

Senate Standing Committee on Environment and Communications  
Parliament House  
Canberra ACT 2600

*Via online submission*

10<sup>th</sup> March 2016

**Re: *Inquiry into harm being done to Australian children through access to pornography on the Internet***

Dear Committee Secretary,

Electronic Frontiers Australia (EFA) appreciates the opportunity to provide this submission in relation to this inquiry. EFA's submission is contained in the following pages. EFA is happy to provide further information, if required.

This submission is not confidential and is intended for publication.

#### **About EFA**

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,



Jon Lawrence - Executive Officer  
On behalf of EFA's Policy Committee

## **Inquiry into harm being done to Australian children through access to pornography on the Internet**

### **1. Introduction**

EFA has no particular expertise in relation to the first item in the terms of reference for this inquiry: trends of online consumption of pornography by children and their impact on the development of healthy and respectful relationships.

EFA is concerned that this inquiry, like many before it, is in danger of unnecessarily problematising the ‘online’ element of this issue. To the extent that there is harm being done to Australian children in this context, it is the nature of the content that they may be exposed to, not the communications network itself, that is the cause of that harm.

Pornography and other arguably ‘harmful’ content of course predated the Internet, and while it is undeniable that widespread Internet connectivity massively increases the potential for minors to access such content, an undue focus on the technological context risks an all-too-common mistake of attempting to impose technological solutions in an attempt to address what is, fundamentally, a social issue.

This submission is therefore focused on those areas in which EFA does have expertise, particularly relating to potential technical and regulatory measures that may be considered in an attempt to prevent children from accessing harmful content online.

### **2. Technological Access-Prevention Measures**

EFA has long advocated against the imposition of legislated technological measures that amount to censorship in the name of attempting to restrict the ability of minors to access pornography and other arguably harmful content. The most recent example being the first Rudd government’s attempt to introduce a mandatory Internet filter, which was finally abandoned in November 2012.

EFA remains firmly opposed to such approaches, as they:

- a) are almost always trivial to circumvent for anyone with basic technical knowledge;
- b) inevitably restrict access to entirely legitimate content;
- c) have the potential to harm network performance;
- d) replace parental judgement with bureaucratised or corporate control;
- e) are always subject to scope creep, often very quickly; and,
- f) perhaps most importantly, divert attention and resources away from responses that are likely to be more successful in addressing harm.

#### **2.1 Age Verification**

The Committee will no doubt be aware of a recent proposal from the United Kingdom, which seeks to impose an age verification requirement on sites hosting ‘adult’ content.<sup>1</sup> This proposal is at least in part a response to changes within the online pornography industry which have led to the proliferation of freely-accessible pornography sites – ie those that provide content without the requirement to provide some form of payment, which is in itself a form of age verification.

While such an approach may seem attractive in that it appears to balance the right of adults to access legal ‘adult’ content with the desire to ensure such content is not accessed by minors, this approach has a fundamental flaw.

The proposal assumes that all sites hosting adult content will choose to comply with such a requirement. The reality of course is that such sites are hosted across various jurisdictions, and often choose to host in jurisdictions with particularly strong protections for freedom of expression, or conversely in jurisdictions with particularly loose controls. As such, the likelihood of all sites hosting adult content complying with any such scheme is zero.

Without full compliance, such a scheme is likely to be relatively ineffective in preventing minors from accessing harmful content. In addition, given that those sites that would choose to comply with such a scheme are likely to be among the more ‘responsibly’ managed sites, partial compliance could have the unintended consequence of increasing the likelihood of minors accessing less responsibly-managed sites, therefore putting them at risk of exposure to more extreme content than may otherwise have been the case.

The proposal also raises some alarming privacy issues. It suggests that otherwise ‘free’ sites should require a credit card or other form of payment as a form of age verification. Even if this resulted in only a nominal charge in order to validate the payment method, it would create a record of the fact that an individual visited such a site.

