contemplating brining criminal charges unless the site is returned.

[17] "Modem Hijacking: The Commission has used its training and tools to stop some of the most egregious and technically sophisticated schemes seen on the Internet. For example, the FTC's lawsuit against Verity International, Ltd., was prompted by the influx of hundreds of complaints in the last week of September 2000 through the CRC and logged in Consumer Sentinel. Investigation showed that high charges on consumers' phone lines were being initiated by 'dialer' software downloaded from teaser adult web sites. Many line subscribers had no idea why they received bills for these charges. Others discovered that a minor in their household -- or another person who did not have the line subscriber's authorization – accessed the Web sites and downloaded the dialer software. The dialer program allowed users to access the 'videotext' adult content without any means of verifying that the user was the line subscriber, or was authorized by the line subscriber to incur charges on the line for such service. Once downloaded and executed, however, the program actually hijacked the consumer's computer modem by surreptitiously disconnecting the modem from the consumer's local Internet Service Provider, dialing a high-priced international long distance call to Madagascar, and reconnecting the consumer's modem to the Internet from some overseas location, opening at an adult web site. The line subscriber -- the consumer responsible for paying phone charges on the line -- then began incurring charges on his or her phone lines for the remote connection to the Internet at the rate of $3.99 per minute." (Prepared Witness Testimony ,The Committee on Energy and Commerce, W.J. "Billy Tauzin" Chairman, On-line Fraud and Crime: Are Consumers Safe?" Subcommittee on Commerce, Trade, and Consumer Protection , May 23, 2001, Ms. Eileen Harrington, Associate Director of Marketing Practices Bureau of Competition Federal Trade Commission.)

[18] "Pagejacking" and "Mousetrapping": "Earlier, in FTC v. Carlos Pereira d/b/a atariz.com, the Commission attacked a world-wide, high-tech scheme that allegedly 'pagejacked' consumers and then 'mousetrapped' them at adult pornography sites. 'Pagejacking' is making exact copies of someone else's Web page, including the imbedded text that informs search engines about the subject matter of the site. The defendants allegedly made unauthorized copies of 25 million pages from other Web sites, including those of Paine Webber and the Harvard Law Review. The defendants made one change on each copied page that was hidden from view: they inserted a command to 'redirect' any surfer coming to the site to another Web site that contained sexually-explicit, adult-oriented material. Internet surfers searching for subjects as innocuous as 'Oklahoma tornadoes' or 'child car seats' would type those terms into a search engine and the search results would list a variety of related sites, including the bogus, copycat site of the defendants. Surfers assumed from the listings that the defendants' sites contained the information they were seeking and clicked on the listing. The "redirect" command imbedded in the copycat site immediately rerouted the consumer to an adult site hosted by the defendants. Once there, defendants 'mousetrapped' consumers by incapacitating their Internet browser's 'back' and 'close' buttons, so that while they were trying to exit the defendants' site, they were sent to additional adult sites in an unavoidable, seemingly endless loop." (Id.)

For customers of online adult sites and services:

At the same time, many adult customers of online pornography are worried about the security of their credit card and other financial information provided to the pornography sites or adult verification and payment services. They are also concerned about their privacy and whether their personal information is being shared with other sites and services without their consent.

While these issues relate to e-commerce generally, they have special significance when pornography is involved. Many people are uncomfortable admitting that they are consumers of pornography. They are more reluctant to protect their rights if it means identifying themselves as porn users. In some cases, they cannot find the contact information, or even the identity, of the site operators when they have complaints or need to reach someone.

Therefore, to find sites that are more trustworthy, and to be able to protect one's rights, becomes more complicated.

These issues include, in addition to some of those above:

- Fraudulent credit card and financial practices
- Dispute and complaint resolution processes
- Customer privacy and security violations

For them too, "something needs to be done."

Trying to Reach Consensus

The Challenge of Addressing Issues Impacting Pornography and the Adult Industry

While most agree that something needs to be done, it is not easy to do so. Few issues elicit as much legal, political and moral debate as sexually-explicit content. Charged with the passionate and inconsistent viewpoints of the religious, ethical, legal, child protection and civil rights communities, it isn't surprising that significant inroads have not been reached in curbing commercial abuses relating to pornography online.

It is the sexual content itself that obstructs, with the battles being fought over what constitutes pornography and whether (and/or under what circumstances) pornographic sites should be accessible. Yet while those battles are raging, pornographic content remains readily available, while the commercial abuses are becoming more and more pervasive.

By separating the nature of the sexual content (and related violent and exploitation issues, other than child exploitation issues) from the commercial and marketing abuses and questionable practices that have recently exploded online, most of these communities can reach a broad consensus that addresses inadvertent exposure, fraud, privacy, child exploitation and inadequate security practices, while leaving battles concerning content to another day.[19]

As tempting as it may be to merely condemn pornography and refuse to address anything that involves the adult industry, the potential upside to children is too important to ignore. It is essential that we focus on the benefits to children, innocent Internet users and customers of legal sexual content. It is inevitable that some may focus instead on any benefits to members of the pornography industry. Although this proposal only benefits those that voluntarily refuse to engage in child exploitation and adopt more responsible marketing and commercial practices, some groups may feel so strongly about pornography that they will oppose any plan that could be seen as helping pornographers.

Unfortunately, this proposal only works if the pornographers

[19] Some groups, most notably certain religious groups, have refused to support anything that benefits pornographers in any way, even if children benefit more. While the drafters of this White Paper understand their position and respect it (and in many cases support it), it is hoped that the drafters' desire to "do something" is equally understood and respected.

voluntarily adopt the best practice guidelines recommended herein. It is unlikely that they will do this unless they see a potential benefit in doing so. This is a classic catch-22 situation unless you put the children's interests first. If you do that, all else falls into place.

Understanding Online Pornography

According to recent studies[20], there are approximately one million commercial adult websites worldwide. Many of these are controlled directly or, through affiliate programs, indirectly by a much smaller group of website operators, some of which control thousands of websites.[21] Although a relatively small percentage of the global community of websites, pornography sites comprise a large percentage of online revenue and traffic.[22]

The majority of traffic to the online pornography sites is from the US, UK and Germany.[23] See chart from the Reuters' Study (published in 2001) regarding the country sources of online adult content revenues (redacted to reflect only years 2001 – 2004):

Table 3.4: Global Online Adult Content Revenues, [2001-2004] (US$m)

Country	**2001**	**2002**	**2003**	**2004**
US	1858	2190	2437	2602
UK	164.7	216.5	289.4	351.5
Germany	85.7	108.3	150.5	187.0

[20] Others have estimated that this number may be as high as 2 million sites.

[21] According to a Reuter's study issued in [2001], "The majority of the revenues from the online adult content sector are generated by a small number of US companies, each operating huge numbers of websites. For example, VS Media reportedly owns 20,000 webmasters, each operating around four or five websites." Some estimate that for every website, there are 15-20 different URLs pointing to it. That is one of the reasons statistics regarding online pornographic sites are so unreliable.

[22] "The online adult entertainment industry generated $2.5 billion globally in 2001; this figure is expected to reach $4.6 billion by 2006. Adult content sites account for just 1.5% of all sites on the Internet. In 2001, around 66% of all online content revenues were generated through adult content. 59.2% of US adult online content revenue was generated through advertising and merchandising in the US in 2001; the rest was via subscriptions." (Reuter's Study, p. 24)

[23] "The US, the UK and Germany are by far the three largest online adult entertainment markets, accounting for 86% of the overall industry in 2001. Online adult entertainment revenues in these three countries were $2.1 billion in 2001; this figure is expected to reach $3.8 billion by 2006, representing an 81% increase over the period." (Reuter's Study, p 25).

