REGULATORY OPTIONS TO FACILITATE THE ADOPTION OF INTERNET PARENTAL CONTROLS

PUBLIC CONSULTATION

RESPONSE FROM NETSWEEPER INC

16 May 2014

Netsweeper Inc.
104 Dawson Road Suite 100
Guelph, Ontario, N1H 1A7
Canada

Please direct all enquiries to:
Hisyam Halim
Sales Director, APAC
Mobile: +60 12 2733 464
Email: hisyam.halim@netsweeper.com

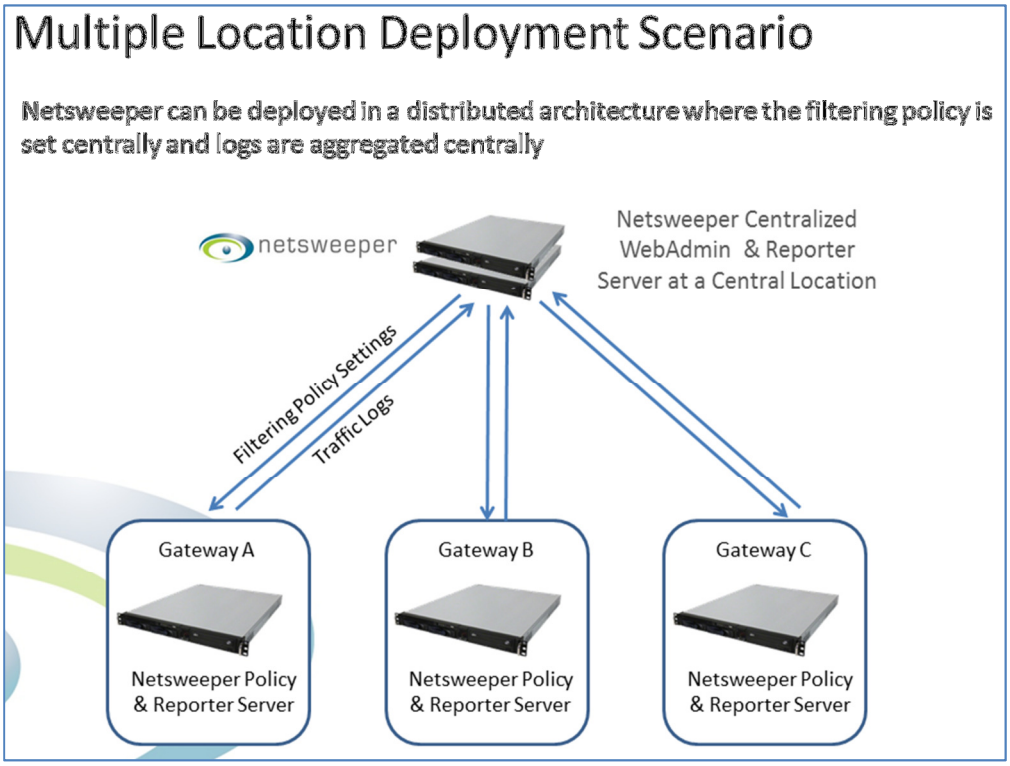
INTRODUCTION

1. Netsweeper is a global performance leader in web filtering for large networks. Our solution is used by service providers for the purpose of complying with regulator's filtering requirement and as a value added service (VAS) such as parental controls and filtering.

2. Mobile operators & fixed-line ISPs use Netsweeper to offer a parental control service where the parents can chose the filtering policy for their child's mobile number and their home routers. The parents can choose to block different categories for different mobile number or home routers and enforce them at different times.

3. Netsweeper is filtering more than 400 million internet users in service providers worldwide. This gives us an unassailable advantage in creating the largest & most dynamic real-time database of URLs in the world. Currently our database size is 6 billion URLs and we scan & categorize 20 million new URLs every day.

4. With Netsweeper's distributed architecture, our solution is also used for nationwide filtering where the Netsweeper Policy Servers are located at multiple gateways to enforce filtering based on the policy set centrally by the Netsweeper WebAdmin Server located at the regulator's data centre. Traffic reports will be aggregated at the central location to get a complete picture of the internet activity. This can be used to filter access to sites and URLs not allowed by the regulator and enforcement of polices on online gambling and e-commerce.



