TRAFFIC MANAGEMENT AND 'NET NEUTRALITY'; Response by Brilliant Digital Entertainment to the Ofcom Discussion Document.

Introduction

Brilliant Digital Entertainment (BDE) is pleased to be able to provide a response to the Ofcom Discussion Document 'Traffic Management and 'net neutrality' (Discussion Document).

Brilliant Digital Entertainment Pty. Ltd. (BDE) is a content management business and its related entities are engaged in search engine optimisation, on-line music subscription services, web development, software development and technology research and development. BDE operates a technology business incubator from its offices and its principals are long term participants in the development of businesses related to the internet and digital technologies.

BDE's principals also have considerable experience in the commercialization of global P2P customer platforms and their prosecution. Our businesses and experience make us uniquely placed to respond to the Discussion Document.

BDE would in particular like to respond in brief to the following question;

> *Question (iii) Can you provide any evidence of economic and or consumer value generated by traffic management?*

We would however also like to make some comments about the role of Search Engines in the 'Net Neutrality' discourse. Given the critical role that Search Engines play in the operation of the internet, the expenditure of internet resources, the almost complete absence of investment in the architecture of the internet and the role they play as leading proponents of unfettered 'net neutrality' the absence of any reference to them in the Discussion Paper questions should be of concern.

Question (iii) Can you provide any evidence of economic and or consumer value generated by traffic management?

Background

The internet is often thought of as some ontologically distinct place, an infinite space – a cyberspace. It is in fact a finite resource, a machine or a vast array of machines that are inter-connected. At best the internet is a hyper spatial machine but one that has a clearly limited capacity.

The Discussion paper speaks of surging consumer demand for internet access; ever increasing data pay loads (as customers shift to video or

entertainment related protocols) and increasing global usage of the internet as the drivers of ISP traffic management activity.

We propose that the shift to traffic management has more obvious drivers, ones that drive all responsible businesses and community members in the ordinary course of their lives and businesses. We do not propose to dwell on them or refer to them comprehensively as they are well documented but ask that Ofcom take the time to consider these matters;

1. The architecture of the internet has clearly definable limits. With only 30% of the world's population currently accessing the internet, the surge in data being trafficked combined with the vast number of people yet to access the internet means that it is likely internet demand will outstrip supply in the foreseeable future. Traffic management will become inevitable even if it starts by only ridding the internet of data which is obviously illegal in any event.

2. Much of the hardware that makes up the Internet's architecture has reached its natural energy thresh hold. This means that amongst other things much greater energy usage will be required to maintain the internet as its machinery moves from air cooled to refrigerated and the efficiency of the energy expended will beyond a certain traffic level/speed be insufficient to maintain quality of experience and service delivery.

3. Despite the rhetoric from sectional interests there are torrents of obviously illegal data being trafficked across the internet. That illegal traffic can not for much longer get a free pass simply because the work 'internet' is added to the crime's description. This illegal traffic in a 'net neutral' environment is subsidized or sponsored by ISP customers – hardly a good policy outcome and indeed one that would be repugnant to the public at large. Furthermore dealing with this illegal traffic is necessary in building a sustainable social platform.

4. It makes no economic sense to invest in the development of a customer base and not serve them. It makes less economic sense to create a customer base and then let the whole of the market place use your customers and your resources to provide them with services you could provide more directly/quickly/conveniently and at a shorter haul, thereby expending less of the internet's resources.

5. The carbon footprint of the internet industries is on the increase. As the internet population increases and usage per customer increases unfettered energy use will dramatically increase the harm the industry does to the environment.

6. As internet usage per customer increases and the competition to provide internet access increases the market will reach a point where the commercial incentive to enter the internet service provider industry will disappear. ISP's will need to manage traffic on behalf of their customers as a natural means of creating sustainable businesses.

7. There is a significant commercial/revenue opportunity for ISP's in managing out the illegal traffic on the internet.

Traffic management is integral to a sustainable internet.

It is currently possible to automatically prevent the on-line traffic in individual items of illegal or otherwise infringing content, directed at individual customers across the internet, by utilising existing hardware and processes. The application that makes this possible was developed in Australia and is based on existing patents; it is known as Global File Registry.

This level of crime prevention or content management occurs instantaneously at the speed of the wire, automatically, without any discernible impact on technical performance, without false positives, without infringing upon any communication or the privacy of people using the internet.

The very same technology can automatically manage out the infringing traffic of the large scale commercial pirate operations that deliver content such as music, films, games, books and software to millions of people around the world simultaneously. In this mode the crime prevention application more specifically becomes a content management tool creating a legitimate commercial opportunity out of every attempt to distribute a previously confirmed infringing file.

This delivers a dramatic increase in revenue to Internet Service Providers (ISPs) and Content Owners. Indeed for the ISPs the increase in gross billing revenue can exceed 30%.

Notwithstanding the ability to remove from the internet millions of child sexual exploitation images and billions of infringing content files or the capacity to generate a significant new revenue stream for both ISPs and Content Owners market adoption is likely to be slow and piecemeal unless supported by mandate.

GLOBAL FILE REGISTRY

GFR is a content management system with business and crime prevention functionality, based on a centralised data base that contains unique identifiers of millions of infringing files captured, confirmed and collated on behalf of multiple content owners.

