



# Response to the Media Development Authority of Singapore's Public Consultation on "Regulatory Options To Facilitate the Adoption Of Internet Parental Controls" ("call")

## Submitted by

Paul Southern  
Principle  
Pasoco Pte Ltd  
paul@pasoco.biz

Friday, May 16, 2014

Version: Final

Status: Submitted to [policy\\_consultations@mda.gov.sg](mailto:policy_consultations@mda.gov.sg)

Distribution: Public

File: IPC\_Consultation-Pasoco-140516

---

The information contained in this document represents the current view of Pasoco Pte Ltd on the issues discussed as of the date of publication. This document is for informational purposes only. PASOCO MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Because of the rapidly changing media industry, Pasoco cannot guarantee the accuracy of any information presented after the date of publication. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Pasoco Pte Ltd. Pasoco may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written agreement from Pasoco, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. ©2014 Pasoco Pte Ltd. All rights reserved. Pasoco is a trademark of Pasoco Pte Ltd in Singapore and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



©2014 Pasoco Pte Ltd. Learn more about Pasoco at [www.pasoco.biz](http://www.pasoco.biz) or contact [anggara@pasoco.biz](mailto:anggara@pasoco.biz).

<b>Contents</b> .....	
<b>Executive Summary</b> .....	<b>4</b>
<b>1 Introduction</b> .....	<b>6</b>
<b>2 Comments</b> .....	<b>7</b>
2.1 General Need for IPCs .....	7
2.2 Response to the MDA’s Specific Questions.....	9
2.3 Recommendations Beyond this Public Consultation .....	12
<b>3 Summary and Conclusions</b> .....	<b>14</b>

## Executive Summary

### Definitions

IASP – Internet Access Service Provider

IPC – Internet Parental Controls

Pasoco's experience in IPCs is derived from the principle's (Paul Southern's) involvement with Microsoft's CETS solution which assisted Law Enforcement Agencies to investigate child pornography crimes, rescue victims and arrest and prosecute perpetrators. As a longterm resident of Singapore, a Boy Scout leader, a school PTA board member and an involved parent, I applaud and thank the MDA's proactive engagement with the public in this area and this call for public consultation.

While the legal and education frameworks appear robust and there exists a plethora of advice the problem is increasing the parent should have the prime responsibility to safeguard the child. An observation of Pasoco is that a large proportion of parents are unaware and shocked at the ease that children can view objectionable / pornographic content through either 'stumble upon' or 'deliberate' behavior.

In response to the MDA's 5 specific questions, Pasoco believes:

- Question #1 – Adoption by Opt-Out in order to (1) be proactive, (2) improve uptake, and (3) align to the principle of secure by default.
- Question #2 – By default (and for free) block (1) Adult/Mature Content/Pornography/Nudity, and (2) Child Pornography at all COPINE/SAP levels.
- Question #3 –
  - If the MDA means the term 'network' to mean IASP/National Network, ie: an IASP or an IASP's provider of network connectivity or the zone where IASPs interconnect – This mode is effective by (1) providing capability across devices, (2) ubiquity across location, and (3) preventing bypass.
  - If the MDA means the term 'network' to mean Home Network', ie: a home's connection to the IASP and the subtending devices – This mode is not effective as it fails to ubiquity across location
- Question #4 – Cost of minimum level free to consumers and encourage upsell of advanced features.
- Question #5 – Technical assistance is required.

Furthermore, Pasoco proposes a visionary solution of centralizing IPCs independent of the IASPs. Pasoco fully realizes this proposal is beyond the scope of this call for public consultation however Pasoco feels strongly for the protection of children from internet perils and believes far more must be done. The advantages of centralizing IPCs are:

- Consumers' choices are broader and independent of their IASP's limited offerings.
- IPC vendors are given an environment where they can compete and promote.
- Larger market size encourages cost-reduced solutions.
- Government oversight thus showing leadership in the protection of the vulnerable.

continued...