RESPONSE TO PART 2

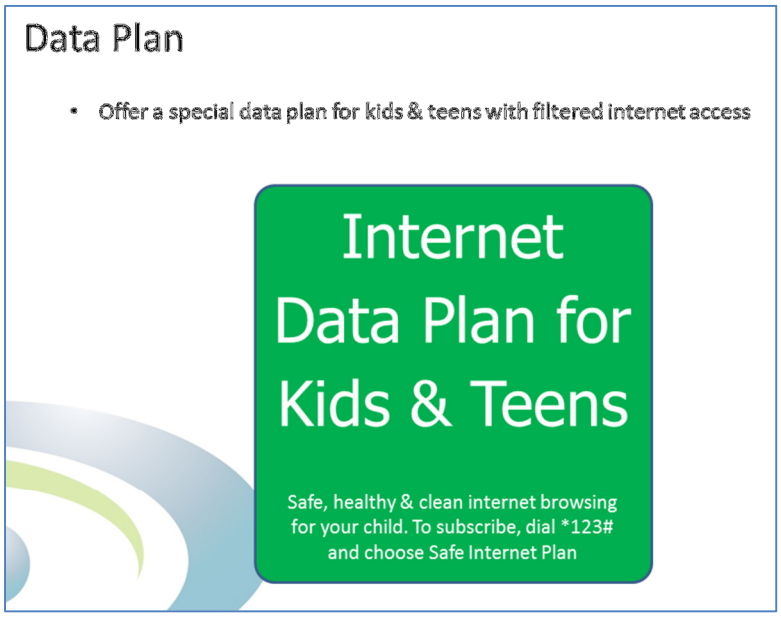
5. In response to Part 2 of your paper, we agree with your recommendation to require the consumer to make an explicit decision upon subscription and renewal of the internet access service.

6. For new subscription, this could be done via a form or verbal instruction as mentioned in your paper. For purchase of a new prepaid SIM card, the vendor will have to ask the question & record the decision in the registration system provided by the mobile operators.

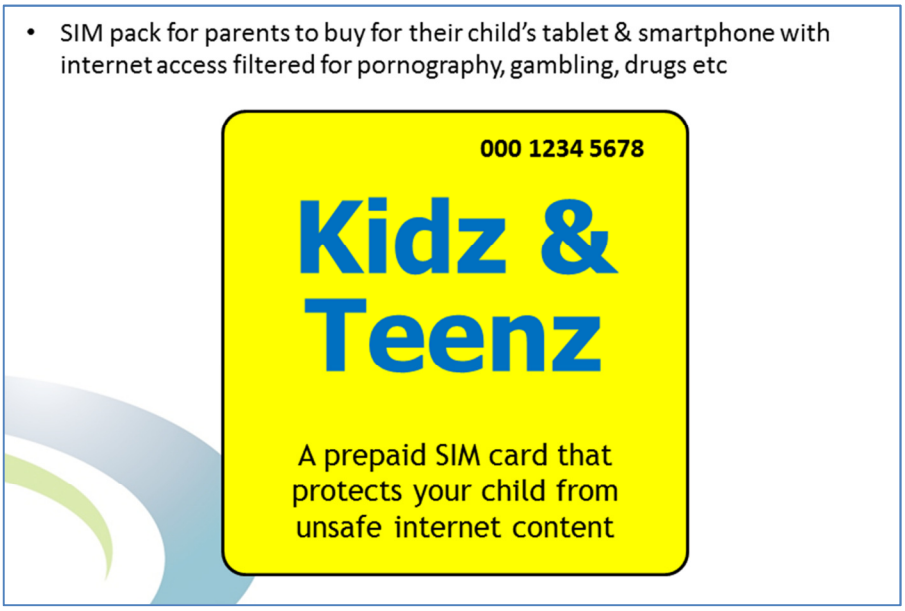
7. It is a bigger challenge to get the consumer to make the explicit decision for existing customer since typically there is no renewal process for subscription of fixed line or mobile internet access. As a regulator, you can mandate the service providers to make a call to each subscriber to ask the question on filtering and record their answer as what has been done in the UK since early this year for broadband customers.

8. Calling each subscriber for a decision should be effective for fixed line internet access since the phone number on record belongs to the parent or guardian of the household. However for prepaid mobile consumers, the number called may be in the custody of the child and they may not pass the phone to their parents & guardian to make the decision on filtering.

9. As an addition to the calling exercise, the mobile operators can create a special mobile internet plan for kids & teens that they can promote to the parents. This plan comes with filtered internet access where pre-selected categories have been selected to filter such as pornography, drug abuse, gambling etc. In the marketing promotions & material, the mobile operators can encourage the parents to sign up their children's mobile number to use the special mobile internet plan for kids & teens. This has a simple message to the parents to take action compared to asking them to activate the parental control service.



