Yui Kee Computing Ltd.

# Newsletter

February 2008

## Contents



## Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal

*<web-link for this article>*

*Allan Dyer*

A hot topic in the news recently has been the circulation of erotic pictures, apparently of Hong Kong celebrities Edison Chen Koon Hei, Gillian Chung, Bobo Chan, and Cecilia Cheung. Arrests have been made and Assistant Commissioner (Crime) Vincent Wong Fook-chuen has said "We are quite confident to say that the source [of the photos] is confirmed. Someone had sent his computer for repair and the pictures [stored inside] were stolen without the consent of the owner." Apparently, the prosecution will focus on whether the data was stolen, and whether obscene articles were distributed.

Press comment has pointed out that distributing obscene material in Hong Kong is a serious crime, although possession of such material for personal use is not. Assistant Commissioner Wong was asked why the police have not acted against other obscene photos circulating on the internet, he gave the rather unconvincing response, "In my 20-plus years as a policeman, I have not come across such an issue". Is he unaware that there is obscene material on the internet? The police are now open to the accusation that this case has been investigated because it involves celebrities, while other cases, such as former lovers posting intimate photos as revenge, have previously been ignored.

The law on these matters is outdated, how can we draft new laws that protect the vulnerable without flying in the face of the realities of an interconnected world?

Obscenity cannot be defined precisely, and reference is usually made to "community standards". When we judge community standards in Hong Kong, shouldn't we also consider the material being accessed by Hong Kong people through the internet from other sources? I suspect that an investigation of web access logs would reveal that many people in Hong Kong are accessing material the Obscene Articles Tribunal would classify as obscene. Doesn't that mean that the Tribunal is failing to keep up with changing community standards? Why should it be considered a crime if consenting adults indulging in legal activities choose to have images of those activities recorded, and choose to have those images distributed to other consenting adults?

So the offence in this case is not one of obscenity, but of invasion of privacy. Fortunately, Hong Kong does have a Personal Data Privacy Ordinance. Data Protection Principle 3 seems directly applicable:

**Principle 3 - Use of personal data** This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.

Distributing private photos without consent clearly violates this principle. You could also consider that the owner of the computer sent for repair had violated Principle 4:

**Principle 4 - Security of personal data** This requires appropriate security measures to be applied to personal data.

It seems entirely reasonable to hold someone who chooses to keep intimate photos responsible for their safety. Other principles can be usefully applied to different "sex photo" cases:

**Principle 1 - Purpose and manner of collection** This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.

No secret filming! What about photos kept by former lovers?

**Principle 2 - Accuracy and duration of retention** This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

If the original purpose was enjoyment by lovers, then the purpose ended when the relationship ended, and the photos should be destroyed.

Unfortunately, there are currently two problems with applying the Personal Data Privacy Ordinance. Firstly, the Ordinance is largely toothless: the Privacy Commissioner can merely issue an Enforcement Notice, and only non-compliance will result in a penalty - but the damage is done when the data is first released. Secondly, the Ordinance includes a broad exemption for "personal data held for domestic or recreational purposes".

**13th February 2008**

The controversy over this incident is continuing, with many commentators seeking a high moral stance. The Catholic Church's Diocesan social communications office director Dominic Yung Yuk-yu has advocates that schools should use the case to promote ethics based on religion, saying, "Every student has already seen those photographs. There is no reason not to talk about them." **Every** student? How does he know? Are there really no parents in Hong Kong who have installed a web filter and who check their children's internet use?

In a letter to the South China Morning Post, Peggy Leung Pui-ki write, "The police commissioner, Tang King-shing, has claimed that the police are patrolling the internet more frequently, which is very much appreciated." Well, to any Bobbies patrolling this area, "G'evening Officer, cold night." I guess we can soon expect the Courts to be flooded with thousands more cases of "publishing obscene material", because, although certain Police Commissioners may not have noticed, there are a lot of images of a similar nature on the internet.

Peter Gordon has written interesting commentary on the issue in The Standard.