Rest of World	351.60	385.20	443.10	544.70
TOTAL	**2,460.00**	**2,900.00**	**3,320.00**	**3,685.20**

Source: Datamonitor Reuters Business Insight, p.25

How Do The Pornography Sites Make Money?

The online adult community is comprised of several large enterprises and many more smaller ones. The larger enterprises typically develop content which is displayed on the smaller sites and operate on a subscription model. The adult sites work together to share traffic, with many smaller sites being paid to refer traffic to the larger ones to generate subscriptions. Large adult verification and payment sites also receive traffic from the smaller pornography sites and pay referral fees for any subscriptions generated.

No online industry is as successful and as sophisticated as the online adult industry in monetizing all activities online.[24]

Many referrals are delivered through the use of banner advertisements that, when clicked, refer the viewer to another site. Fees are paid to the referring site for eyeballs (everyone visiting the page, even inadvertently), for click-throughs (when the banner is clicked upon and the viewer referred to the page being promoted) and for eventual subscriptions and paid services.[25] When possible, profiles are tracked and online behavior is studied to improve the marketing and promotional practices and find new sources of revenue in tracking consumer behavior, preferences and patterns.[26]

Each of these mechanisms involves complicated rules for how much and when the referral and promotion fees are earned. But even

[24] According to the Reuters' study in 2001, "[re]venues can be generated from a number of sources including paid subscriptions to the site, advertisements carried on the site, sending traffic to other sites, sale of sex-related products, and providing auxiliary services such as adult content search engines, content for other adult website operators, or age verification services." (Reuters' study, p.26).

[25] Any visit to the site (even inadvertently by children) generates a CPM payment ("cost per mille" standing for 1000 site visits, no matter how short the visit is for). A click-through generates a CPC payment ("cost per click"). Eventual subscriptions, purchases and other revenues derived from the advertisement generate a CPA ("cost per acquisition") payment. Obviously CPMs earn the least per instance, while CPAs earn the most.

[26] "The adult sites also expertly monitor and filter traffic, building demographic profiles of customers to target ads specifically to users. 'You don't try to sell a lawnmower during "Oprah,"' explains Andrew Edmond, chief executive officer of SexTracker, a Seattle- based service company that hosts porn sites and markets statistical analysis tools." SEX-DOOR NEIGHBORS WEB PORN BIZ FINDS NICHE IN SUBURBIA, Patti Hartigan, 2 June 2000, The Boston Globe.

inadvertent viewing (by children, for example) will often earn a site advertising revenues.

Given the slowing growth of Internet adoption (as more and more people join the online community), competition among the pornography sites is increasing. Without being able to count on the growing number of users, it must now compete for the existing Internet users.[27] According to the Reuters' study, the methods used online to increase revenue include:

- Sending unsolicited e-mail ("spam") that advertises the site[28]
- Placing advertisements for the site on other websites
- Paying search engine companies for more prominent placement in their
- search engine's results
- Acquiring domain names with sexually oriented words in them
- Acquiring domain names based on common misspellings of non-sexual
- website addresses
- Acquiring expired domain names that have acquired some reputation for generating traffic
- Paying other websites to obtain their exit traffic (also known as mousetrapping)
- Mailing list subscriptions (for which a user must make an explicit "opt-in" choice)

(Reuters' Study, p.28)

With the exception of opt-in mailing lists (which this White Paper recommends) and truthful advertising and search engine placements, these methods exactly track the abuses this White Paper is trying to address. What is seen as essential marketing practices by the online adult industry is considered an abuse or questionable marketing practices by Internet users and, in many cases, regulatory agencies.

How Do Some Pornography Websites Misuse Marketing Practices?

[27] "Since the pool of customers is no longer rapidly increasing, competition within the online adult entertainment industry will grow and the market is expected to get tougher over the next five to ten years. As a result, structured strategies for customer attraction and retention will become more and more necessary." (Reuters' study, p 22).

[28] "Some estimates say email traffic now is running at more than 40 billion messages a day, of which more than one-third is spam, most of it pitches for sex sites. Email is a principal tool used by pornographers to attract paying customers. They buy lists of addresses from email 'skimmers' or use software to generate random addresses. They invade poorly protected corporate networks and steal bandwidth by using their open relay systems to blast the internet with millions of messages inviting recipients to 'click here' for access to their sites - all for a small fee and your credit card details. Although the response to such advertising is only about 0.1 per cent, that is enough to generate more than [Australian]$2 billion a year, according to banking experts." *Downloading porn out of the home*, by Garry Barker, 6 March 2003, The Age.

Many adult sites misrepresent their content or the nature of their website by registering domain names that are intentionally confusing, use webpage coding designed to mislead search engines, distribute false advertising to promote site traffic or hijack website visitors from another site.

Few Internet users have escaped one of these schemes. They are among the top complaints of Internet users, worldwide. These issues are particularly compelling when children are implicated. They are the biggest source of unintended exposure to sexually explicit images and content.

Even when children try to avoid online adult content, it may confront them involuntarily, or they may inadvertently stumble on it. This happens, among other ways, when they receive SPAM or unsolicited instant messages with graphic sexual images, content or links to pornographic sites. Many of these masquerade as a message from someone they know, or as a promotion from a trusted brand or website.

Children may also be tricked into visiting an adult site when they search for age-appropriate words or phrases on a search engine. Many pornographic sites come up in the most innocent search, having misrepresented their content or subject matter to the search engines, or at the top of any search results (using special codes and methods to do so). Or children may misspell the name of their favorite site and find themselves directed to a pornographic site that uses typical misspellings and typos to attract children to their sites, without their knowledge.

These same practices are also used to attract unwitting adults to their sites (the adult web site operators may not care whether the hit is an adult or a child, since they are indistinguishable online), when obvious misspellings of popular website names are registered by the adult website operators and redirected to their site, or search engines are deceived into miscategorizing their sites as something other than sexually-explicit.

Why Do Adult Sites Use These Tactics When Children are Unable to Purchase Their Services?

While it makes sense that since children do not have the ability to purchase commercial online adult services the adult webmasters would try to avoid them, this is surprisingly largely untrue. Remember, the name of the game is "site traffic" when adult sites are concerned. So they can't rely just on keywords to direct traffic to their sites.

According to a recent report by The US National Academy of Science, Computer Science and Telecommunications Board ("CSTB"), Youth, Pornography and the Internet ("CSTB Report"), increased competition means adult websites are resorting to more aggressive marketing techniques, which include targeting children as well as adults. Citing a 2002 Nielsen/Net Ratings report, approximately 16% of the visitors to adult websites in February 2002 were under the age of 18.

One source who testified before the CSTB was quoted as saying that 20–30% of traffic directed at adult sites is comprised of children (see CSTB Report, p.78). Depending on the type of marketing/advertising model used by a particular site, there may be no incentive to filter out children. In fact, targeting children may be an effective way of increasing advertising revenue for a site.

How else can they increase traffic at a site? According to the CSTB Report (chart 3.1) the online methods for increasing traffic to an adult website include:

- Sending SPAM advertising the website
- Advertising on other websites
- Paying search engines for more prominent placement in search results
- Using domain names which include sexually-explicit terms
- Using domain names with commonly misspelled words
- Acquiring expired domain names with established traffic
- Paying for exit traffic from other sites (mousetrapping)

All but the use of domain names with sexually-explicit terms on this list and legitimate advertising links at other adult sites come at the cost of inadvertent child and adult access to sexually-explicit content online.

Why Would Adult Webmasters and Site Operators Adopt Voluntary Best Practices?

This White Paper would be an extraordinary waste of time if the adult webmasters and site operators were unwilling to adopt best practice guidelines. It is not being proposed or intended that the adult sites be forced to adopt the guidelines or acquire .xxx domain names. But the nature of the adult industry, and the pressures of expected upcoming prosecutions for publishing illegal sexual content, may provide an incentive for the more responsible sites to adopt the guidelines voluntarily and, if necessary, acquire .xxx domain names.