For the avoidance of doubt, in order to effectively protect children, these proposed modifications to the Class Licence must be complemented with methods to address:

- Second-hand phones, tablets, etc
- Businesses offering internet connections, eg: WiFi hotspot, gaming café.

In a very high level summary, obligatory internet parental controls (IPCs) are akin to the revised seatbelt law of 2012<sup>1</sup> - both are a commonsensical measure to protect the most vulnerable (the child) because sadly some parents don't. In closing Pasoco is willing to support the MDA (or more generally the Singapore government) in the area IPCs and internet governance.

---

<sup>1</sup> Refer to Singapore Statute: Road Traffic (Motor Vehicles, Wearing of Seat Belts) Rules 2011

## 1 Introduction

Pasoco Pte Ltd is a privately-held Singaporean company engaged with innovation in the internet, media and privacy area and primarily offering consultancy services to government, enterprise and NGOs.

Pasoco's experience in Internet Parental Control (IPC) is derived from the owner's (Paul Southern's) involvement with Microsoft's CETS solution. CETS – Child Exploitation and Tracking System – was a goodwill/CSR initiative of Microsoft Corporation to assist Law Enforcement Agencies (LEAs) to investigate child pornography crimes, rescue victims and arrest and prosecute perpetrators, all within a trust framework that protected witnesses, evidence and the autonomy of the LEAs. CETS also automated much of image correlation improving accuracy and speed and not subjecting investigators to the ordeal of manual visual correlation. As a Boy Scout leader, a school PTA board member, an involved parent and an IT buff, Southern has sought to apply solutions for the protection of the vulnerable inside and outside his home.

The following are Pasoco's comments on

- The situation and the need for IPCs in general (section 2.1)
- Response to the MDA's Specific Questions (section 2.2)
- Proposals Beyond this Public Consultation (section 2.3)

## 2 Comments

### 2.1 General Need for IPCs

The purpose of this section is to provide background and context for the need for IPCs in general and opine on some of the factors which have resulted in the current low uptake.

#### 2.1.1 Legal and Education Framework

Overall, Singapore's legal framework for the protection of society and the engagement of the public appear robust, pragmatic and appropriate. The Media Literacy Council<sup>2</sup> and the Inter-Ministry Cyber Wellness Steering Committee (ICSC) are evidence of this.

Singaporeans are not only IT-savvy, as evidenced by smartphone penetration, but take good and appropriate steps to protect themselves online as evidenced in Microsoft's Computing Safety Index<sup>3</sup>. Singaporean children appear to be well educated in online safety matters various means and especially through the MOE's Baseline ICT Standards for Cyber Wellness Skills and Values<sup>4</sup>.

#### 2.1.2 The Duty of the Parent

Under most countries' law, including Singapore's, parents have a statutory responsibility to protect the welfare of their children and a broader duty of care to protect all children, to the extent that that protection is deemed a right<sup>5</sup>. To meet that responsibility, parents, depending on the age/maturity of the child, must protect and/or teach the child of risks in society, online being just one society. A perpetual debate is the extent of the responsibility and what is deemed a threat to a child varies immensely by culture and by individuals; views on Internet Parental Controls are no exception<sup>6</sup>.

Other entities may supplement that protection/teaching but parents must not ever ambiguously outsource that responsibility to external parties to the school or otherwise<sup>7</sup>. Too often this is the case. To exacerbate this risk, in Singapore and many other countries, the ambiguity exists inside the home where the parent is less present and a grandparent or a foreign domestic worker (FDW) is effectively in-charge. It is not difficult to conclude that those less experienced with the internet and its risks are less capable to protecting/teaching. At a very

---

<sup>2</sup> See <http://www.medialiteracycouncil.sg>

<sup>3</sup> In Microsoft's 2012 Computing Safety Index, Singapore scored top of the 20 countries surveyed and the 2012 Mobile Safety Index Singapore scored 3rd place. In Microsoft's 2013 survey, while declining slightly, Singapore maintained a high rating. See <http://www.microsoft.com/security/resources/mcsi.aspx>

<sup>4</sup> See <http://ict.moe.edu.sg/baseline/cyberwellnessskills.html>

<sup>5</sup> Reference the United Nations' Universal Declaration of Human Rights and the Convention on the Rights of the Child.

