Children's Charities' Coalition on Internet Safety

85, Highbury Park
London N5 1UD
22March, 2010

Peter Robbins OBE, QPM
Chief Executive
Internet Watch Foundation
5 Coles Lane
Oakington
CB4 5BA

Dear Peter,

**Blocking access to illegal images: concerns about transparency and accountability**

I have recently been working with others investigating ISPs that do not appear to take any steps to block access to internet addresses known to contain illegal content, namely child sex abuse images. I have been focusing on two ISPs in particular: Supanet and Cable & Wireless (C&W).

As you know, OFCOM recently confirmed that 98.6% of everyone in the UK with a consumer broadband connection belongs to an ISP that blocks access to web addresses known to contain child sex abuse images. They do this by deploying the IWF list of such addresses. It means 98.6% of all UK domestic subscribers cannot obtain direct or easy access to any of the addresses on the list. Supanet is a consumer ISP but Supanet's customers appear to be among the 1.4% not covered. Given Supanet is largely a family-oriented ISP this is very odd. It is the reason I have taken a particular interest in them.

Supanet recently told a newspaper reporter that they do deploy the IWF list. The reporter got in touch with me and gave me permission to repeat this. The reporter said Supanet declined to give any further details and he, the reporter, was not able to contradict the company. Effectively, by this simple device, Supanet killed off a potential story about them.

I note that Supanet is not a member of the IWF. Thus, if it is the case that Supanet is using the IWF list, it must be because they have brought in a third party solution that incorporates it. We have no way of confirming this.

I have almost lost count of the number of times I have written to Supanet about this matter. They have only replied once, and that was in response to my first email, last October. In that reply Supanet simply ignored my direct question about their use of the IWF list. I think this is called "stonewalling". Disgraceful and impolite, but again effective.

In that reply last October someone called Steve Smart, whom I believe is the Managing Director, referred to the fact that Supanet provided its customers with access to filtering products. Mr Smart did not say the products incorporated the IWF list but the key point is they were optional extras for which there was an additional charge. Having just checked Supanet's site again, there is now only one filtering product listed. It is called "eSafe@home". After a free 14-day trial it costs £7.99 per month. There is nothing to indicate that "eSafe@home" utilises the IWF list.

The point about the IWF list is that, in our view, it should be there by default. Blocking access to child sex abuse images should not be an optional extra. It should be part of the basic service. If someone was determined to have access to this kind of illegal content they are the very last people who would voluntarily pay to have it blocked off. This isn't voluntary or optional for the other 98.6% of UK domestic users. Why should it be for Supanet's customers? On the other hand if Supanet really is using the IWF list in some way or another why do you suppose they will not say so clearly?

You would think that a company such as Supanet would be delighted to help fight against child abuse images by proclaiming, unequivocally and publicly, that they block access to all web addresses known to contain them. You would think a company such as Supanet would be happy to make it plain they apply the IWF list or a similar solution and that they do this irrespective of whether or not their individual customers choose to buy the filtering product the company also promotes.

Turning now to C&W, it is the UK Government's major supplier of ISP services, or at any rate it is one of them. C&W acknowledges it is not a member of the IWF and so has no direct access to your list. They maintain they are not active in the consumer space, they are active only in the Business to Business market, and therefore the same considerations which might apply to consumer ISPs ought not to apply to them. This is not a distinction we have ever accepted. Very many employers allow or encourage their employees to work from or at home so their internet connection is clearly being used in a domestic environment. But even if that were not the case, why would businesses want to be exempt from blocking access to child abuse images? There are lots of known instances of employees accessing this kind of material at work.

C&W nonetheless told the same reporter referred to above that it knew access to child abuse web sites is being blocked within the UK Government Departments it serves via an add on service supplied by Message Labs. I checked with Symantec, who own Message Labs. They have confirmed this. Message Labs do buy in and incorporate a third party solution from a company that is listed as a member of the IWF. They did not tell me which one but I am 99.9% certain I know its identity.

The situation these facts highlight is far from satisfactory.

In the first place, even within UK Government Departments blocking access to child abuse web sites obviously has been an optional and presumably paid-for extra. However, this situation has at least now changed for the better.

On 5March, the Government announced that, in future, any ISP that does not incorporate the IWF list as part of its basic service will risk losing all of its Government and public sector business. This is a world first and we were very glad to be able to congratulate the UK Government for taking such a step and showing this kind of leadership.

Perhaps other large purchasers of ISP services and other relevant online services will take note and follow their lead. We will certainly be doing all we can to encourage such a development in the private sector. We will also be closely following events to see what effect the Government's announcement has in the run up to the renewal of any public sector contracts currently held by C&W, or any new ones C&W bids for.

The second aspect of this which is unsatisfactory from our point of view is that companies such as Supanet should not be able to make a public claim that they are blocking access to child abuse web sites if that claim is not in some way verifiable. I feel this particularly strongly since the vast majority of consumer ISPs plainly has no difficulty with this.

As I understand matters, members of the IWF that take the list directly from you have to self-certificate that they are not only taking the list but also they are deploying it and this is put on the public record. It would be odd if that provision, or the spirit behind it, could be side stepped by a

company or organization simply getting, or claiming to have got, a third party to do it for them. It means companies and other organizations could say whatever they liked and no one would have a legal way of knowing what the truth was. That cannot be right.

Maybe the IWF should consider modifying its rules. If a company or organization claims, say, Websense or Rulespace or NetClean or some other IWF member, is blocking access to known child abuse web sites for them by using the IWF list, then Websense or Rulespace or NetClean or whoever must confirm or deny it. A simple “yes” or “no” would be fine.

Finally, I fully accept that companies or organizations signing up with a new ISP or customized online service should have the right to ask for blocking access to child abuse web sites to be turned off or for it subsequently to be withdrawn, but there should be zero financial incentive for them to do so i.e. if they do ask for it to be turned off or withdrawn there should be no reduction in the charges.

Quite why a company or organization would want such blocking to be turned off or withdrawn is another matter but it is possible for example, if they had already developed an in house or proprietary solution, they might worry about potential conflicts or excessive network overheads. Alternatively there could be an another solution available that better suited them. Within the overall self-regulatory environment within which the IWF operates there ought to be a way of accommodating such situations whilst still maintaining transparency and accountability.

Either way, requiring companies or organizations to ask for a default blocking component to be removed or withdrawn would at least make it quite clear that it was wholly intentional and the company or organization would then be liable for the consequences of whatever happened following such a decision.

I would be very grateful for your comments.

Regards

John Carr
Secretary