In order to understand the incentives, it is important to understand the status and viewpoint of online adult industry webmasters and site operators. There are generally three categories within the adult online industry:

- *Those who are more responsible* e-commerce providers (and just happen to be providing sexually-explicit materials). These include the more famous names and brands within the industry, such as Penthouse;
- *Those who engage in questionable marketing practices* (such as sexually graphic popups, SPAM, and using misleading domain names and descriptors), mousetrapping (where new adult site windows continue to pop up - and then this activity cannot be stopped without shutting down the computer itself) and do not provide adequate security for or protection of their customers' financial and personal data (the largest number of websites probably falls into this category); and
- *Those who engage in, among other things, abusive and fraudulent practices* and criminal conduct such as identity theft, slamming and re-dialers, intentional misuse of financial information, and malicious code (spyware, hijacking web browser settings, Trojan horses, etc.).

It is likely that those in the first group will find many, if not all, of the White Paper recommendations acceptable. Many already follow similar self-established guidelines. But currently these site operators neither derive any credit for their more responsible practices nor can they even be distinguished from members of the other two groups. They are unable to credibly market themselves as belonging among the safer and more responsible of the adult sites, since they lack any kind of third party "seal of approval" or framework.[29] A formalized set of guidelines that identify those in compliance with those standards would change that.

For others, adopting a best practices code of conduct that protects not just children but the online community as a whole, clearly separates the pornographers with more responsible practices from the rest. This may encourage those who fall into the second group, and are often found to use misleading and questionable marketing practices, to clean up their commercial act.

Once a way to brand a site as more commercially responsible is developed (arguably pursuant to the recommendations in this White Paper) marketing *that*, rather than (for example) sending unsolicited and sexually graphic SPAM, will be good for their business. The

[29] Many subscribe to privacy seal programs, such as TRUSTe and BBBOnline. But currently neither provides the breadth of coverage of these proposed best practice guidelines.

validity of this assumption is confirmed by the number of adult websites already qualifying for and subscribing to privacy seal programs, such as TRUSTe and BBBOnline. It is clear that the more responsible adult website purveyors want to be seen as trustworthy e-commerce providers. Adopting a broad set of best practice guidelines is the way to do that.

During heightened competition for existing adult content consumers, promising privacy and security, a possible reduced likelihood that the site's practices will result in financial abuses criminal investigations (thereby exposing their customers' identities to third parties), and responsible business practices can make a big difference. How many consumers are willing to put their privacy and financial security at risk when other sites, just as legally erotic, offer better protection?

The time is ripe for someone to take the lead in creating these guidelines and communicating those to the adult industry for consideration and adoption. Arguably, that entity may have to come from outside the adult commercial community (although they would need to be knowledgeable about the adult industry and have the industry's cooperation and input).

The CSTB Report recognized that many of the more responsible adult website operators wanted to establish thresholds on commercial abuses, such as stolen or illegal content, fraudulent or deceptive practices and improper credit card transactions. The same report, however, noted that there is no core of the adult community that could lead on any meaningful self-regulatory or best practices movement. A potential benefit of any .xxx TLD application is to provide that core; the place where adult webmasters could work together to benefit themselves, the online community (children and adults) and their customers, by adopting acceptable best practice guidelines as a condition of their .xxx domain name registration.[30]

The Carrots

The incentives for the pornographers to adopt these practices fall into several categories. They cover customer service and trust incentives. They also include financial incentives relating to potentially reduced credit card transaction fees, penalties, chargeback practices and reporting requirements. The possibility that pornographers which adhere to commercially responsible practices being able to access the

[30] Many groups, experts and industries have been consulted in the preparation of this White Paper. Some have cautioned that although there is a benefit to be gained in the adoption of best practices, an .xxx TLD that incorporates certain of these best practices is not a complete solution. It is only one, albeit important, tool in the toolbelt of child protection and online safety, privacy and security.

financial markets is enhanced as well. And safe harbors under certain laws relating to marketing practices and availability of their content to children may be available. Being able to attract better and more loyal customers, savings on credit card fees, being less vulnerable to bad faith chargeback claims and reducing the risk of regulatory and criminal enforcement for their marketing, privacy and security practices are powerful incentives to the adult industry.

Currently, most pornography sits require a credit or debit card to access. Some may instead require a membership in an adult verification service, which in turn requires a credit or debit card, or some verified financial account. Yet, most adult sites do not disclose offline contact information, the name of the billing entity or content provider. Customers often cannot tell the difference between commercially responsible websites and those designed to defraud their customers, sell their personal information and steal their financial identities. This, arguably, has kept some potential customers from using online adult services entirely. It has also kept others from trusting their financial and personal information to non-brand name sites. Arguably, the more financially-secure the customer, the more important these issues become.

Providing better privacy and more secure services for their customers should promote more pornography customers to their sites. When customers can choose (and tell the difference) between the sites that offer privacy and security protections and those that don’t (and even worse, intentionally share financial and other personal information with others), they are likely to choose better protection. The more frequently these customers access pornography, the more important these protections become. So, frequent and financially-capable customers are likely to respond to these “more responsible” pornographic websites. Marketing this will be an important factor in developing the “more responsible and trustworthy” branding of these sites.

Dispute resolution processes are an important incentive as well. Currently few adult sites provide offline contact information or mechanisms for reporting customer service problems and billing disputes. If a customer is double-billed or didn’t receive the services for which he or she was charged, their only current option is to dispute the charge with their credit card company or payment intermediary. Rather than being able to resolve the matter from a customer service perspective, the site is now faced with onerous chargebacks from their credit card providers. They have not only lost a customer, they have now lost the payment for services they may have legitimately rendered.

By providing a process and an intermediary to help resolve disputes without having to get the credit card and payment service companies involved, everyone is better served. This too should help direct customers to the sites willing to adopt better commercial practices that include dispute resolution and customer service processes.

Pornography sites have a serious problem collecting on credit card charges. The credit card companies and payment intermediaries have been reluctant to work with the adult industry online.[31] They have learned that the amount of fraud and contested charges involved with the adult industry online is twice that of the more traditional e-commerce industries. In some cases (most notably American Express[32] and Paypal), they have refused to allow their payment services or their credit cards to be used at adult websites and services.

Members of the credit card and payment service industries may, however, revisit their positions and special considerations may be made for sites that adopt stringent and commercially responsible privacy and financial security practices. This could eventually lead to reductions in the high costs, penalties and onerous rules impacting the adult industry for those adopting these best practices.[33]

Finally, at least one financial writer has recommended investing in securities issued by adult content online operators. In "Stocking up on Sin: How to Crush the Market with Vice-based Investing," Caroline Waxler recommends buying equity stocks of the adult online companies.[34] (There are several already listed on the Australia

[31] Visa put special rules into effect in November 2002 designed to reduce fraud and chargebacks. Under these new rules the websites must supply their correct corporate name, address, domain names, and merchant identification numbers. They have to also identify their principals. "Visa says that the rules, targeted specifically at adult-content Web sites, are … a way to make sure that all transactions on Visa cards are legal and traceable. Visa will continue to permit transactions involving Web-based pornography sites, as long as the sites are legal -- for example, they do not involve child pornography, and the customers are adults." *Visa, MC Tighten Their Internet Merchant Rules*, by David Breitkopf, 22 November 2002, American Banker.

[32]" Online sex is the only industry where American Express has adopted a blanket ban on card use, said AmEx spokeswoman Joanne Fisher, and it did so because of 'what we consider an unacceptably high number of customer disputes.' *INTERNET PORNOGRAPHY CAUSES PROBLEMS FOR CREDIT CARD ISSUERS,* Mary Deibel Scripps, Howard News Service, 17 September 2000, Dayton Daily News .

