Why Internet Censorship Does Not Work

By Ben Tasker | 17 June 11

Contents

Click the titles to jump to the relevant section

Introduction

There are often calls in the UK for the Government to regulate and 'protect' children from pornography (and other adult material) on the Internet. In the past, I've recounted the basic reasons why it doesn't work but let's take a more practical approach this time.

We'll be looking at some of the means of filtering (at both the wide-scale and the home user level) and the technical issues with them, including how easily they can be bypassed. Rest assured that if there is a way to bypass a control, a child will find it – especially if they are actively seeking out pornography!

This document looks at the issue of pornography in particular, but applies to most materials that may be censored.

I've tried to avoid jargon where possible, as this document is actually aimed at those who have an interest in preventing their children from accessing certain materials (and who generally speaking, are not techies!).

Bypassing The Most Common Methods

DNS Filtering

This is perhaps the easiest means for a home user to configure, and is one of the tools often used by larger censorship projects.

The DNS system is (simply put) much like an address book, networks deal with IP addresses (i.e. 192.168.1.1) but we often deal in URL's (i.e. www.google.com). DNS translates our URL to an IP.

So the way DNS filtering works, is it 'lies' about the address for a blocked site, often leading the user to a page warning them the requested resource was filtered.

So for example, although www.mynaughtysite.com may have an IP of 1.2.3.4 the DNS server might return 4.3.2.1 to prevent access to the site.

This option is available to home users through services such as OpenDNS.com (free to use) and offers a range of filtering categories (porn, gambling etc.) but it's not a magic bullet, and here's why;

If we slip into teenager mode, we want to access mynaughtysite.com but it's been blocked using DNS filtering. Here are the steps to bypass (and don't think a teenager can't work it out!);

1. Access dnsquery.org (or run a web-search for "IP Address lookup")
2. Enter mynaughtysite.com into the "DNS Record Query" box (use Google.com if you want to test it)
3. Hit query
4. We now have the IP address for the site we want to access
5. Copy that IP into the address bar and browse to your heart's content.

Now for some sites, this won't work because links are coded to force use of the URL (web address). There is however a way around this too;

1. Open your computers HOSTS file in a text editor
2. Enter the IP address we retrieved earlier followed by a tab and the web address

Problem solved!

There's not a huge amount you can do to prevent this, you can make sure your kid doesn't have the permissions to write to the hosts file but that just means they need to do everything manually.

Content-filtering is needed to catch the pages that get past the DNS filtering, or indeed are forced past the DNS filtering by your kid!

Content Filtering

Beloved of the Chinese Government, content filtering examines the page as/before it loads and searches for keywords that might trigger a block.

You can either run content-filtering software on the PC your child is using (the common home approach), or run all connections through dedicated hardware (the corporate approach).

Generally content-filters suffer from two main problems;

- They miss things
- They get bypassed

When dedicated hardware is used, simply using an encrypted connection is sufficient to bypass the filter (i.e. using https instead of http). Of course, the hardware can be configured to allow it to see encrypted streams but no-one would want an Internet Service Provider or the Government to actually do this!

If it were to happen, the ISP/Government would be able to more effectively filter porn etc. but they (and all their employees) would also have the capability to see your passwords, Internet banking and all the other things you might like to keep secure.

This actually happens already in the criminal world and is known as a Man In The Middle Attack.

So, on the national censorship level accessing https://www.mynaughtysite.com instead of http://www.mynaughtysite.com is likely to remain a viable way to bypass the filters for the foreseeable future.

Software installed on the users PC can be very effective, but it does also put it in reach of those who have an interest in disabling it. Most of this software is unaffected by the use of an encrypted connection, but can instead be more readily tampered with.

This becomes even more apparent if you choose to use the same password for it's settings as you do anything else – Kids aren't stupid, they **will** try every one of the passwords that they know you use.

