No magic formula

Index on Censorship
June 2013, vol. 42 no. 2 pp.136–139
http://dx.doi.org/10.1177/0306422013491368

The UK now has an Internet censorship system that is used to address various unlawful use of the Internet, but it was initially restricted to blocking images of child sexual abuse. The system is easy to bypass, but it was hoped to reduce the likelihood of people accidentally accessing such images. At any one time there were only a few hundred web addresses blocked, and all entries were manually checked, so it was rare for material to be incorrectly categorised. However, once the blocking system was in place, there was pressure for its remit to be extended. First, the movie and music industries successfully obtained court orders to add entire websites which facilitated access to copyright infringing material. Now the UK government are proposing censoring legal adult websites too (unless the person who pays for the Internet connection requests an opt-out from the blocking system, and proves their identity and age). The system to block adult material is already in place for customers of mobile Internet connections, but due to the huge number of websites now being blocked, the quality of checking of what belongs on the list has gone down. Websites being incorrectly blocked include political parties, news sites, and sexual education information. Measures that started off as blocking of a small number of carefully selected web addresses containing illegal material universally regarded as abhorrent have morphed into the mass censorship of legal material with little or no human intervention. In the US, Internet users can even be disconnected entirely from the Internet if anyone from their household is too frequently accused of infringing copyright; the UK government is one of several others discussing similar measures.

Blocking child sexual abuse images does not stop the crime, and for the vast majority of other crimes involving the Internet there are no technical measures which can prevent the crime occurring. Therefore the emphasis in legislation has been on detecting and punishing perpetrators in the hope that it will deter others. One area of rapid growth in this field has been Internet surveillance, with the draft Communications Data Bill being the UK government's latest and most privacy-intrusive proposal yet. This law, if enacted, would allow public bodies to order ISPs to record their customers' activities, even when the customer is not suspected of having committed a crime and where there has been no judicial oversight of the order. The costs of implementing this bill would be substantial (very conservatively estimated at £1.8 billion over 10 years) and the purported benefits debatable (the Parliamentary committee investigating the bill described the Home Office's estimates as “fanciful”). If enacted it would also create a chilling effect on freedom of speech. Highly sensitive details of people's lives would be recorded and put at risk of unauthorised disclosure due to failures of computer security, human error, and corruption. Even developing the technology for surveillance is dangerous, as demonstrated by the numerous European companies who designed spy software to fulfil Western governments' needs but then sold the same products on to repressive regimes. The German firm Elaman, even marketed their product as useful for identifying “political

opponents”. Following the toppling of the Gaddafi regime, software from French firm Amesys was discovered to have been used to target journalists and members of the Libyan human rights NGOs. Additionally University of Toronto researchers have discovered that the UK-developed FinFisher surveillance system, which installs software on the targeted computer and monitors the users' activities, was sold to countries including Bahrain, Egypt and Turkmenistan.

The problems are not however limited to legislation that was specifically written with the Internet in mind. In some cases laws are stretched to apply to areas which were not envisaged when written, leading to undesirable implications. One such US law is the Computer Fraud and Abuse Act (CFAA), intended to criminalise hacking, but has been applied to bullying over the Internet and the use of shared passwords. The US Justice Department has interpreted this law as meaning that any violation of the small print on websites could be a crime punishable by up to ten years in prison. The cases to which the CFAA has been applied so far have been serious, but this interpretation grants the state the discretion to prosecute almost anyone they like, and so represents a threat to civil liberties. In the UK, we have seen jail sentences handed down for people making poor jokes online which probably very few people would have seen had the media not drawn them to the public's attention. The Communications Act prohibits the sending of messages which cause offence even if the offended person is not the recipient of the message. Far worse jokes are being made, both over the Internet and in person, but what makes the Internet different is that it's easy for someone who wants to stir up trouble to search for a comment that someone might find offensive and drum up a lynch mob and prosecution. However, progress is being made: two courts have ruled against the Justice Department's interpretation of the CFAA, with one pointing out the result would be an “overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals.” In the UK, the Crown Prosecution Service published guidelines advising against prosecution where communications were not intended for a wide audience, and sets a higher bar for what is considered offensive.

However, the Communications Act and CFAA are two particular examples of a more widespread problem: when activities involve computers things that were legal become illegal and things that were illegal get punished far more harshly than before. There are a number of possible reasons for this trend. One is simply that the people setting and enforcing laws are not familiar with the Internet; their main experience is when it has been abused. To these people the Internet appears to be a strange lawless place which needs to be controlled, not helped by describing the Internet as “cyberspace”. In fact, communications over the Internet are just speech, and need to be protected in the same way that speech is protected over more traditional media. Another reason for harsh punishment is exaggeration and hype, both over how fragile the Internet is and of how much damage can be caused over it. The security industry quotes vast overestimates of the scale of the problem, to encourage people to buy their products. Companies which are subject to attack claim they resulted in huge costs to encourage law enforcement to investigate. But when the numbers actually matter, in legally required disclosures to the Securities and Exchange Commission, out of the top 100 US companies 27 declared that they were attacked

only 1 said that there were “limited losses” with the remainder saying that there was no material impact. Another reason that punishments are harsher for Internet-related crimes are that prosecutions are rare due to the relatively small number of law enforcement personnel dealing with these types of crime, and consequently the sentences for those who are caught get pushed up to provide a deterrent. This doesn't feel fair to those singled out for prosecution, especially as they are often those who were just easy to find rather then the most serious offenders.

There's no magic formula for dealing with Internet related crime; as the examples above show, it is possible to slip up both when drafting laws specifically for the Internet and re-tasking laws written for other purposes. Education, on what the Internet is and how people use it, for policymakers, lawyers, judges and law enforcement will go a long way to correcting some of the imbalances, and digital rights NGOs are helping in this regard. This will encourage a recognition that the protection of speech on the Internet is necessary to consider in the drafting of any law which may restrict it. Greater transparency would also be a benefit. More proportionate actions could be taken if there were better ways to estimate the cost of crime on the Internet, as well as to understand how resilient networks are. Also, transparency on what surveillance equipment is being sold to which countries would encourage ethical behaviour. For example, following disclosures that Nokia-Siemens had sold surveillance software to Iran the company put in place an ethics review process on sales, which resulted in three being cancelled in 2011. In contrast, export control laws have done little to prevent companies from selling surveillance software to repressive regimes, but the added bureaucracy has hindered the distribution of software designed to protect human rights. As is often the case, the way forward in addressing Internet crime, while protecting liberties, is more speech not less – through open consultation with experts, accurate data, and transparency of process.