[33] "In November 2002 Visa USA said that such high risk merchants must register directly with Visa rather than using third parties for billing. PayPal has subsequently said that it has stopped processing payments for online pornography, and stops processing sex related products on 12 June [2003]." *More lawsuits for Visa and MasterCard*, 22 May 2003, Cards International, By Tony Morbin.

[34] The Globe and Mail, Report on Business: Globe Investor Securities, Tired of ethical investing? Profit from vice instead; Writer provides guidance on defensive portfolio of sin

financial exchanges.)

Most adult industry members have been closed out of the financial markets due to perceived irregularities and the unreliability of the industry as a whole, as well as the risk of criminal liability for illegal content and activities. Those adopting more stringent financial and security standards are more likely candidates for the public financial market opportunities. This provides an additional incentive for compliance.

The Sticks

An additional incentive to acting now to adopt best practices is fear of criminal prosecution and consumer protection enforcement actions. The regulators and prosecutors in many countries have recently "turned up the heat" on the online adult community. Recently the U.S. Department of Justice has reorganized how and by whom obscenity cases will be handled within the FBI and appointed a well-known and very effective federal prosecutor to address online obscenity criminal prosecutions.[35]

Laws have been adopted holding website operators criminally liable for misleading children to their sites. The U.S. Attorney for the Southern District of New York (Manhattan's federal prosecutor) charged a famous typosquatter with criminal typosquatting, who pleaded guilty to the charges in December, 2003 and was recently sentenced to 2-1/2 years in prison. The potential to create a safe harbor exists for those adopting either an .xxx address or other identifiers which identify them as adult, rather than children's, content. There is a possibility of using the best practice identifiers or .xxx TLD to establish safe harbors in other laws around the world as well.

The UK has recently denounced violent sexual content online. And a joint task force has just been established between the UK and the US to address this. It is expected that this interest in stopping what is seen as criminal or fraudulent behavior will only grow. Italy has adopted criminal SPAM laws, as has at least one state in the United States.

Given what we have heard while researching this White Paper, this is only expected to increase. As more and more of the general population are confronted with what they consider offensive and often unintended sexual images, they are demanding that something be done to stop it.

stocks that she believes will hold up, Carolyn Leitch, 20 March 2004.

[35] *DOJ returns attention to policing the porn industry*, Vanessa Blum , 11 March 2004, **The Recorder**.

Given the "stick" being provided by law enforcement in the United States and other countries around the world, the "carrot" is even more attractive. It is expected that those adult sites that voluntarily submit to the best practice standards will likely be seen by the law enforcement community, financial markets, regulators, advocacy groups and consumers as more trustworthy and safer for e-commerce. That immediately benefits their bottom-line.

Singapore and Looking Forward

Sometimes the stick and the carrot can be combined, encouraging best practices under existing legal frameworks and safe harbors. In Singapore, Internet content is regulated by the Media Development Authority who has adopted a pragmatic combination of regulations (through a class licensing regime) and policies which encourage industry self-regulation and public education.

Currently 100 adult websites are blocked for viewing in Singapore. These sites are not identified, except when someone accidentally tries to access that site. Then a notice appears explaining that the site is blocked and why. This symbolic blocking is meant as a statement of Singapore's value system.

Understanding that pornography online is a fact, and recognizing the need for addressing inadvertent exposure, especially for children, the Media Development Authority see the adoption of a best practices standard by more responsible members of the adult industry as another piece of the puzzle. The Media Development Authority encourages and supports industry self regulation efforts and has indicated that it will take into account this development in determining the 100 sites they block.

Obviously the best practice standards must address the issues reflected in this White Paper to qualify for such considerations. But this is a first, but very powerful, step in trying to separate the adult sites that adhere to responsible commercial practices and a code which prohibits child sexual exploitation from the rest.

The challenges the adult industry faces, given the widely diverse censorship laws and criminal prosecutions, payment intermediaries and charge-backs, intellectual property infringements, fraud and the criminal behavior of some of the less responsible members of the industry, can be largely addressed by the voluntary adoption of this best practice model. Those within the guidelines will be considered the more responsible members of the adult industry, while those without will be more suspect. The upside of that to the adult website operators and webmasters is clear - a reduced likelihood of being targeted by law enforcement (other than on content laws), and a better ability to attract paying customers, collect on their charges and operate in the more traditional business community.

Attempts to Regulate and Control Pornography Online

Since the Web was launched, governmental agencies and organizations

(GOs) and non-governmental organizations (NGOs) from around the world have tried to regulate, criminalize, filter and shutdown online sexually-explicit content and services. They have also often sought to apply offline standards to the online medium with increasingly limited success.

The regulatory schemes vary widely from jurisdiction to jurisdiction. They include holding ISPs responsible for certain pornographic content which they fail to filter , blocking a specific but undisclosed list of pornographic sites , attempting to block all pornographic content, and applying offline standards to the online content. These efforts are largely unsuccessful. Unfortunately, the regulatory framework has also, uniformly, failed to control the marketing practices and financial abuses often associated with certain members of the online adult industry.

Global Access Means Finding a Global Solution

The regulatory schemes, cultural and societal differences as well as the nature of the Internet itself, prevent a unified global standard or approach to dealing with adult content online. The Internet was designed to avoid obstructions. Censorship and many national laws are merely seen as forms of obstruction and the Internet routes around them. That’s why anything short of a unified approach is likely to fail online.

Remembering that the Internet isn’t owned or controlled by anyone, and doesn’t exist in real space is difficult, especially to those trying to regulate the Internet. Regulatory schemes are largely ineffective when it comes to controlling the entire Internet. Because it is global, in order to control what is accessible on the Internet, the Internet would have to be regulated globally. That involves setting global standards and being able to enforce the laws on a worldwide basis.

This is unlikely to ever occur when adult content is involved. There are simply too many values, standards, viewpoints and existing regulatory schemes to permit a common understanding on what should or shouldn't be regulated, how and by whom.

With a global perspective, individual countries are unable to impose their standards on the rest of the world. By limiting the need for additional governmental regulations, voluntary best practice guidelines avoid conflicting standards and governmental controls. They are capable of being enforced as contractual obligations by consent of the adopters.

And by addressing many of the most commonly recognized abuses of some members of the adult industry, the pressure felt by governmental regulators and legislators is reduced. The more the industry polices itself, the less the government will be required to step in. Everyone wins.

The .XXX TLD

Its Potential Role in Promoting Best Practices in the Adult Online Community

Undoubtedly, the easiest way of administering and enforcing best practices would be through the formal TLD registry mechanism. ICANN application processes require that the TLD applicant demonstrate, among other things, that the interests of the identified stakeholder groups are addressed. This includes the Internet community as a whole. At least one applicant for an .xxx sponsored TLD has identified many of these issues as core to their application. They also have indicated that the diverse stakeholders' viewpoints will be represented through the corporate governance of the NGO registry. (See description of ICM's intentions, attached as Annex B.)

Best practice recommendations for the adult community have been proposed informally for many years. This White Paper was first conceived in 1999, following the appointment by one of its drafters by UNESCO to help combat child pornography and online paedophilia. But the challenge of getting the recommendations adopted by the adult industry, or even identifying those capable of leading within the adult industry, proved too difficult and it was abandoned. The fact that an application to ICANN for an .xxx TLD has been made provides a unique opportunity for these views to be shared in a meaningful way. Therefore, it has been updated and the advice of other online safety and child protection groups and experts from around the world has been sought. The applicant for the .xxx TLD has requested that these recommendations be formalized, and will recommend that its NGO board seriously consider all or some of these recommended guidelines as their TLD terms of service.