If you make the mistake of letting your kid have an Administrator account, they may also choose to just completely disable the software. They don't necessarily need to access the software itself to achieve this - in Windows simply disabling the service is often sufficient;

1. Control Panel
2. Administrative Tools
3. Services

So again, whilst it may seem effective content-filtering can quite easily be circumvented with very little research.

More effective solutions

Both of the solutions below need to take place on a local scale and can't or shouldn't be regulated/implemented by the Government – you must implement them yourself;

The walled-garden approach

There are two main ways of restricting internet access using web-addresses – blacklisting and whitelisting. The DNS filtering we discussed above generally uses a blacklist of 'banned' sites.

The problem with blacklisting is that there are just too many sites to add, it would take years of research just to get a basic list. Even then you'd probably miss more than you'd catch.

A whitelist is more restrictive but uses a more sensible question – which sites **do** you want to allow access to?

Any site not listed on the whitelist is blocked by default, which can be really annoying but does ensure that your kid only sees content approved by you.

Setting up a whitelist can be achieved in a number of ways, including within the browser itself. You need to choose the technology you use carefully to ensure your kid doesn't have the ability to disable/bypass it.

You could opt to use dedicated hardware to manage your whitelist, which would make it harder to tamper with. There are also companies that provide a service similar to OpenDNS but utilising a whitelist based system.

It should be reasonably clear why the Government shouldn't be allowed to implement a whitelist based system; to do so without infringing freedom of speech would be impossible!

Cold Hard Parenting

The tried and tested method to date is to be sat near your kid when they are on the Internet. Don’t give them access in their room, and ensure they PC is in a very public area.

Talk to them about the dangers of the internet; warn them that certain areas are far from savoury and that you don’t want them actively seeking these things out. Follow up on your rules, and don’t undermine them by having your own porn stash on the PC!

Monitor their usage (you can even get software to keep a log of what they view), but understand that ultimately if they **want** to find it, there is nothing that either you, the Government or your Internet Service Provider can do to stop it.

Not talking to your kids about this issue is one of the worst things you can do, sooner or later it’s likely they’ll either develop an interest or manage to stumble upon just the kind of material you were trying to shield them from. Recently there was a story about a teenager researching his chemistry homework; quite naively (as he didn’t know any better) he ran a websearch on the word bondage from a school computer!

You very rarely stumble on pornography by accident, but because of the naivety of childhood kids don’t realise that some of these phrases are double entendres. Talking to them about these issues is the only thing you can do, because pornography is never going to go away.

Ultimately, the Internet is an adult area and children need to be supervised when entering that world. Whatever your feelings on pornography as a whole, a lot of the technology you take for granted came about because the porn companies were the only ones so see a commercial advantage in pursuing development – In the days when the Internet was still a hobbyists playground, porn sites were some of the few commercial entities that had a web presence.

How many of those reading this saw porn before the Internet? People used to leave their magazines lying around at bus stops and similar places, it may be more readily available but it’s always been there. Only good parenting can counteract any perceived damage that exposure may cause.

More Information

Browser Based Technologies

One word of warning about **any** browser based filtering solution; it really doesn't take much effort to bypass these measures. Your kid could, for example, choose to use a portable Firefox install or the really determined could achieve things manually (admittedly, not many are likely to be determined enough);

1. Start Menu
2. Run
3. Cmd
4. telnet http://mynaughtysite.com 80
5. GET / HTTP/1.1

They can then copy and paste the output into notepad, save as a HTML file and open in the browser. Not exactly graceful, especially if you want to browse an entire site, but still entirely possible.

Despite this, however, many browsers do incorporate basic filtering methods. These can be effective, but are reliant on sites conforming to certain standards. Unfortunately, the sites you are likely to want to block are the very ones likely to ignore these!

The adult industry appears to have no interest in serving their content to minors, and already incorporate robust mechanisms to prevent access by minors. The sites that pose a perceived risk are those that do not care who they serve their content to, who by their very definition aren't going to worry about including meta-tags to identify their content as adult.

