SUBMISSION TO THE JOINT SELECT COMMITTEE ON CYBER-SAFETY

BY BRILLIANT DIGITAL ENTERTAINMENT

INTRODUCTION

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.

Brilliant Digital Entertainment Pty. Ltd. (BDE) is a content management business and its related entities are engaged in search engine optimisation, web development, software development and technology research and development. BDE operates a technology business incubator from its Sydney 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 comment upon matters included in the Terms of Reference.

BDE intends to make submissions in relation to a number of items in the Terms of Reference. We will commence however with an overview of Global File Registry (GFR). Given that GFR provides a highly effective and dynamic crime prevention-content management platform whilst at the same time creating significant new revenue stream for the digital economy it is relevant to multiple Terms of Reference items.

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 which just generate large numbers of offenders 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.

A power point presentation on the GFR process flow is attached as *Annexure A*.

GFR has undergone live trials with an Australian ISP and its customer base with positive results. A sample report on child porn search results delivered from customer searches by GFR is attached as on a confidential basis *Annexure B.*

THE ON-LINE ENVIRONMENT

‘in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers)’

On any view the full extent of innovation, market reach and exploitation has yet to occur in the on-line environment.

Innovation relating to the internet and digital technologies goes largely unfettered and in Australia is well supported by business and government. The guiding principal of ‘innovation without permission’ stands true and it is hard not to believe that the removal of any obstacle to increased performance, customer satisfaction and business profitability is only a key stroke away. Accordingly the internet has yet to exhaust the ways in which people and businesses can extend their own reach globally, neither has it achieved its maximum efficiency.

Market reach in the main will be fuelled by two factors. Firstly despite the perceived pervasiveness of the internet it has barely reached one quarter of the world’s population. Secondly demand for internet based service will increased dramatically over the next few years. Cisco Systems in their current Visual Networking Index predict that internet traffic will increase by a factor of four from 2009 to 2014.

Put another way internet traffic will increase from 15 Exabytes per month in 2009 to nearly 64 Exabytes per month in 2014. An Exabyte is equivalent to all of the data on 250 million DVD’s!

Further Cisco estimates that the various forms of video, TV, VoD, Internet Video and P2P will constitute more than 91% of global consumer traffic and mobile data traffic will double every year up to 2014. As such the next few years will see a dramatic increase in the number of people accessing the internet and at the same time a massive increase in traffic demands of existing customers.

Exploitation closely follows on opportunity. This explosive increase in demand multiplied by the billions of yet to be engaged potential on-line customers creates a hotbed for those who adopt the new technologies for the purpose of exploitation.

Even an increase in exploitation proportionate to the increase in traffic/population poses a significant challenge to law enforcement and government. This highlights the importance of this Committee’s inquiry and the far reaching effects of any recommendations.

ISPs presently disclaim any liability for the conduct of individuals or corporations on-line despite access not being possible without their acquiescence almost always only granted after payment. Whilst in the public discourse there are many reasons proffered by ISPs as to why the industry cannot control illicit traffic, as opposed to why it won’t; the principal reason relates to a lack of technical capacity to do so. That may well have been the case many years ago but it no longer is the case.

Consider for example currently available hardware solutions utilised by the majority of ISPs in one form or another to manage customer traffic;

http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps9591/ps9613/data_sheet_c78-492987.html Cisco Systems

Whilst this document speaks for itself note that the device supports application-level classification of IP traffic for the real-time management and control of content-based services for a given subscriber or group, can track up to 32 million concurrent unidirectional application sessions, can manage up to 1,000,000 concurrent subscribers and supports more than 600 protocols.

http://www.juniper.net/solutions/literature/solutionbriefs/351154.pdf Juniper Networks,

Again this solution drives high level subscriber specific on-line traffic management solutions.

http://www.ipoque.com/products/prx-traffic-manager Ipoque

Here is another solution that can manage high level on-line traffic management; indeed it is able to 'enforce legal file sharing'.

It is clear from the above examples that GFR constitutes a minor refinement of the hardware and processes yet delivers dramatic crime prevention and commercial results.

Beyond the ISPs the stakeholders with the greatest capacity to change the nature of on-line traffic and its legitimacy are the content owners. It is the traffic in content, legitimate and infringing, that represents the greatest demand for access and social discourse on-line. Indeed presently intellectual property represents one of the most valuable forms of on-line currency.

Much of the accessing and trading in child sexual exploitation images tends to occur through applications found at the edges of the network.