Since ICANN requires that a sponsored TLD address the needs of its constituency as well as the Internet community at large, a.xxx registry applicant should adopt a set of best practice guidelines, along the lines of some of those proposed in this White Paper, to accomplish that goal. In order to incorporate the stakeholders' concerns, the registry applicant has agreed to include representatives from the child, privacy, security and civil rights advocacy communities, as well as adult webmasters and those within the adult industry in its decision-making processes.

The credibility of a TLD registry that is seen as independent from the adult community (although sensitive to its needs), can deliver improved adult commercial and good netizenship standards most effectively. A well-constituted oversight board could allow for a broad consensus on policies that meet the needs of all stakeholders, including the adult industry members. An independent registry is uniquely positioned to accomplish those goals.

However, this White Paper is not solely reliant on any form of .xxx TLD adoption. While an .xxx voluntary TLD would make this much easier to accomplish, and for those responsible to confirm compliance with the guidelines, the benefit of best practice guidelines is not limited to an .xxx TLD. It is feasible to develop a seal program that would identify those among the more responsible adult sites, protecting privacy, security and the general Internet community, while providing sexually-explicit content to consenting adults. [36]

It should be noted, however, that without the generally perceived value of an .xxx TLD, and the oversight and structure of an .xxx TLD registry, it would be a much harder sell. It is unlikely that a responsible adult "seal" would have the perceived value of an .xxx structure, in setting those who adopt best practices apart from the rest. It would also be very difficult to monetize any structure other than a TLD. The marketing costs of establishing trust in the TLD are more than compensated with the income derived from the sale and maintenance of domain names and related services. In addition, a self-regulated seal program might always be suspect without an oversight structure, such as the registry, which would have to answer for failure to enforce its policies.

Conclusion

There is no "silver bullet" solution. But something needs to be done, now. The time has come to address the enormous problem of inadvertent exposure to pornography, abusive marketing practices and fraud. By combining the voluntary adoption of a code of best practices with carefully-crafted and enforceable laws, enforcement of those laws, awareness and educational programs, parental controls and technology tools we have addressed the problem. Although the problems may not be completely solved, they will be improved.

Failure to address the problem because we hope it will go away, or someone else will do it, or because we fear the depth of the challenge cannot be condoned any longer. This problem will require creative minds and expertise. It will take the active involvement of all

[36] One author of this White Paper has recommended a structure for a permanent council to be created to oversee any seal program in the event an .xxx TLD is not approved. That structure appears as Annex C hereto.

stakeholders. Spotting the issues, and framing the abuses are far easier than forging the solutions. Balancing the rights of children and others to be free from marketing abuses, fraud and misrepresentation with the rights of consenting adults to access and consume legal sexually-explicit content isn't easy. And this is further complicated by disparate worldwide legal systems, values and societies.

Attempts to censor content have failed. These failures can be attributed, *inter alia*, to unenforceable or faultily-crafted laws, the magnitude of the problem, the limits of law enforcement and regulatory agencies, the nature of the Internet and the demand for the content itself. Rather than propose another method to impose censorship or restrictions that may not be enforceable or may not be upheld, this White Paper seeks a contractual agreement among those in the online pornography industry.

Additional Best Practice Components:

Voluntarily Listing with Filtering Tools, Labeling and Rating Services

Assuming the members of the responsible adult industry are serious about not wanting children inadvertently exposed to, or being able to access, graphic sexual images, they can easily cooperate with ratings groups, classification technologies and parental control tool providers to help parents filter sexually explicit sites and content.[37] While not essential to the best practice guideline goals, making a list of adult sites available to the filtering and rating services means fewer innocent sites will be inadvertently blocked.

It is important that we do not confuse voluntary ratings and notifying the filtering companies that the content at the adult site is inappropriate for children with censorship.[38] Many child advocates have been amazed at the level of controversy wrought over the issue of parents using filtering products to help enforce their online choices for their children.[39] But putting control over what children may or may

[37] A few years ago, parents had two choices when it came to using technology to help control their children's surfing. They could use a filtering/blocking software, or they could unplug their computers. But all that has changed. Over the last couple of years, many new and innovative products and services have been developed to expand parents' online safety tech-arsenal. There are now many multi-featured filtering and blocking products. All of their features can be engaged, or just whichever ones match the family's (or child-by-child) needs. There are products that monitor your children's surfing and everything they say and do online, then give you a blow-by-blow account or generalized report. Other products give your children their own customized child-friendly desktop, which can also filter Internet access and restrict certain activities, like e-mail. There are even products for home use that use smart cards to permit or limit access, child by child.

[38] Civil rights advocates worry that classification of sites, either in a list or in a specified TLD, puts the adult content providers at risk that the entire list or TLD will be blocked. While these are important concerns, the drafters of this White Paper believe that the risks are overblown.

[39] The arguments that are usually raised against filtering in the home are:

- The products overblock by blocking "innocent" sites.
- The products underblock, by letting certain sites through that ought to be blocked.
- Children should be taught how to handle inappropriate information, not be fitted with "blinders."
- Parents rely too heavily on these products and fail to take other precautions, thinking that these are the single solution.
- The people who select the filtering criteria have biases that are reflected in their
- selection.
- These biases may not be clear to those using the product or service.
- The people who select the sites for blocking are untrained or unsupervised, and may not perform their jobs properly.
- Certain content, like information about parental drug or alcohol abuse, or incest, should be freely available to children without their parents' knowing that it is being accessed by the child.
- Kids can get around the software easily.
- Children should have unlimited access to all legal information — they have free speech rights, too.

not view online into parent's hands is the right choice.

Teaching parents how and when to use these products, and not to rely entirely on technology to protect their children online, is time well spent. Time is even better spent teaching children ways to avoid all kinds of inappropriate content and communications online.

It has also been suggested that a parental control "lite" can be developed to provide parents with basic features without charge.

Reserving Advocacy Names and Child Protection Names

During a meeting conducted at the House of Lords, a member of a children's charity suggested that the names and brands of child protection groups be reserved, so that they could not be used by anyone within the .xxx space. Stuart Lawley, Chairman of the .xxx TLD applicant agreed and promised to address it when the policies are set by the non-profit board of directors should the TLD be approved.

Cooperation with Tiplines, Hotlines and Law Enforcement

Any group overseeing the best practice guidelines compliance will have to work closely with law enforcement or hotline organizations. While the group overseeing the code of conduct may be unwilling or unable to police compliance, a complaint drive model can be very successful in spotting and reporting violations. Once any violations are identified to the entity overseeing code compliance, action can be taken. When child pornography or commercial fraud (such as identity theft, phishing and spoofing) is involved, in addition immediately shutting down the offending site, complaints can be quickly turned over to the applicable tipline, hotline or law enforcement (or regulatory) agency.

- Once we allow any kind of filtering, we risk starting down the "slippery slope" that leads to governmental censorship.
- Any rating or categorization of content is restrictive and can lead to censorship and generalizations on content selection.

Most of these are effectively addressed by voluntary submission of adult sites to filtering and rating services.

Annex A

The Abuses The Best Practice Guidelines are Designed to Control

This Annex discusses, in detail, the various abuses currently associated with adult websites. The proposed Best Practice Guidelines would require that any website adhering to the Guidelines refrain from engaging in these practices. Additional technological developments are expected to continue to be used by unscrupulous marketers, especially those in the pornography industry. It is intended that this is only a summary of existing abuses, and not an exclusive list of practices that should be avoided.

Mechanisms used by many adult sexually-explicit websites to mislead children and others online.

Some of these practices are already regulated under the consumer protection, intellectual property, and advertising and fraud laws. Others may also violate certain child protection criminal laws (such as the U.S. typo-squatting law) or civil or criminal SPAM laws (such as Italy's anti-spam criminal code).