<sup>6</sup> See Journal of Computers and Education, Internet Use and Parental Mediation: A Cross Cultural Study, Morentin et al, volume 70, 2014, p.221-221.

<sup>7</sup> For example religious organizations, NGO's, governments, community organizations, kindly enterprises, etc

minimum, the education must instill the rules of where the internet-enabled devices are used, when and how much they are used, under what conditions and what they can do or cannot do.

Simply stated, parents and all others effectively in-charge of children need greater education and tools.

### **2.1.3 IASPs offering IPCs**

There are pros and cons of IASPs offering IPCs. As the MDA noted, in Singapore where IASPs do so, the results have been less than desired.

Two inherent problems with IASPs offering IPCs:

1. Firstly, IPCs are not a core offering of IASPs and there seems to be little incentive to drive user uptake. In Pasoco's short survey of two of the main three IASPs' IPC offerings last week, in one case the call-center agent had no information and failed to provide so later in spite of promising to do so and in other case their webpage had broken links. To further lend credence to this opinion, one will notice each IASP chose to offer a single vendor's solution. While complying with the Act the IASPs offer little choice or flexibility to the end-user as there is simply no incentive to do so.
2. Secondly, amongst the public, there is often a latent distrust of IASPs due to their profit-seeking motivation, complicated contracts and inability for consumers to buy-and-try. Out of this distrust, there is likely a lower uptake of IPCs.

While there are inherent problems with IASPs offering IPCs, Gartner reports<sup>8</sup> that consumers' perceived value of IPCs provides the IASPs a premium revenue opportunity. It would be advantageous to study the implementations of British Telecom's Parental Controls and other jurisdictions where IPCs were moved from optional to Opt-Out.

### **2.1.4 A Plethora of Advice**

There is a plethora of parental education material coming from such parties as software vendors, IASPs, community organizations, NGOs, governments, industry bodies and more. One can reasonably assume that advice and the presence of educational material is not an issue. One could opine that this abundant supply in fact leads to choice fatigue.

---

<sup>8</sup> See Gartner's report Value-Based Pricing Strategies Help CSPs Drive Brand Loyalty and Revenue Growth, Published: 21 March 2014, ID:G0026340'



### 2.1.5 The Problem is Increasing

When the initial suite of IPCs were introduced – for example Net Nanny in 1995 – there were only 2 devices to support: Windows and Apple. The world is vastly more complex now with multiple operating systems ranging from Linux, Android, iOS, Windows RT and Windows Mobile and multiple proprietary systems that can access the internet, including for example gaming devices/consoles, OTT/zapper boxes, eReaders, etc. Access too has broadened from FBO offerings of DSL/fiber and 3G/LTE to WiFi in cafes, schools, and as universally offered via Wireless@SG. Adding to the complexity are VPNs and anonymizers.

It is important to note that solutions must address the following 2 behaviors of children:

- The stumble-upon behavior where a legitimate search (for example) returns objectionable content.<sup>9</sup>
- The deliberate behavior of seeking objectionable content.

In summary, while the legal and education frameworks appear robust and there exists a plethora of advice the problem is increasing the parent should have the prime responsibility to safeguard the child.

## 2.2 Response to the MDA's Specific Questions

Pasoco's responses to the MDA's specific questions are as follows:

### 2.2.1 Question #1 – Adoption by Inform and Offer, Required Decision or Opt-Out

While the MDA recommends Required Decision, Pasoco recommends Opt-Out. This is a proactive measure that prevents non-use of IPCs due to forgetfulness, laziness, analysis paralysis, procrastination, fear, transfer/delegation, confusion and other human-factors.