10. To send a simpler message to the consumer, the mobile operators can go one step further by introducing a new prepaid SIM pack for kids with filtered internet access. This is ideal for parents who want to buy the first internet connected smartphone or tablet for their children. Web browsing with this SIM card will be filtered for pornography and other inappropriate and there will be no settings required or needed to activate or deactivate the service.



11. These are ideas and suggestions based on our observation in promoting parental control services in markets that we operate.

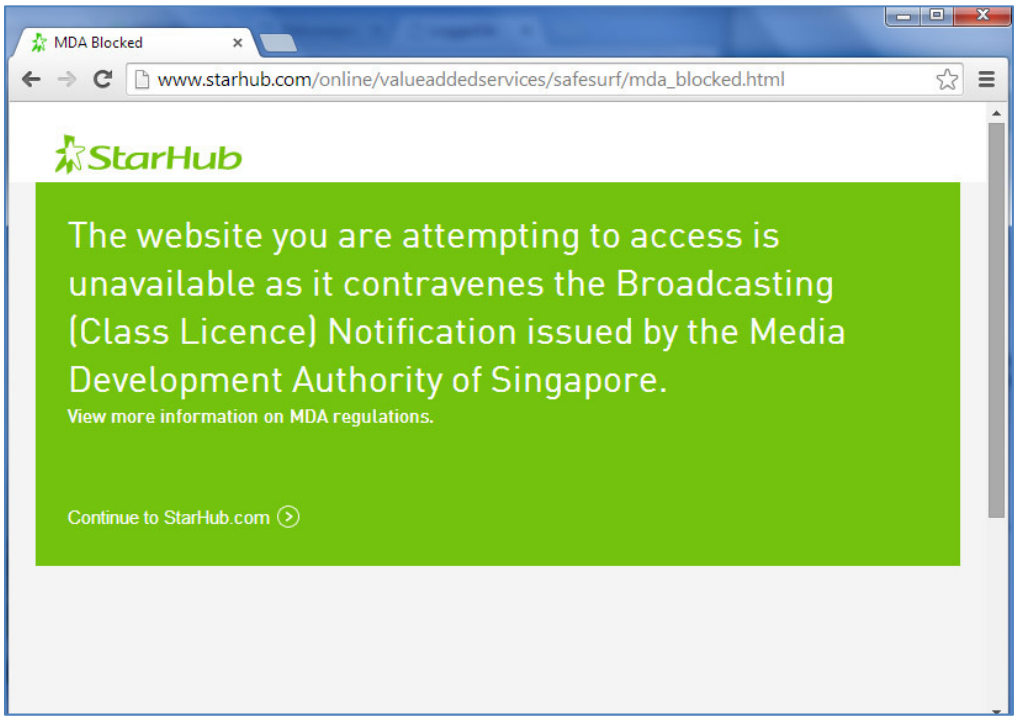
RESPONSE TO PART 3

12. In response to Part 3 of your paper, since we are a vendor of filtering solution we will respond to the question of the mode of where the content is filtered. The other questions are more relevant to the consumers and parents in Singapore.

13. We agree with MDA's recommendation in requiring the IASP to have a network level filtering solution as opposed to a device level solution. This facilitates adoption of the service by concerned parents due to simpler activation as compared to installation of applications in devices such as internet filtering services offered by M1 (https://www.m1.com.sg/Personal/Add-onServices/InternetFiltering).