These practices are not accidental. They require that the webmaster or site operator codes the site with hidden descriptor terms and phrases, lists the site with a search engine, or registers a typo-squatting domain name or a popular brand name, in order to misdirect Internet users. Some also promote their sites using unsolicited bulk e-mails and instant messages with misappropriated or falsified e-mail and instant messaging addresses, also intentional. Some of the more common methods used are more fully described below:

- Typo-squatting: Many adult sites use a domain name that is the same as a very popular site, and misspell it—so when people who are trying to contact the real site make a mistake in typing or spelling, they end up at the adult site instead. Over the few years, these "typo-scams" have included www.yahhoo.com (which, although now fixed, used to lead to www.rawsex.xxx.com) instead of www.yahoo.com, www.webcralwer.com (a pornography site), instead of www.webcrawler.com (a popular search engine), www.infosek.com (a pornography site) instead of www.infoseek.com (another search engine).
- Using different TLDs for popular domain names: Adult webmasters use our limited understanding of how domain names

work against many netizens, especially those new to the Internet. Most surfers have learned that when looking for an obvious brand or famous name site, they can often just add a "dot com" to it and find the site. Two of the most notorious instances of someone using a famous name to gain traffic from people making mistakes in the ".com," ".gov," or ".org" or various country designations are www.whitehouse.com (a pornography site that is still up[40]) rather than www.whitehouse.gov (the real site for the President's office, the White House in Washington, D.C.[41]), and www.nasa.com (a pornography billboard site that was shut down in 1997[42]) rather than www.nasa.gov (the official site for the National Aeronautics and Space Administration of the USA).

- The NASA site was put into operation during the first Mars photo landing, and held four to six rotating graphic sexually advertisements of pornographic sites. Hundreds of thousands of children worldwide logged onto the site, expecting to see Mars landscapes. Instead they were confronted with several very graphic sexual hardcore images. There are many more examples, worldwide.
- The Use of Generic Names Not Associated with Adult Content: The use of generic domain names, which most people would not expect to contain adult content, is also a popular way adult webmasters increase unsuspecting traffic to their site.
- Porn-Napping – Registering Lapsed Names with Loyal Traffic: There are several similar schemes or practices designed to increase traffic to adult websites from unaware surfers. Porn-napping (the popular name for adult sites that register domain names which have either lapsed or where not renewed either intentionally or accidentally) is a less well-known practice. A paper analyzing the impact of domain-napping of popular and well-established domain names by adult webmasters who register them and use them to house or redirect to sexually-

[40] Dan Parisi, the New Jersey-based owner of the well-known adult site, whitehouse.com (among other related domain names), has recently announced that he will sell the domain name to anyone who will not use the site to advertise or contain adult sexually explicit content. He has also indicated in an interview with Parry Aftab on February 13, 2004 that he will not sell the domain to anyone seeking to donate it to the U.S. government. The sale is was expected to take place after March 2004, once the auction mechanism has been arranged. Mr. Parisi said that he doesn't want his son to hear that his father is a pornographer. He is leaving the adult business completely following the sale of the domains. Mr. Parisi is expected to donate Whitehousekids.com (and other children's domain names) to a child online safety group.

[41] The Whitehouse site could not be shut down even after a written demand from White House counsel, since the name is considered generic and is not legally protected.

[42] The NASA.com site was shut down relatively quickly upon its being discovered, since NASA's name is legally protected in the United States.

explicit content documented thousands of porn-napping instances.[43]

- One of the best-known cases of porn-napping of a child's site involved Moneyopolis, an award-winning children's site created and run by the consulting house Ernst & Young. The site was linked to by many other sites and promoted in many Internet guides for children. It was a very popular and quality resource teaching children about financial matters. The main site was . org, with the .com pointing to it. When the domain registration was allowed to lapse in 2001 for some reason[44] (in all TLD formats), a pornographer purchased moneyopolis.org. He shortly thereafter pointed it to his EuroTeenSluts.com website. (Ernst & Young was eventually able to reacquire the domain name.)
- Metatags – the invisible code: When used properly, special keywords and descriptions help search engines identify relevant sites, based either on their subject matter or keywords and descriptions. These special subject terms, keywords and descriptors are written in a hidden code called "metatags."[45] The metatags are visible to search engines but not generally visible to the site visitor (unless they deliberately "display source" and then search for it in the code). Many adult sites use metatags either to misrepresent their sites, or to draw traffic based on famous names, brands and popular search terms.

[43] Ben Edelman, "Domains Reregistered for Distribution of Unrelated Content: A Case Study of 'Tina's Free Live Webcam'" http://cyber.law.harvard.edu/people/edelman/renewals/. In Edelman's article he tracked certain names that were re-directed to a directory site. One of those names, http://www.mandela-children.org/default.asp, was pointed to this domain directory page. Interestingly, when that page was accessed, it hijacked Parry Aftab's browser to changing her WiredSafety.org home page (without her consent) to the redirected http://www.mandela-children.org/default.asp page. Hijacking browser settings and home pages may violate certain consumer protection and computer criminal laws.

[44] The reasons given for failure to renew the domain registration differ depending on the source, but are irrelevant for the purposes of this paper.

[45] Metatags are essential to accurate search results online, when they are not misused. Since most search engines use technology to gather the first 25, 50 or 100 words from a site to determine what subject and search terms apply to that site, metatags (when used properly) can be very helpful. Without them some sites might be indexed based on the first blocks of words at the site, such as "Welcome to our site. We update it often and are happy to hear from you. Stop back often to see new articles and all our new features." This tells you nothing about the site, who runs it or what information it contains. Search engine technology (typically called "spiders" or "bots") typically uses the first few words found on the page to index the site. A good webmaster, to help index the site more accurately, uses words that describe the site content. For example, "skateboards, sporting goods, sports, kids sports, games, athletics, outdoor sports" in metatags will inform the search engines that the site is about skateboarding. That allows the site to come up when any of those terms is searched for online. Without metatags, you may not know what content is contained at the site. Unfortunately, using metatags that misrepresent the content at a site allows for unintended exposure to content, in often cases sexually explicit content from adult websites.

- To increase traffic to an adult site (probably to increase advertising revenues), many webmasters use popular search terms in their metatags to trick search engines into displaying their site in popular search results.
- Ironically, one of the first sites to enforce the intellectual property laws against an adult site misusing a metatags was Playboy Enterprises, Inc. (best known as "Playboy"), which is an international adult business organization. 1Another adult site used Playboy's name in their metatags. When people searched for "Playboy," the search engine results could include the infringing site (ironically, often at higher placements than the real Playboy site). The law was clear. Playboy quickly resolved the litigation in its favor, and the other site was forced to remove all references to any of Playboy's marks. Today, Playboy polices its mark using special technologies to scour the Internet for any infringements and is quick to sue to enforce its rights.[46]
- Posing as a Child Pornography Site: Many sites use metatags to attract traffic from adults seeking child pornography. Terms such as "Lolita," "preteens" and others are typically used to misrepresent their content to those seeking images of pre-pubescent children being sexually molested. ASACP (the entity run by adult website operators to find, and report child pornography and exploitation online) and some adult site operators have compiled a list of the generally accepted "outlawed words," which most within the adult industry agree should not be used to promote adult sites in metatags or otherwise.
- In the experience of those groups that combat child pornography online, this list would need to be supplemented to include the use of combinations of words or phrases, which taken singly are not problematic, but when combined create an impression of child molestation, such as "little boys." While not as heinous as images of, or which appear to be, children being sexually molested, use of these terms, according to many groups, promotes the market for child pornography and exploitation online.