Reference also (1) the famous Microsoft whitepaper<sup>10</sup> on Trustworthy Computing which inter alia set a goal of "Secure by Default" and (2) the Privacy by Design foundational principle<sup>11</sup> #1 of "Proactive not Reactive; Preventative not Remedial".

Skeptics often cite Opt-Out as onerous however Opting-Out is a commonplace action. The trouble is commercial law and transparency; one can understand the IASPs reluctance to implement Opt-Out after the "missed-call service for roaming subscribers" criticism by the Consumers Association of Singapore (CASE) in 2004<sup>12</sup>. With better transparency the problem could be alleviated.

---

<sup>9</sup> For example, the social-network "Edmodo" used by educational institutes can be misspelled as "Edmondo" which is/was a pornography site or a seemingly innocuous search term could also be slang for genitalia or sexual activity.

<sup>10</sup> See [http://download.microsoft.com/download/a/f/2/af22fd56-7f19-47aa-8167-4b1d73cd3c57/twc\\_mundie.doc](http://download.microsoft.com/download/a/f/2/af22fd56-7f19-47aa-8167-4b1d73cd3c57/twc_mundie.doc)

<sup>11</sup> See <http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/>

<sup>12</sup> See CASE's monthly journal C@SEBites issue 28.

## 2.2.2 Question #2 – The categories of content that should be filtered by default, when the Internet parental controls are switched on.

Pasoco recommends the following content categories should be filtered by default:

1. Adult/Mature Content/Pornography/Nudity
2. Child Pornography --- It is strange that “Child Pornography” even appears on the list given Singapore’s accession in 1995 of the United Nations Convention on the Rights of the Child (UNCRC). In any case, using the COPINE and SAP<sup>13</sup> scales, Pasoco believes all levels (including level 1 in both scales) should be blocked
3. Intimate Apparel/Swimsuit --- Refer to COPINE/SAP guidelines. If the model is a child, intimate apparel should always be blocked and ‘swimsuit’ may or not need to be blocked.

## 2.2.3 Question #3 – The mode by which the content is filtered, i.e. whether at network level or device level.

The MDA’s call, section 3.3.1 states:

*Internet parental controls can be deployed either at the network or at the device level. At the network level, content is filtered as long as the Internet connection is via the network or gateway belonging to the particular IASP that the consumer is subscribed to. There is typically no need for any installation of applications or software onto devices. To illustrate, if a household subscribes to network level Internet parental controls for both their home and mobile broadband Internet plans, all devices with Internet access capabilities will have filtered content if Internet access is via the subscribed networks. However, if the device taps on an alternative third-party network such as the public wifi, the content will no longer be filtered.*

However, the term ‘network’ (and ‘network level’) can mean both the following:

1. An IASP or an IASP’s provider of network connectivity or the zone where IASPs interconnect, hereafter called IASP/National Network.
2. A home’s connection to the IASP and the subtending devices, hereafter called Home Network.

Both these terms make sense grammatically and in context but these terms are very different and have very significant differences in how one would interpret this question and the MDA’s recommendation. In normal use, ‘network’ commonly means the former whereas the latter normally requires the adjective ‘home’.

Due to ambiguity in the MDA’s call, I will answer this question using both possible meanings. However, regardless of meaning, the following are problems of device-level:

- There are a plethora of devices, many of which don’t have IPC applications or, if they have an IPC application, it is a separate application with different control and management functions from the other devices. This then means multiple learnings, subscriptions and support arrangements.

---

<sup>13</sup> See the UK’s Sexual Offences Guideline Consultation, page 79 at [http://sentencingcouncil.judiciary.gov.uk/docs/sexual\\_offences\\_consultation\\_guideline\\_%28web%29.pdf](http://sentencingcouncil.judiciary.gov.uk/docs/sexual_offences_consultation_guideline_%28web%29.pdf)

© Pasoco Pte Ltd

- Easier bypassing methods of a device (eg: changing a SIM card on a mobile, rooting and hack exploitation). It is very easy to find these 'solutions' on the internet and/or find a vendor (or a tech-savvy friend) who can do this for you.
- The move to IPV6 exacerbates the problem with increased devices.