Government Intervention

Most people do not want Government Intervention for a number of reasons, but primarily because it just doesn't work. The Chinese Government have implemented the worlds biggest censorship mechanism, and yet it is still bypassed by multiple users.

The Chinese, in fact, have an advantage because they have managed to convince their populace that the censorship is for their own good. Many of those who may otherwise bypass don't purely because they believe the Government must be acting in their best interests.

It seems unlikely that this culture of faith will ever form in the UK, especially as each of us is able to read exactly what the consequences of it are in China.

Government Intervention/Regulation will also cost a lot of money, the hardware required does not come cheaply and every taxpayer (or Internet subscriber) will bear part of the cost, whether they have children or not.

A cost that will be needlessly spent on an intrusive and ineffective solution, we've already shown above how easily the two main mechanisms can be bypassed. We certainly don't want the Government to give their censorship hardware the ability to read our encrypted connections as all pretence of privacy can be abandoned at that point!

The experiment with the Great Australian Firewall has shown just what a slippery slope Government mandated censorship is. The GAF was implemented to block 'illegal' content such as Child pornography and the more extreme adult pornography. It soon came out, however, that ministers had been misusing the system leading to the blocking of

- A Queensland Dentist
- A Kennel Operator
- A tuckshop
- A Photographers website (all images were rated PG by the Australian rating committee)
- A site relating to Euthanasia
- An Encyclopedia Dramatica article titled "Aboriginal"

The Internet Watch Foundation

The IWF is the UK's blacklist based filtering system for child-abuse material. It is voluntarily implemented by the Internet Service Providers (i.e. BT, Virgin etc) and is often held up as an example of how censorship can work.

However those who would hold the IWF as a shining light often neglect to mention it's spotty history, or the concerns relating to due process;

- The IWF reported a site to the UK Police for containing fictitious erotic material of an extreme nature, this led to the unsuccessful prosecution of the site operator (the prosecution offered no evidence)

- In 2008, all UK users were blocked from editing Wikipedia articles after the IWF added a Wikipedia page to the blacklist, forcing all users to appear to originate from the same IP address. The IWF later rescinded the block (more info below).

- In 2009 the IWF blocked the Internet Archive in it's entirety despite their policy to only block the specific content. It was blamed on a 'technical hitch' but the content causing the issue never became publicly known

Concerns regarding due process have arisen because the IWF does not just block *illegal* content, it also blocks content which it believes *may* be illegal under UK law. The blocking of Wikipedia is a prime example of the difficulties this introduces, the image blocked was the cover art from the 1976 album Virgin killer by the Scorpions. You can still legally buy the album, with that cover, from high-street stores and Internet music stores alike. The IWF, however, decided that the image was *potentially* illegal and without judicial oversight proceeded to block the relevant Wikipedia page.

Repeatedly criticised for blocking legal websites and not telling the website operator about the block, the IWF keeps it's blacklist secret and is self-regulated which means there is absolutely no oversight over their actions.

Current Censorship Projects

If you've purchased a new SIM card for your mobile phone recently, you'll know that the mobile networks are now blocking adult material by default. This provides a great example of how filtering

a) Is Worked around
b) Inconveniences Everyone

Usually to lift the block, you either need to go in-store with ID or provide a credit card number. Most kids are unable to do either of these, and yet are still able to access porn on their phone! Why? Because the enterprising ones have started posting it on Facebook! So already the expense of implementing the filter (which ultimately the customer pays for) is already wasted because the kids have found a simple solution. In response to the blocking of Facebook, kids have moved onto other medium such as Multimedia Messaging.

On the other hand, if you happen to be trying to access something innocent like a forum, you may struggle. A lot of the operators have begun blocking forums purely because of the content that can be posted there!

