SUBMISSION OF BRILLIANT DIGITAL ENTERTAINMENT TO THE JOINT SELECT COMMITTEE ON CYBER-SAFETY INQUIRY IN RELATION TO THE CYBERCRIME LEGISLATION AMENDMENT BILL 2011.

Brilliant Digital Entertainment Pty. Ltd. (BDE) is a Sydney based company specialising in online content management and online crime prevention technologies. Our stakeholders have extensive experience in the global management of online content, serving and managing online consumers and online crime prevention.

The amendments contained in the Cybercrimes Legislation Amendment Bill 2011 (the Bill) are a necessity if Australia is to meet present and emerging cyber-challenges.

Those challenges include;

1. The internet and associated technologies blur national borders allowing many social and commercial activities that were previously constrained by geography to be internationalised.
2. The internet and what falls within the term 'cyberspace' is an international network that belongs to private networks. Indeed if 'cyberspace' existed it would be a company town. This means that the majority of law enforcement initiatives the State wishes to impose upon those networks require the approval, permission or genuine support of the owners of the private networks if they are to work.
3. The corporations that own and control the access to the internet, and the traffic on the networks that constitute the internet, have proven they will not impose the rule of law on their networks unless the obligation is imposed upon them by the State.
4. The corporations that own and control access to the internet, and the traffic on the networks that constitute the internet, conduct their networks as private property. As such it is only right that ever increasing law enforcement responsibilities must be given to the Carrier or Carriage Service Provider C/CSPs.
5. It is estimated that by 2015 there will be as much as 500 billion hours of content available on the internet connecting with roughly 15 billion devices being trafficked to and from approximately 30% of the planet's population, improvements in technology reduce digital transactions to nano-seconds, the Information and Communication Technology (ICT) industry's carbon footprint will have doubled.

It should be noted that the Bill also contains safeguards against possible misuse of the proposed legislation that when combined with existing legal protection provide the best possible balance for the needs of law enforcement and individual rights.

Given the international nature of the internet, its community and its commercialisation it is absolutely critical that Australia accede to the Council of Europe Convention on Cybercrime (the Convention). The Convention is a truly international treaty which was produced after considerable consultation and has received widespread international support. One of the reasons for that international support is that the Convention provides a mechanism for the development of new laws, policies and

practices to respond to rapidly evolving cyber activities such as cyber warfare where criminal capabilities have rushed ahead of any legal framework.

It is ironic that those who are the loudest proponents of special considerations being given to internet activity because of its international or borderless nature are also often the loudest opponents of any international cyber law enforcement regulation and the Convention.

BDE would like to submit a number of comments to the Committee that relate to the assertion that the Bill will have no financial impact.

The statement that the Bill will have no financial impact is found in the Explanatory Memorandum.

BDE is of the view that any Australian C/CSP acting in good faith can and will benefit financially from the imposition of the proposed legislation.

The view that no financial impact will result from the proposed legislation derives from Section 314 (2) of the Telecommunications Act 1997 which ensures that the C/CSP's compliance is on a no profit, no loss basis and the knowledge that the technical capacity for compliance already exists within the C/CSPs technology infra-structure.

The assumption is flawed for a number of reasons;

1. It assumes that S313 of the Telecommunications Act has been complied with in good faith. This is not simply not so. S313 requires C/CSPs 'do the carrier's best or the provider's best *to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences* against the laws of the Commonwealth or of the States and Territories.

   Presently S313 is mostly honoured in its breach. As a matter of practice the provision is relied upon almost always for investigation and not crime prevention. This is so because the operation of S313 occurs only on a low level negotiated basis between the law enforcement agencies and the C/CSPs. It is clear from history that the C/CSPs will not voluntarily apply any crime prevention technologies or practices and when obliged to do so by legislation will seek to negotiate the lowest possible level of compliance obligation.

   As a result the C/CSPs have avoided the opportunity to be part of the development of viable crime prevention technologies that could also resolve many of their other commercial and technical challenges.

   Many of the crime prevention technologies are capable of simultaneously generating new revenue streams. There are a wide range of commercially available online crime prevention technologies and hardware. In many cases the capacity for online crime prevention activities to take place already exists within the machinery already established in C/CSPs. Despite this it is not possible to give away for free any crime prevention technologies to the C/CSPs.

2. Once under a compulsion to undertake traffic management activities such as those to be required in the Bill the C/CSPs will exist in an environment where, due to the exigencies of corporate activity, they will be required to contemplate the other performance, commercial and technical opportunities available from the existing technology they would rely upon to comply.

   Being required to apply existing technologies to additional traffic management responsibilities would result in the C/CSPs benefiting from cost savings and other efficiencies that would have a positive financial impact for them. Further the same existing technologies could be relied upon to deliver new revenue streams to the C/CSPs, their shareholders and the Australian economy.

3. There is in the existing technologies already relied upon by the C/CSPs the opportunity to undertake significantly cheaper compliance with the legislation.

   The present costs for compliance with the existing and proposed legislation have not and are not challenged. In the case of one existing technology, Global File Registry (GFR), managing illicit online traffic simultaneously delivers the opportunity to generate an increase in gross billing revenue of C/CSPs by as much as 30%. Application of GFR would mean that the C/CSPs could make a profit from compliance with the existing legislation and proposed legislation. This in turn would mean that the cost of cyber law enforcement operations would diminish dramatically.

In support of our submission we refer the Committee to our earlier submission to the Committee's Inquiry into Cyber-Safety (Submission 102) which sets out comprehensively details of GFR's capacity to deliver online crime prevention and revenue opportunities to C/CSPs in complying with the proposed legislation in the Bill.

We commend the Government for its action in making the necessary legislative amendments to accede to the Convention.

BDE is available and looks forward to the opportunity to provide the Committee with any further information it may require or to respond to any issues that might occur.

Michael Speck
Manager
Brilliant Digital Entertainment