**If the MDA means the term 'network' to mean IASP/National Network, ie: an IASP or an IASP's provider of network connectivity or the zone where IASPs interconnect:**

IASP/National Network-level (versus both Home Network-level and device-level) addresses the solution far better by the following:

- Ubiquity across all devices, including second-hand devices (which have large uptake by children/youth).
- Ubiquity across all access points, eg: a parent doesn't need to be concerned with their child when it visits a friend's home or use Wireless@SG.
- Frustrating bypass methods, eg: anonymize, VPN, SSL, SIM card replacement, direct IP address, caching, proxy servers, etc;

IASP/National Network -level also provides the following advantages:

- The ability to address the AGC's proposal to block sites that infringe copyright.
- The maintenance of the MDA's blacklist.

**If the MDA means the term 'network' to mean Home Network', ie: a home's connection to the IASP and the subtending devices:**

The Home Network-level is a simple and cost-effective solution for the IASP, however, since Home Network-level fails to provide a solution on alternate access points, eg: a friend's house, a public WiFi spot, Wireless@SG, etc, it has very little real value and should not be considered. Moreover, unless these failures are very explicitly explained to the subscriber, the subscriber could easily infer that this mode provided good/ubiquitous protection.

**2.2.4 Question #4 – The cost to consumers for subscribing to Internet parental controls, as part of the subscription to any Internet access package.**

If the IPC were offered directly by the IASP, then Pasoco proposes that the costs for basic IPC be included in the bundle and inseparable if opted-out of. This cost is negligible – at approximately a dollar a month. One would abhor a parent not protecting their child in order to save that negligible amount.

Pasoco proposes too that the IPC offer premium plans where they could upsell device/user-tailored features, such as:

- Additional categories to block, eg: social networks.
- Port blocking, eg: applications, communications.
- Time-based restrictions, eg: time of day, day of week, hours per day or week, etc

- Application/origin-based restrictions, eg: gaming site, downloads, eg: YouTube, Youku.

### **2.2.5 Question #5 – The provision of technical assistance to consumers who want Internet parental controls.**

The entity offering the IPC must offer some basic technical assistance. However, in-depth assistance could be provided by the manufacturer or distributor as is the case for example of Malifax providing consumer support to SingTel’s DSL subscribers who use 2Wire residential gateways.

## **2.3 Recommendations Beyond this Public Consultation**

Given the afore-mentioned risks/concerns:

- Low uptake of IPC services to date<sup>14</sup>
- The duty of the parent and ambiguity of who’s in charge
- IASPs offering IPCs and low incentive
- The increased problem and increased methods to bypass controls

Pasoco proposes improved education and a visionary solution of centralizing IPCs independent of the IASPs. Pasoco fully realizes this proposal is beyond the scope of this call for public consultation however Pasoco feels strongly for the protection of children from internet perils and believes far more must be done.

### **2.3.1 Recommendation #1 – Improved education**

Education should be improved in the following areas:

- Start with awareness<sup>15</sup>
- Target of education specifically children, parents and caregivers (grandparents, FDWs).
- Depth of education to include “How to’s” and greater illustration of perils.
- Reach of education to include print media in, for example, public transport and video pre-rolls in cinemas (in addition to the existing Cyberwellness programs).
- Mandatory training for FDWs who care for children.
- Community Centre-based training for grandparents and FDWs.

### **2.3.2 Recommendation #2 – Centralized IPC administration**

Whilst the MDA’s public consultation is for FBOs, Pasoco believes there are several strong advantages of implementing a centralized IPC administration. For example:

---

<sup>14</sup> See the Public Consultation paper, sec 1.3.

<sup>15</sup> Pasoco’s survey showed little awareness of the ease that children can view objectionable / pornographic content through either ‘stumble upon’ or ‘deliberate’ behavior as described in section 2.1.5. In Pasoco’s observations of 10 supposedly concerned parents, 4 parents expressed shock at that ease.