Try loading a page even loosely related to a blocked term and you're stuck. It doesn't matter that the page you're trying to access contains nothing adult, if it appears to do so it will be blocked.

This broad-brush approach not only inconveniences adults, but can prevent kids from using the internet for their homework. Try researching basic human biology on a device with this filter enabled and you'll understand the difficulties caused by such a "one-size-fits-all" approach.

Anything the Independent Mobile Classification Body rates as adult will also be blocked, but given that they only rate 'commercial' content a lot of content will still be missed.

Green Dam Filtering Software

The Chinese Government used an image-scanning technique to aid their censorship efforts. The attempt came about partially as the result of site operators posting pornographic images on pages with neutral text (so that the filter wouldn't pick up on 'banned' phrases).

The software scans images to try and ascertain how much skin was on display in the image, although it correctly identifies some images it suffers from a number of technical issues;

- It does not recognise images of people with darker skin (or in the case of cartoons – red skin)
- Some very graphic sexual acts are missed because not much skin is visible

It also generates a lot of false positives, which led to the automatic filtering of a lot of non-adult content including;

- Images of the cartoon cat Garfield
- Images of Roast Pork
- Images of Johnny Depp's face

Green Dam also includes a content-filter, which drew scepticism about the Chinese Government's claim that it was to "protect the growth of young people" when it was discovered that 85% of the pre-programmed keywords were related to political matters and just 15% related to pornography.

Not only does *Green Dam* filter internet use, but also monitors applications such as Microsoft Word for 'inappropriate' phrases. Should something inappropriate be detected (in the browser or otherwise) all windows are closed without notifying the user.

Multiple security vulnerabilities have also been found, allowing attackers to access personal data, remotely compromise ('hack') or use the machine to send SPAM.

The filter is actually a piece of software called *Green Dam Youth Escort*, which was originally mandated on all new PC's by the Chinese Government. However, it was then made voluntary and the deadline has repeatedly slipped.

At time of writing, the company behind Green Dam is on the brink of collapse having received no further funding from the People's Republic of China. It appears that the Chinese Government may have abandoned plans to use *Green Dam* in their censorship programme.

Conclusion

Hopefully this article has given you an insight into why government mandated filtering cannot work, the methods of circumvention I've given are some of the most simple and yet they work.

Far more advanced methods can be used, and are harder to mitigate. Do you really want everyone to foot the bill for a system that will never work quite as well as you hope and may even give some a false sense of security?

Pornography has been available since the earliest days of man, and there's no reason to believe it's going to go away anytime soon. If you are truly worried about the affect it may have on your children you need to stop expecting others to act, and take matters into your own hands.

You may need to search the net and read a more detailed guide than this to find the solution that fits you best, but as a parent it's your responsibility to do so. There are not many other areas where we expect to be allowed to remain uneducated in how to work something we use regularly. Even the Car driving test now expects drivers to have some knowledge of maintenance, why should your PC be any different?

There is a perception that local measures are easily circumvented, I hope this article has shown that wider scale controls are just as easy to circumvent. If a teenager is able to circumvent something that you have installed and configured, it's quite likely they'll be able to figure out how to bypass anything the Government might choose to put in place.

Not only are wide-scale solutions ineffective, history has shown that once a mechanism of censorship is implemented it is often abused by those in power. Removing elected officials ability to abuse the system leads to a self regulating body such as the Internet Watch Foundation, whose record is less than clean.

It seems clear then, that when discussing suitability of material for children, those best placed to decide are not elected officials or corporate bodies but the parents of each child.

"Parental responsibility cannot and should not be abrogated to government - if it is, our society will only become weaker ..." **- Cory Bernardi , Australian Liberal Senator**

"We believe in parental responsibility, and that you should take care of what your children are reading. But it's not your responsibility to tell a whole class of kids what they should read." **- Michael Gorman, Writer**

Distributing this Document

More whitepapers and other resources available at http://www.bentasker.co.uk/