Child Pornography and Child Sexual Exploitation

Child pornography was almost eradicated in many places around the world prior to the launch of the Web. Until then, the child pornography which remained were mainly pictures produced years before that were

[46] It is assumed that an .xxx TLD registrar will include mechanisms for enforcing intellectual property rights within the TLD, both of competing adult sites and non-adult brands.

constantly recirculated. But since the advent of the Internet and the popularity of the World Wide Web, child pornography has rebounded, becoming a booming e-business and its production and distribution an emerging cottage industry. (Child pornography isn't pornography that is made available to children. It's pornography that uses (or appears to use) children in sexual acts or in a lewd manner. The age of consent differs from state to state and from the state to the national levels of governments, as well as from country to country.)

While the laws differ substantially, and in some cases only outlaw production and distribution[47], rather than also outlawing possession, the laws typically look at several factors in determining whether an image is child pornography. The laws usually consider:

- whether the depiction focuses on the child's genitals or pubic area
- whether the setting is sexually suggestive
- whether, taking into consideration the age of the child, she or he is depicted in an unnatural pose and inappropriate attire
- whether the child is only partially clothed or nude
- whether the depiction suggests sexual "coyness" or is designed to elicit a sexual response or
- whether the child is engaged in actual or simulated sexual activity

It is a visual depiction of a crime scene, where children are being molested before cameras, or depicted as being molested. In addition many believe that viewing child pornography may help encourage actual child molestation by the viewers. Voluntary best practices guidelines should prohibit the sexual exploitation of children and prohibit the promotion of child pornography (real or virtual) and any site or service misrepresenting themselves as having child pornography at their sites. Requiring sites to stop falsely advertising child pornography shouldn't be a burden to the adult sites. In certain jurisdictions advertising that you are offering child pornography, even if you aren't, is already illegal.

Further, many sites claim to contain "teens" having sex. They usually only contain images of eighteen-year-olds having sex, not underage children. But clarifying this, by requiring the site to note the age of their actors and that they do not use images of underage children, would help reduce child pornography and exploitation online. The United States has similar laws relating to actors engaged in pornographic media, but these laws are not effective for adult content

[47] Some countries, most notably Canada and the UK, outlaw the online viewing of child pornography as well.

produced in other countries.

SPAM and "SPIM"

Everyone hates spam and its newest permutation with instant messaging, now commonly known as "SPIM". Most of us open our e-mail boxes (and, increasingly, ICQ messages and instant messages) to find hundreds of unwanted messages, many of which contain live links to adult sites. All children have to do is click on the link in the message, and they will be instantly transported to sites filled with sexually explicit images.

Sometimes these links are clearly labeled as sexually explicit, other times they aren't. For example, while the obvious ones are labeled as "XXXBlondes," others try to mislead the recipient of the e-mail into clicking on the link by saying things such as, "Hi. Last week I promised to get you the address for this site. Here it is." While the name may not be familiar, many click on the link and find themselves confronted with graphic sex images. This problem affects adults and children alike, but children may be particularly vulnerable to the graphic images.

While adults may oppose SPAM and SPIM, especially when they contain links to graphic sexual images and falsified return addresses, children are particularly susceptible to spammers and spimmers. Children's addresses are often picked up for bulk mailings, given the nature of the methods used to gather screen names, instant messaging addresses and e-mail addresses.

Sometimes they use e-mail addresses captured when someone accesses their sites, but far more frequently they use software and people to collect e-mail addresses, screen names, ICQ, and instant messaging addresses from chatrooms, newsgroups, and online profiles. This is called "harvesting." These millions of addresses are then often sold to other spammers as part of a bulk e-mailing list. Children often post messages and are more public online, in chat, in site-registrations and in public postings of their contact information, such as on websites, and in profiles and guestbooks. They also send and respond to chain e-mails, where harvesters easily gather hundreds and even thousands of addresses.

In addition, many children open e-mails and respond to instant messages without understanding the consequences (as do many adults). Responding to or opening a message that is being tracked with a web bug or other tracking or spyware provides important and financially valuable information to the spammer or spimmer. They provide intelligence that an address is still active and that the person behind the address may open or respond to the message.

This is key to the spam operation, because although the spammers might have known that the e-mail address, screen name, ICQ, and instant messaging address existed at the time it was harvested, they don't know if it is still in use. That is — not until someone opens a message being electronically tracked, or replies to the spam complaining about it, or asking to be taken off the list. Then they know it's a live account. That means the e-mail, screen name, instant messaging, and ICQ address will be far more valuable when they sell it to the next spammer. Children's addresses, since they are so active online, often get identified (with or without the knowledge that a child is behind a certain screen name) as the most valuable to bulk mailers.

While adult webmasters' best practice guidelines will not stop SPAM or SPIM, it will help reduce the number of fraudulent headers and hijacked e-mail and messaging accounts used to transmit SPAM and SPIM, and the inadvertent exposure by minors and unconsenting adults to graphic sexual images.[48]

Pop-Ups, Pop-Unders, Adware and Spyware

One of the most complained about problems by parents is the recent explosion of sexually explicit pop-ups. While this is a problem that adults also face, children are particularly vulnerable to the stealth installation of adware or spyware that delivers pop-ups and related advertisements.

Many game sites trafficked by children install these applications. So do many P2P services and other popular services and sites among children.[49] And the advertisements served often include sexually explicit websites and images. This problem has grown quickly – it currently tops the list of parents' greatest concerns about their children's online activities.[50]

Privacy issues and the Adult Website Operators

[48] Many jurisdictions are criminalizing or regulating unsolicited bulk messaging that uses fraudulent or stolen headers. Probably the most stringent of these criminal laws has been adopted by Italy, but its application is limited to those residing within Italy.

[49] Adware and spyware applications are not always installed without the "consent" of the person accessing the site or installing other applications. "Consent" is often buried in the software license or terms of use language that must be agreed to as a condition to its installation. Children, even if they read the legalese, would rarely understand its full implications. Adults rarely read the agreements, even if they would have understood it terms. While this White Paper cannot address all the concerns about spyware and adware, it does address the kinds of content advertised, when this involves graphic sexual images or links to adult sites.

[50]Governments seeking to apply their laws extraterritorially share this concern.

Privacy concerns are not limited to adult websites and services, but they have a particular significance when the adult industry is involved, and when responsible websites are involved. Adults who knowingly access and subscribe to adult content and services online may be uncomfortable with sharing information about this preference. They may be more reluctant to pursue the redress of unauthorized charges and fraudulent practices involving their subscriptions or adult content use. Also, the less responsible adult sites may not be responsive to complaints from their customers about unauthorized charges and payment disputes.

Sometimes when children and teens knowingly access adult sites, using their parents' credit cards, disputes arise about whether the charge is authorized or unauthorized by the cardholder under applicable law. Protecting adults' subscription information is of unique importance in the adult field. When adult content subscribers seek public office, or find themselves in the midst of a matrimonial action, the knowledge that their personal activities receive the protection of applicable law is very important. Best practice guidelines can protect the civil rights of adults accessing materials online, which although inappropriate for children, are in many places legal for adults.[51]

A significant component to online privacy is trust. If people accessing a site trust that the site will not misuse their information, and will use it only for purposes they consent to, they are usually willing to consent to sharing that information. This may impact the adult community even more acutely. Which site is worthy or their customers' trust?

Many adult websites are under common control, or have agreements to share customers' preferences or personally identifiable information among them. Others are not as careful about security practices, putting their customers' personal and credit card information at risk. The more unscrupulous sites engage in active criminal conduct and facilitate identity theft and financial fraud.[52]

Some adult webmasters have addressed concerns about their data collection and use practices by applying for third-party privacy certifications, such as the TRUSTe and BBBonline seal programs. These programs and any best practice guidelines require four basic levels of compliance: notice about what is being collected, how it is

[51] One of the foundations for promoting a voluntary best practice model is to avoid conflicting legal frameworks and values.

