

Hong Kong Internet Service Providers Association's Response to Consultation on Copyright Protection in Digital Environment

30th April 2007

HKISPA is the industry association representing the interest of Internet Service Providers in Hong Kong. In response to the consultation paper, the Executive Council of the HKISPA would like to register the following comments taking into account the commercial, operational and technical realities of Internet Service Providers:

1. Concerning Secondary Liability of Internet Service Providers

The ISP industry is generally of the view that we provide a purely conduit service to our customers, and we must respect the privacy rights and other lawful rights of our customers. Generally speaking apart from those routing information that are known to ISPs purely for and as a consequence of operational or network management requirements, ISPs do not, and are not supposed to, possess the knowledge of what kind of information is exchanged within and through their network, and ISPs do not possess the knowledge to judge whether a piece of information are subject to copyright protection or not. Our telecommunications licence(s) granted by the Office of the Telecommunications Authority does not permit us to eavesdrop.

Hypothetically, if an ISP possesses the knowledge that infringing activities are being carried out on their network, we believe that any liabilities imposed on the ISP due to its inability to directly assist copyright owners to take down the material are outright unfair and operationally impractical. This is elaborated below.

2. Concerning the proposed Take Down System

The mode of operation of an ISP is now heterogeneous in nature. We would like to avoid a comprehensive study of this at the moment, but would like to raise a few examples to illustrate this.

Example 1: ISPs normally provide hosting service for their customers to connect their servers to the Internet. Customers directly operate the assigned IP address range, where they could operate their own Internet service, which might involve an e-mail system for communication with their customers, or a discussion forum for a specific special interest. The ISP providing the connectivity service normally does not have direct administrative access to the system. In the event that a copyright owner found a BT seed in a discussion forum of a

customer-operated server and issued a take down notice to the ISP, the ISP could only inform the concerned customer to take down the material. If the customer is not responsive (they are not defined as “Online Service Provider” by the current consultation), the only means for the ISP to take down the material is to disconnect the whole system from the Internet. We believe this act is commercially too impractical, as the infringing material was just a BT seed but the remaining system is legitimate. Furthermore, how can we as commercial ISP operators be expected to possess the skills and knowledge needed to always judge with certainty what is infringing and what is not? In such event, would the copyright owner fully indemnify ISPs from and bear all cost and consequences of the take down act by the ISP? How good is this indemnity if the copyright owner is not registered in Hong Kong and has no assets for us to enforce against in Hong Kong? Should copyright owners first place a significant deposit with the ISP?

Example 2: Suppose we can still find infringing material on the Internet via the search engine google.com.hk. Copyright owners could, by the proposed take down mechanism, directly request the domain-name operator or the concerned ISP to de-list the domain name google.com.hk. If the domain-name operator or the concerned ISP refuses to do so, would they bear the so called “Secondary Liability”?

Example 3: A customer of ISP operates a web site, and ‘hyperlinks’ or ‘frames’ another web site containing infringing material. The infringing materials reside on the ‘framed’ foreign web site but not on the customer’s machine or the network of the ISP. Would that customer’s machine be subject to disconnection from the Internet? Under such circumstances, who is the party to judge and rule that this is an infringing act or assisting infringements?

Example 4: If the take down mechanism is enacted, copyright owners have a very low cost of collecting IP addresses that are using BT and sorting those addresses that reside in Hong Kong. In the event of a copyright owner giving a massive list of IP addresses to an ISP requesting a take down act, the ISP has difficulty in identifying the actual customer, and also due to the dispersed and complex network of larger scale ISPs, it is operationally very costly to pinpoint, isolate and identify those IP addresses, save the dynamic nature of IP address allocation. Then, who would bear the costs associated with such undertakings?

The above are only brief examples of operational difficulties. We have not mentioned about the massive scale of hyper-linking between contents on the Internet, the scattered and cross border nature of the Internet, the encryption methods of materials, the different types of content delivery technologies, the dynamic and evolving technologies being employed. Therefore, it is outright unfair, in our opinion, to demand ISPs to bear any kind of liability for

their failure to take down any material on the Internet.

3. Concerning Data Collection

By varied practices on the type of data and length of storage, ISPs, purely due to operational reasons, collect data about the connections/disconnections of customers, the e-mail send/receive record of e-mail users, the web site access records to sites hosted on their platforms. These are data that are practical to collect, but it is still very costly to maintain and preserve such records for considerable length of time. Apart from such, it is nearly impossible for an ISP to collect any other data.

The Internet Protocol is packet-switched, where the actual 'data' to be presented to the user involves resembling the TCP connection, sorting the packets in order, decrypting the data by application software or the operating system, and then fed to the user application (e.g. Internet Explorer) on the user's desktop to make it meaningful. Packets that are going in and out of an ISP's network simply do not carry any meaning to the ISP. It is not like a traditional telephone network that we could 'tap' the line and record the conversation. Therefore, it is technically absolutely impossible to record the so called 'all activities' of online users.

We agree that the length of time of storage of trivial and accessible data by ISPs could be specified by law, but what kind of data are to be kept, for what reasonable length of time, to whom those data could be reveal, and who would bear the cost of such undertakings must be carefully and separately studied and consulted in prior.

4. Concluding Remarks

By the current laws of Hong Kong, copyright owners have proper and complete means to protect their own rights. ISPs in Hong Kong are in general very cooperative with law enforcement departments like the Police and the Custom and Excise Department. Hong Kong having the first case of BT abuse successfully prosecuted may have reflected this fact. We believe this consultation on Copyright Protection in the Digital Environment must itself be reviewed of its principles and priorities before the next round of consultation.

The Executive Council

Hong Kong Internet Service Providers Association

Website: <http://www.hkispas.org.hk/>

E-mail: exco@hkispas.org.hk