

# Online Safety

## *Choosing what works*



***The Greens unequivocally support measures that will genuinely protect young people online and combat child pornography.***

We advocate replacing the Government's proposed ISP level filter, which has been sidelined by the Gillard government and formally opposed by the Liberal and National parties, with a range of interlocking measures to strengthen existing cyber safety initiatives and tackle cyber crime, particularly child pornography offences.

The Greens propose an immediate halt to expenditure on implementation of the proposed ISP level filter and diversion of resources to the initiatives outlined below.

The Greens online safety plan will:

- Commit to more systematic research into online risks and effective measures to combat them. We can not intervene effectively before we better understand the complex and rapidly changing nature of the problems faced by Australians online.
- Strengthen our cyber crime law enforcement capability through:
  - Earmarked federal funding to address the under-resourced cyber crime units in the States and Territories;
  - An online single portal for reporting cyber crimes, which will be used to coordinate interstate police responses and generate valuable data on cyber crime.
- Introduce an obligation upon ISPs to offer home-based filtering to their customers. Those who accept will be assisted to activate and customise the filtering capabilities in their operating system, download and configure a free filtering program, or activate the filtering capability of their modem - whatever method best suits their circumstances.
- Strengthen online media literacy programs through schools, universities and public libraries.

### Background

#### ***Funding these initiatives***

The Government has budgeted \$40.8 million over five years to fund its cyber safety initiatives. Before the program was sidelined, an undisclosed proportion of this sum was to go towards implementing the mandatory ISP level filter, with more going to a grants scheme intended

# Online Safety

## *Choosing what works*



to encourage ISPs to offer a broader range of ISP level filtering on a commercial basis. The Greens would not proceed with those two elements of the Government's cyber safety plan.

Since the Government did not disaggregate the \$40.8 million, it is not possible to quantify the savings this would generate. The Greens will advocate in the new Parliament to establish the magnitude of these savings and ensure they are redeployed to the initiatives outlined here.

### ***Targeted research into cyber safety***

There is a demonstrated need for further research into cyber safety, particularly in the Australian context. Understanding and countering threats to cyber safety is not as obvious as it may seem. For instance, the idea of 'grooming' generally conjures up the image of an adult male deceiving a child online, yet we know from international research that grooming is generally perpetrated by other young people<sup>1</sup>.

Australia hosts world-leading research efforts on cyber bullying, a phenomenon frequently topping the list of concerns raised by children and parents when asked to rank online safety concerns. However, a report by the Child Health Promotion Research Centre at Edith Cowan University, commissioned by the Government, found that there are significant and major gaps in most other areas of cyber-safety research, particularly for Australian-based research<sup>2</sup>. This view is supported by submissions to the Parliamentary Joint Committee on Cyber Safety.

Repeated questions in Senate Estimates committee hearings have established that the Government does not have data on the prevalence of accidental exposure to child pornography material, the residence time on the ACMA blacklist of refused classification items, or even the number of websites represented on the blacklist (as opposed to the number of content items).

The mandatory filter debate has seen frequent misuse of the term 'evidence based policy'. The Australian Greens will found all future cyber safety initiatives on the findings of peer-reviewed research, with an emphasis on studies conducted in an Australian context.

### ***Law Enforcement***

The best response to child pornography is to prosecute the offenders. There are many ways in which we could strengthen our cyber crime law enforcement efforts, including:



# Online Safety

## *Choosing what works*

- Targeted federal funding for enhanced cyber crime fighting in the States and Territories. While the Australian Federal Police are relatively well resourced in this area, many of their State and Territory counterparts are not, with some cyber crime units reportedly comprising only a handful of staff.
- 'A single portal for standardised online receipt of cyber crime reports across a wide range of cyber crime types'<sup>3</sup>, as recommended by the House of Representatives Standing Committee on Communications in its recent report on cyber crime in Australia. At present, victims of cyber crime find it difficult to find the right person to handle their complaint, as the crime may involve different parties in different jurisdictions. An electronic, largely automated single point of contact that collected a range of relevant information and generated reports to the relevant State and Territory police would make the reporting process much easier for the complainant, result in much more coordinated cross-jurisdictional action, and generate an invaluable database of the sorts of crimes that are occurring online. This would be useful for all cyber crime, including where a person has information to suggest someone is accessing or distributing child pornography. The UK has a mechanism along these lines that is run at very low cost, given that it is largely an automated online system.

### ***Filtering***

The Greens propose that ISPs be placed under a mandatory obligation to offer filtering to all new customers. Customers would be unable to proceed with using the internet until they nominate whether they wish to filter their internet connection. For those who do, the ISP will assist the customer to activate and customise the filtering capabilities in their operating system, or download and configure a free filtering program, or activate the filtering capability of their ADSL modem. This approach has a number of benefits:

1. PC-based filtering solutions deal with far less traffic, and therefore are likely to have far fewer technical problems than ISP level filters (such as the Government's proposed mandatory filter). In the event that they do malfunction, they only affect the users of the computer in question.

# Online Safety

## *Choosing what works*



2. PC-based filters can be customised to block the content of concern to the household. Most parents do not only want their children to be protected from the narrow range of content on the Refused Classification blacklist. They may also want to shield their children from legal R and X rated material and gambling sites, for example. Many PC-based filters use lists generated by wholesalers who have dedicated staff trawling the internet to find content of concern, whereas the Government's proposed filter that will only suppress a list of 10 000 pages (which may be only a handful of websites) that have been the subject of complaint from the public.

3. Like the Government's proposal, this measure accounts for the risk that some households will be exposed to content of concern because they are unsure how to block it. They will have to make a decision about filtering and receive assistance with set up before they are able to use the internet.

Feedback from the sector has indicated that this approach could be implemented at no cost to the taxpayer and very little cost to ISPs. ISPs that sign up to the Internet Industry Association's code of conduct are already obliged to offer customers filtering solutions. However, more comprehensive consultation should be undertaken prior to implementing this policy to explore whether some small financial assistance may be required for smaller ISPs.

### ***Education and media literacy***

Another critically important area to address if we wish to ensure young people are safe online is education and media literacy. While young people need to be educated in the use and potential of the internet, they must also be made aware of the dangers and strategies for managing them. This should encompass not only the more explicit dangers such as cyber bullying and grooming, but also efforts to exploit young people for commercial purposes through advertising or harvesting their personal information. Young people need to be taught to think critically about what they encounter online.

# Online Safety

## *Choosing what works*



The Safer Internet Group, a coalition of some of Australia's biggest online organisations, recognises this need and advocates 'Properly funding a national comprehensive cyber-safety education program for children and parents on how to avoid inappropriate material and stay safe online'<sup>4</sup>. A stock take of the consistency and adequacy of the online safety and literacy education that is presently being offered throughout Australian schools is a good place to start. The Council of Australian Governments must look at this issue and develop a comprehensive, evidence-based approach that can be implemented in all schools nationwide.

---

1 Review of Existing Australian and International Cyber-Safety Research, Child Health Promotion Research Centre, Edith Cowan University, May 2009, Section 2.

2 Ibid, p.9.

3 Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime, House of Representatives Standing Committee on Communications, June 2010, p.88.

4 <http://www.saferinternetgroup.org/coreprinciples.html>