We all know what a smart bomb is – or is supposed to be. In the Gulf War, we were shown computer-game images of these clever devices seeking out the bad guys while leaving all surrounding buildings and innocent people unscathed.

In many ways, initiatives like web blocking and other measures to restrict access to online information are like those smart bombs – except in reverse.

They are stupid smart bombs, which manage to leave the intended target entirely unscathed while doing all sorts of collateral damage to innocent people, to innovation, to free speech and to the openness that is at the root of the success of the Internet – and therefore at the root of the success of many of your businesses.

Pirate bay

The blocking of Pirate Bay in Denmark is a perfect example of this.

The content industry suffered collateral damage through demeaning itself by exploiting the already existing blocking of child exploitation sites. They argued that blocking of Pirate Bay was proportionate as it involved little extra investment by the Internet providers.

The Internet access providers suffered collateral damage because they saw the “voluntary” blocking of child abuse websites starting a domino effect which will result in them being obliged to pointlessly try to police more and more activities on the Internet.

Society at large suffered collateral damage as online communication, a key element of democracy and free speech is slowly strangled by demands for more and more restrictions and more and more extra-judicial policing and prosecution by generally unwilling internet providers.

And what about the allegedly illegal activities that this measure was meant to address?

The Pirate Bay announced a 12% increase in traffic from Denmark in the days that followed the imposition of the block.

Child abuse websites

And what about blocking of child abuse websites – surely that protects children?

Surely that is a real smart bomb, tackling abuse by targeting those evil websites?

Well, firstly we need to realise that it only addresses

- the small proportion of child abuse images that are on the web
– and then, only the small proportion of the websites that are actually publicly accessible;
– and then, only the small proportion of the websites that are publicly available and are in a fixed location;
– and then, only the ever-smaller proportion of websites that are publicly available and at a fixed location and not on a hacked server or free hosting service -where the owner would be eager to help facilitate investigations against the criminals abusing their service, rendering blocking irrelevant.

Okay, fine, it only addresses a tiny part of the problem, but at least it solves that part of the problem, doesn't it?

Well, it doesn't solve the problem that the websites are online – blocking does not delete them, it simply makes them less visible. Financial fraud websites aren't blocked, they're deleted within about three hours of discovery. Child abuse websites are increasingly blocked, and the time it takes to take them offline isn't three hours, it isn't three days, it is about three weeks. Except in Germany, which promotes action against the websites themselves instead of blocking – and their results are far more impressive, the sites remain online for a far shorter time.

It doesn't solve the problem that the criminals behind the sites are still at large. Even worse, it creates a new problem because being blocked will warn the criminal that it is time to move to avoid detection.

It does nothing to identify and rescue the victims depicted in the images.

It doesn't solve the problem of people who want to visit those sites. They can work around any blocking system that is currently on offer. The whole basis of the design of the Internet is resilience, even dropping a bomb on one part of it will not stop traffic from routing around the bomb site.

Does it solve the problem of people accidentally accessing these sites? Well, of the 150,000 people that downloaded the German browser add-on button to make reporting of illegal sites easier, virtually nobody actually finds material that they report via the button. Maybe it would solve the "accidental access" problem if it existed. Or maybe not.

Giving states a way of hiding their inaction is negligent and contrary to the best interests of children.
Targeting Internet access providers instead of criminals that publish child abuse websites is negligent and contrary to the best interests of children.
Planning for failure in international cooperation is negligent and contrary to the best interests of children.

Asked for the evidence on which the decision to promote blocking was based, Commissioner Malmström pointed to some general trends and said... and I quote... “they do give an indication that, to a certain extent and at least partly, this may follow also from action taken, including action to block access to websites in some countries.” This is supposed to be “evidence-based” decision making.

But at least it is better than nothing, right?

What damage does it do?

It gives criminals an early warning that their activities have been identified by law enforcement authorities.
It accepts and plans for failure in international cooperation to delete the websites, prosecute the criminals and identify the victims.

It gives governments the opportunity to make it appear that they are taking action on child abuse when evidence from countries that already undertake blocking is that it is used as a smokescreen rather than as part of a comprehensive strategy.

It simply outsources the problem to access providers who, as you know, can do nothing except take cosmetic measures that don't touch the problem.

**And it damages the democratic and competitive internet**

The European Commission's proposals on Internet blocking do not suggest any particular technology. Many in the Internet industry are not particularly worried by this proposal because, historically, blocking has been a fairly simple deal. The providers invest little in terms of time/money and the government looks like it is doing something to fight child abuse – everybody wins. Well, except that the child abuse sites stay online and the criminals stay free to exploit more children.

For businesses, rolling this out on an EU-wide level is hardly problematic, is it?

As the Directive is currently written, there are no limits to what can be demanded – and this has been recognised and welcomed by Commissioner Malmstrom in a German newspaper earlier this year – where she said that she can well imagine that some governments will demand blocking technologies that are more effective than what is currently being used.

If companies like Virgin and Telia are rolling out deep packet inspection for the purpose of managing copyright or providing a non-neutral access to the Internet, it follows, as night follows day, that the child protection industry will want to add DPI to their next set of demands.

And once deep packet inspection is being used for one purpose, it may as well be used for another – creating a vicious circle where more demands for policing via DPI will lead to this technology being implemented and then this being used to justify and gain acceptance of DPI being used for other business purposes – making it more and more impossible for regulators to intervene to avoid it being used for discriminatory purposes.

Of course, there will be smaller providers that have no business interest in investing in DPI, but wouldn't it be just unforgivable not to invest in order to protect the children?

We have already seen examples of certain incumbents using the tools at their disposal to block or restrict access to their customers. We have seen them block competitive products while developing equivalent products themselves – DPI will make this much easier.

An example of such restrictions was T-Mobile, who refused to recognise legally obtained numbers for hybrid WiFi/GSM provider Truphone at the same time as it was investing in a Jajah, another VoIP product.

The unending creep to wider and wider ranges of content being blocked using more and more intrusive technologies is eroding the openness that gives the Internet its value as a space for innovation and competition, the openness that makes it such a powerful tool for democracy and the openness that is at the centre of its success - and the success of many of your businesses.

***