In its current commercial application GFR relies on file hashes as the unique identifier however, URL, Content Management System ID or other means of uniquely identifying a particular data item can also be utilised in any of the networks supported by Global File Registry.

Unlike other on-line anti-piracy solutions, GFR is both a business and technology platform that can facilitate revenue generation from on-line pirates/illicit data traffickers to copyright owners and their partners. GFR has an integrated ISP billing function so that legitimate alternatives of the copyright infringing content being advertised in Peer to Peer networks can be instantaneously purchased and received by the customer. This enables the ISP to share in revenue gained from converting infringing traffic into legitimate traffic thereby creating a profit that would fund and exceed implementation costs.

Unlike other on-line law enforcement solutions GFR is a crime prevention application first, making the attempt to distribute or possess previously confirmed child sexual exploitation images impossible. When an on-line child sexual exploitation image is being offered in search results GFR can promote a warning and/or educational resource appropriate for any jurisdiction for consumers instead. This crime prevention application can be obtained for free.

These processes are automated and instantaneous.

GFR does not require either copyright owners or the owners of internet service providers to change the fundamental nature of their business operation or the investment in significant operating or capital expenditure. Rather it creates, in managing illicit data traffic, a new opportunity to generate revenue and a considerable contribution to the digital economy.

AN OVERVIEW OF THE TECHNOLOGY

GFR is an application designed to run in highly advanced computers for ISPs (what is known as carrier grade network equipment). The GFR application inspects network packets using Deep Packet Inspection (DPI) to find specific network packets that contain references to infringing or illegal files on P2P networks.

These references to illegal files are, in most cases, search results (advertisements for infringing or illegal content) arriving from other participants in a P2P network after clients of the ISP have performed searches for files on the network. The results are used by clients of the ISP to gain access to and download these illegal files.

When GFR finds these specific packets containing a file hash (unique file identifier) reference to infringing files, it will replace it with a file hash reference

to the legal alternative replacement file - for example, a non-infringing version of the same or similar file. In this way, the clients of the ISP never get an advertisement (search result) with access to that particular illegal file, as they never would have received a link to the illegal file.

GFR knows whether a reference to a file is to be replaced by checking the file hash of the file, which is always included in the packet being communicated between users of a P2P networks. A file hash is like a serial number or DNA fingerprint of a file - it uniquely identifies a file and is used throughout P2P networks to refer and access files in the process commonly known as P2P File Sharing.

File hashes that are not known by the GFR application are not replaced. GFR conducts extensive analysis on files that are not replaced to determine whether they are illegal or infringing. This analysis is conducted without interference by the activity of GFR in the ISP's network. If a particular file hash is found to refer to an illegal or infringing file, it will be added to GFR's block list. That block list is managed by rules that determine which of all the blocked file hashes maintained to install by GFR, focusing on currently active or most popular infringing or illegal files.

This ensures maximum effect and efficiency of GFR on the illegal or infringing traffic. As a result infringing file sharing is then prevented only once a file hash has been determined to be an illegal file.

Finally the GFR process operates across networks at the speed of the data flow, does not impact upon any communication, does not infringe privacy of customers, its impact on technical performance on an overall network is sub millisecond, it operates on only previously confirmed illegal content and its implementation is cost positive.

There can be no doubt that GFR can create tremendous new revenue streams for the ISP industry and at the same time create a real time crime prevention platform protecting the victims of online child sexual exploitation.

Clearly traffic management does represent a significant social economic and social contribution to the community.

A Word on Internet Search Engines

Unfettered 'net neutrality' ultimately creates only one commercial beneficiary. That is the Internet Search Engines. Their present revenues attest to this already.

At present the Internet Search Engine industry is permitted to, on a commercial basis, search for and deliver to customers all over the world whatever illegal data they chose to search for.

It is illogical to contemplate that the Internet Search Engine industry is technologically capable of finding, ranking, promoting and delivering data but not rejecting illicit data.

Ridding the internet of the large volume of illicit data currently being trafficked by not facilitating is location and distribution would greatly alleviate the current traffic burden on the internet.

It is the consumer drive for access to on-line content that challenges the ISPs' resources and drives them to consider traffic management. Ironically it is the ISPs who are under pressure from peak industry or ngo bodies seeking to make 'someone' liable for illicit data traffic. Yet the traffic is located, determined and delivered by Internet Search Engines.

This practice or industry has gone on unchallenged or never rates a mention. Not even when the Internet Search Engine industry attends various fora to promote or support unfettered 'net neutrality'.

This in itself is a complex area but one that must be explored in any consideration of 'net neutrality' if socially and commercially sustainable decisions are to be made.

Given the nature of the Discussion Paper we believe it is not possible to fully explore the role and impact of Internet Search Engines on internet usage in our response. However should Ofcom reconsider the importance of the conduct of Internet Search Engines BDE would welcome the opportunity to assist by attending any meeting or discussions.

CONCLUSION

It is clear that internet traffic management has many social and commercial benefits including; creating new revenue streams for all 'digital' industries, creating new revenue streams for the State, large scale-real time crime prevention and protection of creative endeavours.

Taking the opposite approach – traffic management is more likely to protect the best of 'net neutrality' than unfettered/unmanaged internet traffic which naturally will favour those that obey no laws or respect no property. History has confirmed this.

In closing a useful approach to take here would be to ask, 'How much net neutrality' do we need to give up to maintain and protect the best of what 'net neutrality' has to offer?'