© Pasoco Pte Ltd

- IPC is ubiquitous across access point, including public WiFi.
- Several IPC vendors could be offered (since the current method provides no incentive for IASPs to offer more than one vendor).
- When a consumer changes IASP vendor they can continue with their current IPC as opposed to starting afresh with a new system. (Like mobile number portability)
- Addresses domestic roaming on mobiles.
- Greater ability to showcase IPC solutions side-by-side and comparison shop.
- Greater buying power, thus cost-reduced solution.
- Vendors have greater potential market size and thus more interested to offer and do so at greater promotion.
- Government oversight on vendor selection.
- Common technical support.
- Ability to signup with the vendor directly – thus the vendor can promote. (Currently, in a reseller model, the vendor has no incentive to promote as the IASP doesn't pass the reduction onto the consumer.)
- Government leadership and incentive to encourage uptake. (For example, the IDA's iExperience Centre in the linkway between Suntec City and Raffles City.)
- Upsell of services through higher-valued services via implementation of PCRF – Policy & Charging Rules Function.
- Compliance assured through PCEF – Policy Control Enforcement Function.

A centralized IPC method is closely aligned to the mode of IASP/National Network-level for which solutions are available, eg: the Netsweeper<sup>16</sup> product. Such an IASP/National Network-level mode would offer the minimum level blocking and be complemented with device-level solutions that offer the advanced features such as history reporting, payload/content reporting, time-based controls, on-the-fly configuration, etc...

---

<sup>16</sup> Pasoco has no relationship with Netsweeper and simply uses this vendor as an example.

### 3 Summary and Conclusions

While the legal and education frameworks appear robust and there exists a plethora of advice the problem is increasing the parent should have the prime responsibility to safeguard the child.

In response to the MDA's 5 specific questions, Pasoco believes:

- Question #1 – Adoption by Opt-Out in order to (1) be proactive, (2) improve uptake, and (3) align to the principle of secure by default.
- Question #2 – By default (and for free) block (1) Adult/Mature Content/Pornography/Nudity, and (2) Child Pornography at all COPINE/SAP levels.
- Question #3 –
  - If the MDA means the term 'network' to mean IASP/National Network, ie: an IASP or an IASP's provider of network connectivity or the zone where IASPs interconnect – This mode is effective by (1) providing capability across devices, (2) ubiquity across location, and (3) preventing bypass.
  - If the MDA means the term 'network' to mean Home Network', ie: a home's connection to the IASP and the subtending devices – This mode is not effective as it fails to provide ubiquity across location.
- Question #4 – Cost of minimum level free to consumers and encourage upsell of advanced features.
- Question #5 – Technical assistance is required.

Furthermore, Pasoco proposes a visionary solution of centralizing IPCs independent of the IASPs. Pasoco fully realizes this proposal is beyond the scope of this call for public consultation however Pasoco feels strongly for the protection of children from internet perils and believes far more must be done. The advantages of centralizing IPCs are:

- Consumers' choices are broader and independent of their IASP's limited offerings.
- IPC vendors are given an environment where they can compete and promote.
- Larger market size encourages cost-reduced solutions.
- Government oversight thus showing leadership in the protection of the vulnerable.

For the avoidance of doubt, in order to effectively protect children, these proposed modifications to the Class Licence must be complemented with methods to address:

- Second-hand phones, tablets, etc
- Businesses offering internet connections, eg: WiFi hotspot, gaming café.

In a very high level summary, obligatory internet parental controls (IPCs) are akin to the revised seatbelt law of 2012<sup>17</sup> - both are a commonsensical measure to protect the most vulnerable (the child) because sadly some parents don't. In closing Pasoco is willing to support the MDA (or more generally the Singapore government) in the area IPCs and internet governance

---

<sup>17</sup> Refer to Singapore Statute: Road Traffic (Motor Vehicles, Wearing of Seat Belts) Rules 2011

© Pasoco Pte Ltd

-- end of document --