Those applications are more often than not the very same applications used in the massive ebb and flow of infringing content. It follows that if the Content Owners and ISPs joined together to resolve online infringement much of the traffic in on-line child sexual exploitation material would also be resolved.

Accordingly we would ask that the Committee consider recognising the Content Industries as stakeholders able to influence action here and call upon them to contribute to this inquiry.

ILLEGAL AND INAPPROPRIATE CONTENT

‘exposure to illegal and inappropriate content’

Our discussions with potential adopters of GFR have provided anecdotal information that there may be in excess of 2,000,000 child sexual exploitation images available at various times on the internet. These may include multiple versions of images of victims reconstituted with minor variations and in some cases pseudo images.

We note that it would be difficult to properly undertake research here and provide definitive statistics at present as access itself would constitute a criminal offence in most circumstances.

It bears mentioning that child pornography is a permanent record of a child being sexually abused and that with the continuing traffic many years after the original abuse, the child continues to be victimised by new waves of offenders. However much of the material is one way or another recycled and identifiable in advance and it is therefore capable of being managed out of internet traffic dynamically by GFR. Note that much effort is taken by various law enforcement agencies around the world to harvest the numerical identifiers of confirmed on-line child sexual exploitation images. This works represents existing major data bases of confirmed illicit data that are capable of driving a GFR solution.

In relation to copyright infringing data traffic, whilst industry statistics are contested in some quarters, there can be no doubt that the volume is huge and has a multi-billion dollar value. Take for example the statement from the IFPI Digital Music Report 2009, Key Statistics, document which stated, ‘Collating separate studies in 16 countries over a three-year period, IFPI estimates more than 40 billion files were illegally file-shared in 2008, giving a piracy rate of around 95 per cent’

Other industries with the capacity for on-line content will suffer similar rates of infringement.

Perhaps an example at the opposite end of the product spectrum might best highlight the scale of the problem and also the potential social and commercial value of an effective solution; the percentage of copyright infringing adult entertainment files being trafficked on line is as high as 98%. Imagine the diminution in inappropriate content on-line if this industry re-gained control over its content from pirates.

Much of this material is one way or another recycled and identifiable in advance. It is therefore capable of being managed out of internet traffic dynamically by GFR. Note that much effort is taken by various Content Industries to harvest the numerical identifiers of infringing/illegal content. This work represents existing major data bases of confirmed illicit data that are capable of driving a GFR solution.

Furthermore it must be reinforced that as the applications that facilitate (and profit from) copyright infringing traffic are at the edge of the networks, they are the very same networks that are relied upon by the distributors and the various acquirers of child porn and other illicit content.

The internet has not created new crimes or harms here. It has merely enabled and accelerated the capacity for the networking of offenders and the acquisition/distribution of illicit items. In relation to child pornography and copyright infringement it has simply made hyper-crimes of otherwise well understood illegal activities.

The internet has also, from its own architecture and processes accelerated the capacity to prevent crime and dynamically manage data traffic. However this capacity has not been acknowledged or adopted.

AUSTRALIAN AND INTERNATIONAL RESPONSES

'Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business'

This inquiry will represent an important and timely contribution to the formulation of effective responses to the issues here. There are many individuals and corporations committed to participating in this process. We particularly commend the efforts of Australian law enforcement agencies who have managed to operate in the absence of on-line crime prevention platforms. These agencies have been able, for many victims of on-line exploitation, to turn the chaos and ambiguity of the internet into a deterministic chaos. It should be noted that the Australian Federal Police currently chair the Virtual Global Task Force.

However two of the principal protagonists in the public discourse relating to the nature of infringing or otherwise illegal on-line content, the Content Owners and ISPs, remain locked in a circular debate about who should act and who should be responsible for the on-line traffic in illicit or infringing content.

Much of what is proffered by these stakeholders in support of their positions merely supports the status quo and does not withstand critical examination.

Content Industries as a general position take the view that the ISPs should deal with illicit data traffic at their own expense and as their own responsibility. The ISPs quite rightly see this as unviable on a commercial level. As any management of infringing content traffic on the ISP networks inevitably involves the substitution of that content with legitimate versions of the sought after content, Content Owners must be closely involved in strategic partnerships with ISPs.

The general position of ISPs can be described as them merely being gatekeepers and therefore not responsible for traffic that traverses their networks. Regardless of any 'legal position' here they represent the only architectural opportunity to prevent the on-line infringement of copyright or crimes relating to the possession or acquisition of child pornography.