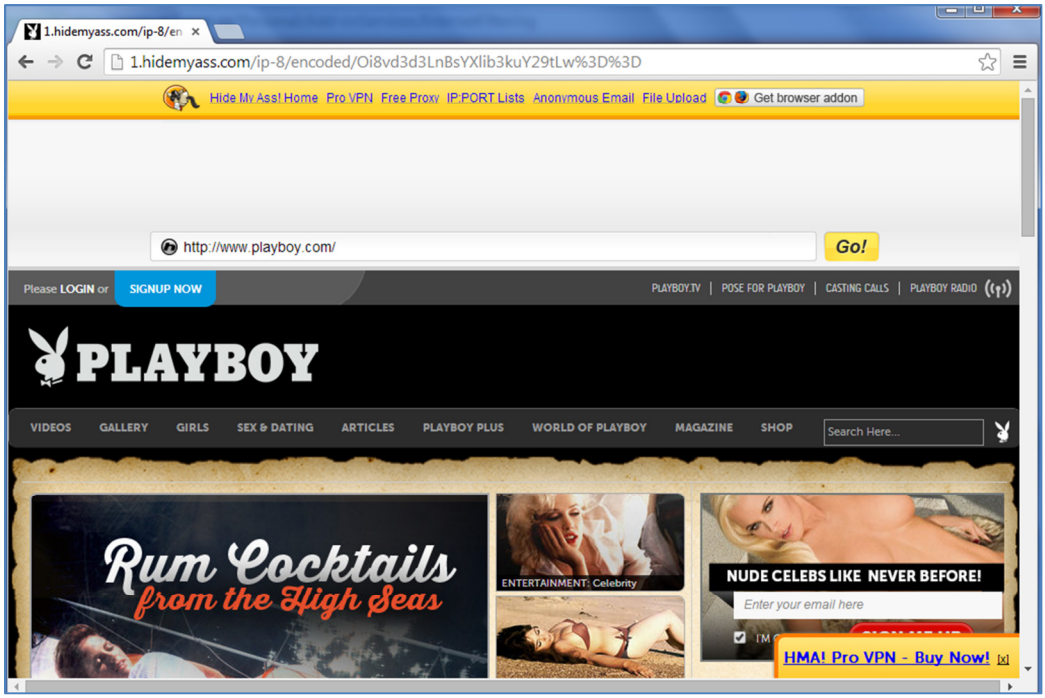
14. However there are several methods of web filtering at the network level. We noticed that the network based filtering offered by StarHub (SafeSearch) and Singtel (Mobile Internet Filter) uses the DNS-based filtering method.

15. DNS or Domain Name System is a system that translates a domain name such as www.playboy.com to an IP address such as 1.2.3.4 for the web browser to request the content from. A DNS based filtering system that wants to block www.playboy.com basically gives a different IP address than the actual one, for example giving the IP address that directs the web browser to a deny page such as shown below.



16. This type of filtering can easily be bypassed by using a proxy to route the web request. A user can use web based proxy such as www.hidemyass.com or key-in a proxy server address in the

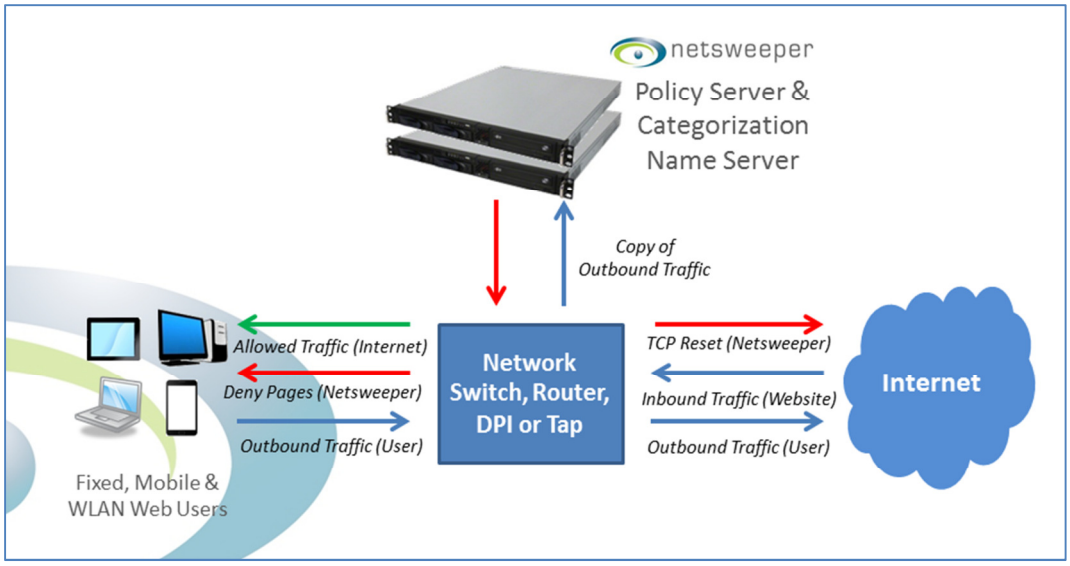
web browser settings or use a browser extension like getgom.com to route the web requests through the proxy instead of the actual destination as shown below.