The proposal suggests an alternative method of age verification, namely that the site confirm their age based on their electoral enrolment. This suggestion, if implemented, would result in records being created that link individuals’ personal sexual preferences directly to their electoral enrolment. This has astonishing potential to become a privacy disaster.

In both cases, the potential for real harm to individuals as a result of these records being breached is very real.

## **2.1 Scope creep**

The notion of rapid scope creep in this regard was very clearly demonstrated shortly after the first Rudd government abandoned its mandatory Internet Filter policy in November 2012. At that point, the Communications Minister announced<sup>ii</sup> that he would utilise section 313 of the Telecommunications Act to request Internet Service Provider’s to block sites that appeared on an Interpol-maintained watchlist, said to include the ‘worst of the worst’ of child exploitation material.

Within a few short months, the Australian Securities and Investments Commission (ASIC) decided they would also use this power to request ISPs to block websites alleged to be conducting fraudulent financial schemes. The technical ineptitude involved with ASIC’s requests resulted in over 250,000 legitimate websites, many of them operated by Australian entities, being inadvertently blocked.<sup>iii</sup> This example demonstrates that once mechanisms for filtering are created, they will be used for an increasing range of purposes.

## **2.2 Device-level filtering**

There are many examples of well-developed mechanisms for content filtering at the device-level, such as Apple’s Parental Controls settings for Mac OS X or iOS, similar features for Windows, and

parental controls settings on many home routers. Such device-level filters allow far more sophisticated levels of access control than any centralised filtering scheme or regulation, thereby enabling parents to enforce decisions about their children's internet consumption, such as customised white list, mechanisms for dynamically approving content as children request it, as well as providing control over media purchases such as in-game purchases, and restrictions over time use, among other controls.

EFA believes that device-level filtering is the most appropriate and effective solution to parental management of their children's media consumption. Clearly, this requires that parents are suitably educated and empowered to understand and to manage the use of such tools.

### **3. Education and Parental Empowerment**

EFA is of the firm belief that education and parental empowerment is the most effective method to address the whole range of issues relating to the potential for harm to children online.

It should of course be noted that education and tools to protect children from inappropriate material can never be a 'one size fits all' solution, as would be provided by legislated access-prevention measures. The content appropriate for a 6 year old is of course very different to that for a 16 year old, and parents need to be empowered to make, and to implement, informed decisions about access to content that reflect their personal values.

New adults also do not suddenly switch from a child with restricted access, limited privacy and no sexual agency, to an adult expected to manage their own privacy and suddenly manage their new rights, sexual and otherwise. In contrast, this is of course a transitional process and should involve respect and support for the journey to adulthood with increasing levels of trust and privacy while acknowledging the entirely legitimate emerging interest in sexuality that accompanies adolescence.

### **4. Legal Reform**

EFA believes that Australia should work towards a legal regime that understands and accepts that sexual behaviour will naturally occur in adolescents, while respecting their privacy and protecting them from harassment and inappropriate adult behaviour. In this regard, the Committee should review the Inquiry conducted by the Victorian Law Reform Commission into 'sexting'<sup>iv</sup> and the legislative reforms that have resulted from that. The Committee may also wish to refer to EFA's submission to that Inquiry.<sup>v</sup>

---

<sup>i</sup> <https://www.gov.uk/government/consultations/child-safety-online-age-verification-for-pornography>

<sup>ii</sup> <http://www.abc.net.au/am/content/2012/s3629110.htm>

<sup>iii</sup> See: <https://www.efa.org.au/2013/06/05/asic-blocked-250000-sites/>

<sup>iv</sup> See: <http://www.parliament.vic.gov.au/57th-parliament/lawreform/inquiry/222>

<sup>v</sup> Available at: [http://www.parliament.vic.gov.au/images/stories/committees/lawreform/isexting/subs/S38 -  
\\_Electronic\\_Frontiers\\_Australia.pdf](http://www.parliament.vic.gov.au/images/stories/committees/lawreform/isexting/subs/S38_-_Electronic_Frontiers_Australia.pdf)