This discourse represents a situation where each stakeholder expects the other to give up part of their position with no recompense.

These stakeholders represent the principal commercial beneficiaries of any solution yet there have been occasions where a GFR solution for the traffic in on-line child sexual exploitation images was rejected because it would create an opportunity for Content Industries to impose their position.

There is potential for significant increases in revenue, quality of service and efficiency dividends yet neither stakeholder has had the courage be move first and adopt a GFR type solution. However privately many on either side have expressed their interest in adoption should there be an industry wide adoption.

In the past reasons proffered by the ISP industry for not adopting solutions to on-line traffic in illegal or infringing content have included;

- the lack of enabling technology
- adverse impact on network speed
- the refusal of victims to pay for the enforcement (content management) action
- the cost of enforcement (content management) action
- privacy concerns
- freedom of speech
- concerns relating to the interception of communication
- the risk of false positives
- a possible shift to encryption
- the question of confirmation of infringing/illegal nature of data files.

Each and every one of these issues is resolved and overcome by GFR. Furthermore GFR generates significant positive revenue with minimal additional capital or operating expenditure.

Should these two stakeholders resolve or be compelled to resolve their conflict the vast majority of illicit traffic would be swept away (and a great deal of money would be generated).

We would ask the Committee to consider asking these stakeholders to advise how they would create strategic partnerships to take advantage of crime prevention platforms such as GFR that resolve all of their obstacles to partnership and implementation of a solution.

BENEFITS OF NEW TECHNOLOGIES

'examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised'

It is clear that there are rivers of gold in the torrents of unmanaged content flowing through the networks of ISPs. This unmanaged traffic is not only a revenue opportunity lost but also comes at a cost which is subsidised by all customers of ISPs. The cost includes the cost of storage of multiple cached versions of popular infringing/illegal content and diminished network/business efficiency.

GFR has been trialed in both its crime prevention and content management modes within an Australian ISP and its customer base.

The results have been unequivocal. GFR dynamically converts infringing or illegal data and delivers; a new revenue stream for our digital economy, does not impact adversely on network performance, has no discernible impact on the customer experience, has no false positives, does not intercept any communication, does not impact on customer privacy, requires little additional capital or operating expenditure, relies upon existing carrier grade equipment and merely refines existing internet processes.

Yet market adoption of GFR or similar solutions is no easy road.

It may well be that the foreseeable nature of the harms created by illegal or infringing on-line harm and the avoidance of available unequivocal solutions such as GFR by ISPs and Content Industries might give rise to a new species of consumer/public protection action in the courts.

We recommend that the Committee consider the need to mandate the adoption of on-line crime prevention platforms.

ONLINE OMBUDSMAN

'the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues'

At present there is no independent position that rises above the opposing position and competing vendors that would enable on-line safety to become a fundamental right rather than wishful thinking.

The proposed role of Online Ombudsman has the potential to have a far reaching effect not only on the safety of on-line activity but also make a positive contribution to Australia's digital economy.

To do so the role of On-Line Ombudsman would need to be appropriately empowered to reach across a wide variety of organisations and take innovative or creative actions.

In order to achieve the full potential of this role the Ombudsman should have the capacity to influence or act jointly with a range of stakeholder organisations such a law enforcement agencies, a variety of other ombudsmen, certain government agencies and have enforceable investigative and dispute resolution powers. The role should have the authority and obligation to submit amicus curiae briefs in Court matters likely to have an impact or otherwise influence the course of internet activity including e-commerce, law enforcement and content distribution.

We would recommend that the Committee consider ensuring that not only the role of Online Ombudsman be established but also that the role is sufficiently empowered to influence the on-line environment.

CONCLUSION

The work of this Committee is incredibly important as any outcomes will simultaneously have an impact on cyber-safety and the digital economy.

We welcome the opportunity to provide the Committee with further information and comments at any time or venue.

Michael Speck

REFERENCE

Page 5

Cisco Systems Inc., Visual Networking Index, accessed June 16, 2010 at http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html

Page 8

IFPI Digital Music Report 2009, Key Statistics, accessed June 16, 2010 at http://www.ifpi.org/content/library/DMR2009-key-statistics.pdf

ANNEXURE'S

Page 5

Annexure A	Global File Registry Process Flow presentation
Annexure B	Global File Registry Child Porn trial sample report,
	Provided on a confidential basis.