**16th February 2008**

Writing in the UK newspaper The Guardian, Cory Doctorow likens personal data to nuclear waste:

We should treat personal electronic data with the same care and respect as weapons-grade plutonium - it is dangerous, long-lasting and once it has leaked there's no getting it back.

He is writing about the negligent disclosure of 25 million personal records by HM Revenue and Customs, and other UK incidents, but the lesson can be applied equally to amateur photographers. Well-known security commentator, Bruce Schneier wrote something similar in 2006, but Doctorow has the better soundbite.

**19th February 2008**

In the original article above, I said that other similar cases, "such as former lovers posting intimate photos as revenge" had been ignored. It turns out that there is at least one such case where existing laws, namely criminal intimidation, publishing an indecent article without required notice and publishing an obscene article; were used in the prosecution. The defendant was sentenced to 240 hours of community service last September, but the prosecutor is now seeking a jail sentence. The initial sentence does appear far too lenient considering the distress and harm to the woman. It is clear from the complaints received by the Broadcasting Authority against Gillian Chung Yan-tung's appearance at a charity concert that there are Puritans who will ostracise and discriminate against the victims in such cases, because the victims have failed to meet their oppressive moral standards. The "moral outrage" could end Gillian's career, and, on a smaller but no less relevant scale, affect the employment prospects and social life of the woman in this revenge case.

**20th February 2008**

Today's (Feb 20, 2008) Leader in the South China Morning Post takes the view, "the most important matter is being missed: privacy". Nice to see someone else promoting the view that I've taken here.

**27th February 2008**

The Privacy Commissioner for Personal Data, Roderick Woo Bun, is pushing for reform of the Personal Data (Privacy) Ordinance, using the nude photos case as an example. Peter Gordon, writing in The Standard, accuses the Commissioner of mission creep and ridicules the idea that the identifiability of the celebrities in these photos makes them "Personal Data", writing, "No one needed these particular photos to identify either the female subjects involved or their camera-happy beau". He also suggests that this interpretation would prevent images from sporting events being published and points out the conflict of the Commissioner's view with the normal understanding of copyright: the photographer owns the photo, not the subject. He claims, "you can't have different laws assigning ownership of the same item to different groups of people without a mess resulting".

Firstly, the identifiability of the subjects is not (always) the private data that should be protected, but it is **the link** which makes the difference between possibly statistical information (e.g. "some accounts at our bank contain over $10 million") and private information about a person (e.g. "Mr. X has an account with over $10 million"). With these photos, the identification of the participants changes the rather banal information, "adults have sex" into the rather personal, "Y had sex with Z". With identification, the private data can be linked to other data that is already known, "Mr. X never buys a round at the pub", "Y and Z are not married".

Secondly, copyright ownership is not the same as property ownership, and the law commonly features situations where different parties all have rights over the same "thing" - take a look at landowners and rights of way, as one example. The issue of publishing images of sporting events is easily covered as a matter of balance and expectations: as many bank robbers realise, you may be recognised if you are in a public place without a mask, the unmasked spectators at a sporting event do not have an expectation of privacy, and the photos are not published in the expectation of their being used to identify the spectators.

Mr. Gordon does raise the valid point about the data being collected on security camera tapes. We are quickly reaching a level of technology that makes George Orwell's vision in "1984" actually feasible. We need public debate about our privacy expectations before everyone is wearing a life recorder, and that includes what happens when private photos are made public, even if they merely affect, "the wholesome image of celebrities" that Mr. Gordon considers, "is not the sort of thing one imagines the Privacy Ordinance was enacted for."