[52] It is recognized that no 'best practices' guidelines or even an .xxx TLD will be able to stop criminal activity and fraud. But it will be able to help adult customers and law enforcement identify those which are conducting themselves in a commercially responsible manner. This makes it easier to spot and stop those engaging in criminal and more nefarious activities.

being used and with whom it is being shared; consent to such collection and use; making sure that the information is collected in a secure manner and maintained in a secure setting; and making sure that the information is accurate and complete. These basic privacy standards will be core to these privacy best practice guidelines.

Annex B

(This is an informational document submitted by ICM Registry, one applicant for an .xxx TLD)

ICM's Intentions

Proposal for a Voluntary Adult .XXX Top-Level Domain (TLD)

The Internet Corporation for Assigned Names and Numbers (ICANN) will be accepting applications for new sponsored top-level domains (sTLD) as part of its initiative to enable new top-level domains and inspire global innovation and competition online. ICM Registry will be submitting an application to become the operator of a new registry for the ".xxx" TLD. The sponsor of the new TLD is the Foundation for Online Responsibility (FOR), a Canadian non-profit entity that is totally independent from ICM.

The ".xxx" top-level domain will create a clearly identifiable area of the Internet that will both help protect children and families, as well as enable responsible adult-entertainment website operators to selforganize and self-regulate on a voluntary basis.

Why Is A Voluntary .xxx TLD Needed?

- As one of the largest and fastest growing sectors of the Internet, the online adult-entertainment industry will benefit greatly from responsible self-regulation.
- According to Reuters, online adult-oriented ecommerce is worth more than $3B USD globally and is growing at a double-digit rate. The number of adult websites has grown eighteen-fold over the last 6 years.
- More than 10% of all online traffic and 25% of all global Internet searching is adult content oriented, with more than 100,000 adult webmasters worldwide, and well over one million adult domains.
- There is continued demand from child and family safety groups to ensure the Internet is safe.
- Internet users are desirous of a system that provides the highest-possible levels of privacy and security.

What Are The Benefits Of An .xxx TLD?

- Online child safety and anti-child pornography will be promoted through best practice guidelines promulgated by a non-profit cross-sector foundation. This foundation will provide assistance through various online support organizations and the sponsoring of technology tools and education programs for parents.

- The online adult entertainment industry wants to create an identifiable space with which its members can elect to associate themselves and wherein they can responsibly self-organize and create guidelines to promote credible self-regulation.
- The voluntary .xxx TLD will maximize and protect free speech – both for content providers and Internet users.
- Privacy protection and security will be promoted for online consumers.
- The .xxx TLD has potential to regularize business processes such as search-engine functionality, privacy, identity theft prevention measures, and security.
- It creates a credible forum for representation and self-regulation where all stakeholders are able to discuss and actively respond to concerns about online pornography.

Where Is The Support For An .xxx TLD?

The .xxx TLD is industry-led, market-driven and non-regulatory, and has drawn the support of a broad coalition of Internet stakeholders, including:

- Child and family safety groups
- Global adult-entertainment industry leaders/members have agreed to voluntarily participate
- Free speech, privacy and security advocates
- Information technology (IT) experts
- Public policy leaders

Who Will Submit The .xxx TLD Application To ICANN?

- • **ICM Registry will operate the registry.** ICM is a financially stable and completely independent entity with no affiliation, current or historic, with the adult-entertainment industry. ICM will operate the registry – providing management, supporting infrastructure and back-end functionality. For more information about ICM Registry go to: http://www.icmregistry.com
- • **The International Foundation for Online Responsibility (FOR) will sponsor .xxx.** IFOR is a Canadian nonprofit entity that will sponsor and serve as the policy-making authority for the .xxx TLD. IFOR is and will remain totally independent from ICM Registry, primarily funded by registration activities. It will have its own board of directors, representing the various stakeholders, including child-safety representatives, members of the free-

speech community and adult entertainment industry leaders. IFOR's mission is to contribute programs and tools to both make a difference in the ongoing battle against child pornography and to become a forum for the online adult-entertainment community to communicate and pro-actively be responsive to the needs and concerns of the broader Internet community.

- IFOR will engage in programs and activities, including: supporting free expression to allow Internet users rights to chose the online content they desire; promoting public awareness of technologies, programs, organizations and methods available to protect children online; enhancing development and proliferation of PICS labels and systems for labeling and identifying content; sponsoring approved child safety and child pornography reporting organizations; prohibiting deceptive or unfair business practices; normalizing online services for registrants to increase credibility and predictability; and enabling enhanced intellectual property law protections.

What Will Be The Obligations Of .xxx TLD Registrants?

Participating Internet content and service providers believe that responsible self-regulation is essential to the industry's continuing viability in the global marketplace. Internet content and service providers that voluntarily register the domain names will adhere to a high-level set of business practices, embodied in an enforceable contract between the Registrant and ICM Registry. The credibility of such practices cannot be preserved by the one time creation of a set of responsible business practices: FOR must establish, revise and continually update these practices to accommodate developments in technologies and societal expectations.

.xxx domain name registrants will be expected to adhere to the following best business practices:

- Safeguarding children from being marketed or targeted online;
- Defending customer privacy;
- Promoting accurate meta-tagging;
- Ensuring clear and accurate disclosures, security of transactions and contact information;
- Protecting intellectual property rights;
- Combating the use of unlawful malicious codes and technologies, like spoofing;
- Opposing fraudulent, anonymous and unsolicited bulk SPAM advertising pornography; and

- Blocking domain names intended to attract child pornography consumers.

In addition, ICM and FOR will make a difference in the battle against child pornography by sponsoring programs to safeguard children**.**

For further information on this application and the goals of the organizations involved, contact:

Stuart Lawley, Chairman, ICM Registry sjlawley@icmregistry.com

Annex C

Some authors of this White Paper have expressed a desire to describe alternate forms of governance of any best practice model. Although not specifically endorsed by those joining in this White Paper, it is important to understand the kind of oversight that would be required absent the formal structure of an .xxx registry. One such suggestion appears below:

Permanent Council

In the event an .xxx TLD is either not created, or any successful applicant therefore does not adopt all or a substantial portion of the recommendations contained herein, formal oversight and administration structures would have to be created. One way to ensure complete agreement among all stakeholders is to create an environment for continuous dialogue, with a focus towards measurable results from time to time. Such results should include, in the beginning, the first set of best practices guidelines.

Later, this may expand to updating the set, compliance, complaint handling, conflict resolving (in cases where individual stakeholders report damage to their interests following adoption of the guidelines), research and monitoring of abuse of the guidelines (for instance: where an innovative approach to business generation by adult industry players emerges, that potentially targets children but is not covered by existing guidelines; or moves by governments to restrict access to adult content that harm the efficient functioning of the Internet itself).

While it is relatively easy to create a mechanism for open dialogue (members representing stakeholders can be inducted voluntarily to a council, and protected online using security technology), ensuring results is another matter. Right from the beginning it will be necessary to lay down a time-bound deadline for declaration of an initial set of guidelines. The set should be created by consensus. The group should also evolve its own articles and memorandum of association within a fixed time-frame. These two actions will more than demonstrate the power of the proposal contained in this White Paper, in the event an . xxx registry is not created, or these recommendations are for some reasons not adopted.

Executive subgroups and Secretariat

A smaller, executive, group should be chosen (if necessary, co-opted) from among the volunteer members, in order to manage a secretariat and administer the technology that keeps the council open to dialogue but secure from external interference (some adult industry players may be operating illegally with respect to the statutes of their own countries). The secretariat will also recommend new guidelines and fees payable to the Council necessary to make it self-sustaining and independent from external control.

Finally, the executive group will also ensure that continual research is undertaken to ensure that the business interests of responsible adult industry players is better served by compliance than otherwise.

Independent Audit

The executive group will inevitably gain some influence over the proceedings of the Council. To ensure the fairest possible process is maintained, an independent monitoring group, reporting (and responsible) only to the Council should also be appointed.