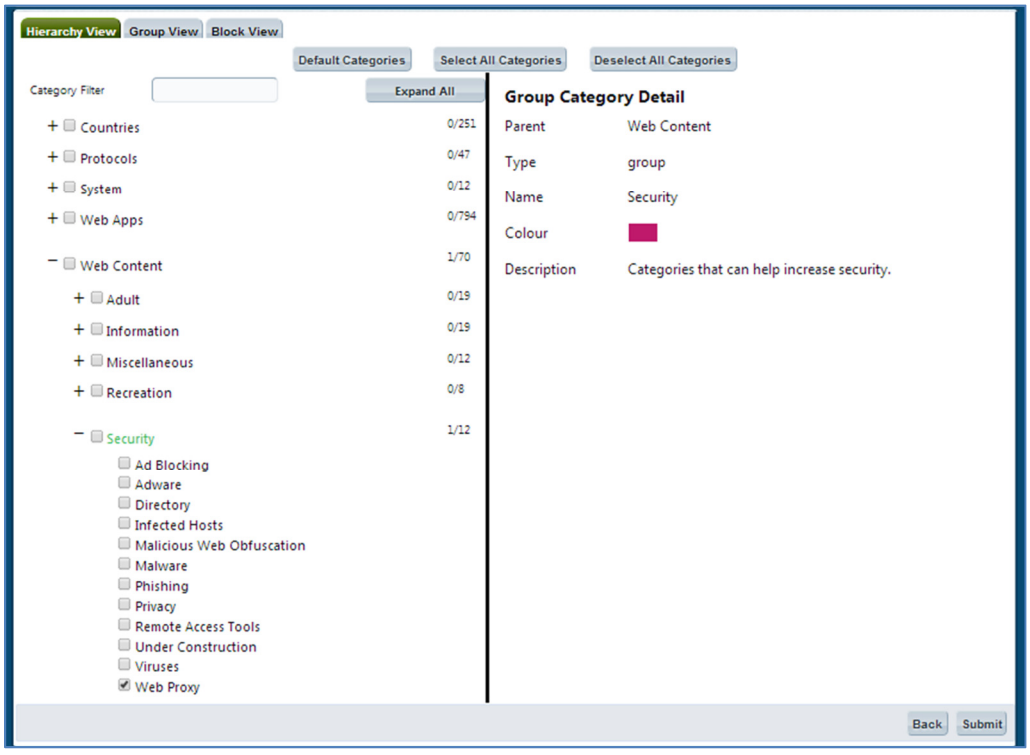
17. Netsweeper performs filtering in a more effective & granular way. In a service provider environment Netsweeper is deployed in a port-mirror mode where Netsweeper will inspect every web request being made in the network and filter according to the policy set by the service provider. This means Netsweeper can filter a specific URL or a webpage instead of the whole website such as using the DNS based filtering method. For example, Netsweeper can filter a specific webpage at CNN.com instead of blocking the whole website.

18. When a user makes a web request, the traffic will go through the network of the service provider where a network device makes a copy of the request and send it to Netsweeper. The original traffic is not interrupted and is not slowed down by this process making Netsweeper effective in filtering large networks without any latency.

19. The Netsweeper system inspects the traffic and destination web address and decides to filter or not based on the policy set for the user. Netsweeper can filter based on a list added to the system or categories selected by the operator such as pornography, gambling etc. If the traffic is allowed, Netsweeper does not perform any action. If the traffic is not allowed, Netsweeper will send a deny packet to the user to perform a deny action such as redirecting to a deny web page or send an error message such as HTTP 404 message. At the same time Netsweeper will send a stop message (TCP reset) to the webserver to stop it from sending the content to the user.



20. The Netsweeper system is able to prevent bypass by using proxies because it can filter access to web proxies. Every day, Netsweeper detects 40,000 new web proxies and adds them into the URL database. The operator can simply prevent the use of web proxies by selecting to filter the category web proxy (see below).



Category to filter in Netsweeper

21. Another consideration when comparing web filtering system is the size and relevance of the URL database. Since Netsweeper scan & categorize 20 million new URLs daily, from inspecting traffic of 400 million internet users worldwide, we detect the latest web content that exists on the

internet; be it pornography, gambling or malware& phishing web sites. Our database of 6 billion URL is constantly refreshed where the URLs for certain categories such as virus and phishing would have a shorter period (time to live) to remain in the database before being deleted, due to their temporary nature. This ensures our database remains current and relevant and only contains URL that still exists on the internet.

CONCLUSION

22. We would like to conclude by stating that the MDA is on the right path in encouraging the adoption of parental control services by parents in Singapore. However the service providers have to play a larger role in promoting the service in a simpler manner and implement a filtering system that can't simply be bypassed by an average Singaporean child.

23. As a suggestion, MDA can consider specifying a minimum technical requirement for a network based filtering solution in MDA's policy. The technical requirement may mention that the solution implemented by the service providers must be able to prevent bypass with web proxies in order to achieve the objective of a parental control service i.e. effectively protecting the children from inappropriate and unhealthy internet content.