Part 2 – Special Topic

HOW TO DEAL WITH SALES OF COUNTERFEIT GOODS VIA THE INTERNET

Hong Kong deals with counterfeit goods over the internet much as any common law country. The problem is particularly acute here given the proximity to China, where goods are sourced from for shipment all over the world.

1. Action available to private rightsholders

For the proactive rightsholder, regular monitoring of websites is a must. Business to business sourcing sites like *alibaba.com* are a constant source of infringing products. Whilst the products themselves are often sourced from mainland China, investigations of the infringer often reveal some connection to Hong Kong – products are shipped or transshipped via our ports (HK companies have traditionally been better placed to meet the demands of international consumers, by taking payment for goods in currencies other than RMB, and thanks to better English language penetration); HK shadow companies legitimise the infringing manufacturer; designs are 'created' here with instructions going to the Chinese manufacturer, who does not know he is infringing; or packaging takes place here, as Hong Kong people have a greater awareness of what Western brands and products are in demand.

Even in the case where the infringer has no direct connection to Hong Kong, then it may still be possible to bring proceedings against them: under the normal jurisdictional rules of the High Court, it will grant permission to serve a claim out of the jurisdiction where the tort occurred in, or resulted in damage in, Hong Kong. This means that it can still be illegal to market infringing goods to Hong Kong consumers and to sell those products in to Hong Kong, even where the infringer is based without Hong Kong. It is usually possible to found jurisdiction on this basis. It gives rightsholders a right of action here, with the benefits of the certainty that our IP laws can provide as against the challenges posed by enforcement in China.

But the enforceability of an obtained judgment can be a problem. In 2006, Hong Kong and China signed an "Arrangement on Reciprocal Enforcement of Judgments in Civil and Commercial Matters". However, in IP terms, this is only useful to enforce monetary judgments awarded on the basis of a breach of contract. It is no use in enforcing infringement judgments against Chinese defendants, as injunctive relief is not available, and a contractual relationship is required. We hope that as time goes on the scope of the Arrangement will be widened. Until then, one can only rely on the usual principles of comity and hope that Chinese courts would give effect to Hong Kong judgments. The uncertainty involved is usually enough to make clients too wary to proceed this way, even where there is a substantial, real infringement in Hong Kong.

Alternatively, the b2b websites offer helpful, effective complaints procedures. Alibaba.com acts quickly to remove infringing listings on receipt of a properly specified and valid complaint by a rightsholder. But there have been no decisions to date on the secondary liability of internet gateways and service providers for their users selling counterfeits, unlike in most other countries where some form of liability has been imposed already. And there is no defined legal 'safe harbour' for service providers, unlike the US Digital Millenium Copyright Act which exempts them if they act promptly to remove the questionable content.

It is rare for IP actions (whether over online infringements or otherwise) to reach the courts in Hong Kong. Due, no doubt, to the limited size of the market here, as well as the certainty offered by Hong Kong law and its citizens' healthy respect for IP rights, disputes can usually be settled by negotiations between the parties.

2. Data protection from detection?

The Privacy Commissioner launched a consultation in August to clarify, amongst other things, whether an IP address constitutes 'personal data' for the purposes of the Personal Data (Privacy) Ordinance. If so, IP addresses would be subject to the usual data protection principles, including restrictions on the use and transfer of that data, and permissible retention periods.

This stems from the Yahoo! case, where the disclosure by Yahoo! Hong Kong of an IP address in China, from which mainland journalist Shi Tao had accessed his Yahoo! email account and leaked documents critical of the Beijing government. This was one of the factors that lead to him being jailed for 10 years. In that case, Yahoo! were found not to have breached Hong Kong's privacy laws. Many think this is an unacceptable result, and so privacy laws should be strengthened.

Making IP addresses personal data will, in some circumstances, complicate infringement investigations as it will become more difficult to learn the identity of infringers – who was operating a certain machine, or visiting/transacting with a certain website, at a particular time when an infringement took place?

Then, once you have a suspect IP address, the position in the US is that you can force ISPs to divulge the identities of users suspected of online infringement via subpoena. This is a simple and effective process.

In contrast, this is currently done in Hong Kong via rightsholders taking out Norwich Pharmacal orders against uncooperative service providers, a procedure which the government consulted on in 2007, decided was flawed, but declined to do anything about.

Hong Kong does not force ISPs to keep logs of the activity of their users, but in practice most do. If IP addresses are codified as personal data, we may expect this practice to be reduced.

3. Criminal actions available

Criminal actions are brought by Hong Kong Customs, either *ex officio* or on the complaint of a rightsholder. This can be done in respect of trademarked or copyrighted goods, but not those protected by patents or registered designs.

Some examples of recent Customs actions are given above.

For copyright, only the distribution of infringing copies of copyrighted works "in a business context" or otherwise to such an extent as to prejudicially affect the rightsholder are actionable offences. The Government considers that this is sufficient to target the root of the problem of the pirate works being distributed or sold over the internet – and accordingly they target their enforcement efforts on uploaders.

Indeed, with the *Big Crook* case in 2005, defendant Chan Nai Ming is believed to have been the first person in the world given a criminal conviction for uploading movie files to BitTorrent. His uploads were held to have prejudicially affected the rightsholder – although, in the writer's opinion, any unfortunate downloaders may have suffered greater prejudice. The films in question were *Daredevil, Red Planet,* and *Miss Congeniality.*