**More Information**

Police trace source of nude internet photos
Net postings highlight need for legal reforms
Please destroy photos, Edison Chen pleads
Net service providers meet police over nude photos
Sex Scandal Photos Shock Hong Kong Showbiz Industry
Edison Chen's Pornographic Photos Cause Uproar
Star apologizes to six artistes in 1,300 racy internet photos
Harry's View - SCMP cartoon
PERSONAL DATA (PRIVACY) ORDINANCE full text
The Ordinance at a Glance
A case of dangerous double standards
6 new photos appear despite arrests
Beware kids' shattered fantasies, parents urged
Computer technician, 23, released on bail
Clerk charged over sex photos is granted bail
There's a lot to learn from saga
Suspect granted bail as Edison's return imminent
Net photo furor fans tricky issues
Personal data is as hot as nuclear waste
Data as Pollution
Jail sought for former boyfriend over online nude photos, sex clips
Proposals to amend the privacy law for better protection of online personal data
Privacy plan takes an absurd turn
Response to the incident of online circulation of nude photos

# Sophos Changes Update Methods

*<web-link for this article>*

In an email to subscribers Sophos has announced that during the next few months it will be making a number of changes to the mailing lists and downloads available to customers. The change is due to the continuing exponential rise in the number of new malware samples, and, as a result of the changes Sophos will be able to substantially increase the number of virus updates released every day, thereby providing even faster and better protection against malware.

The changes are:

- **March 4th 2008:** Individual IDE files will not be available for download from www.sophos.com. Customers are encouraged to use one of the automated update mechanisms available from Sophos to receive their updates. Alternatively users can download the ides.zip file from the Sophos website. This zip archive contains all the ide updates released since the last monthly engine update. Other zip archives are available for customers using older engines although users are encouraged to stay up to date and should not use an engine more than 3 months old.
- Three new subscription lists have been created to provide more targeted satisfaction of customer needs:

- **Sophos Update Alert** Subscription to this service will continue to provide an alert following the release of a new virus update. As the number of virus updates increases, so will the number of update alerts received increase. This new alert email will not contain information about the update itself, only announcing that an update has taken place. Subscribe by email.
- **Sophos Daily Update Digest** This email is for those customers wanting basic information about recent identity updates. Initially this subscription will simply provide a link to www.sophos.com/downloads/ide. From March, this email will provide subscribers with a daily digest about the updates released in the previous 24 hours. This information can also be viewed by subscribing to the Sophos RSS feeds. Subscribe by email.
- **Sophos Protection News** This newsletter will be a regular review of the updates released over the previous month, providing some statistics and analysis of these releases. This information will also be found on the SophosLabs blog which provides an easy way of keeping abreast of the very latest information about malware seen by our global network of analysts. This mailing list will also be used by SophosLabs to send out any urgent notifications about malware outbreaks where significant action should be taken. Subscribe by email.

- The format of emails from the existing alert service, Sophos Alert System, will change on February 4th 2008 in line with the new alert service, Sophos Update Alert.
- The existing alert service, Sophos Alert System, will then cease to send update alerts from March 4th 2008.

Sophos encourages subscribers to sign up to one of the three new mailing lists above should they wish to continue to receive this information. On subscribing to one or more of the above mailing lists, you will automatically be removed from the current update alert service.

**More Information**

Advisory: Changes to the Sophos Alert System Mailing List

# PCCW Responsible for YouTube Outage

*<web-link for this article>*

Acting in concert with Pakistan's government and Pakistan Telecom, Hong Kong's largest ISP, PCCW blocked worldwide access to the popular YouTube video-sharing website for over an hour early Monday morning, Hong Kong time. Two mistakes were blamed for the problem.

The incident occurred after the Pakistan Telecommunications Authority, acting on a policy set by the Pakistan Ministry of Information Technology, instructed ISPs in Pakistan to block YouTube because, "of videos depicting humiliation of the Prophet that were blasphemous in nature" last Friday. Pakistan Telecom implemented the ban by adding a rule to their routers that directed traffic to the YouTube IP address range to a black hole. The first mistake was that the rule used a more specific address range than that used by YouTube itself. The BGP routing protocol therefore regarded the new rule as the "best route" to YouTube, which should be propagated to other routers. The second mistake was that PCCW, Pakistan Telecom's ISP, blindly trusted the information provided by their routers and PCCW propagated the route to the rest of the world.

The problem was fixed when the rules were corrected by the ISPs. The Pakistan Telecommunications Authority has since lifted its ban on YouTube. There have been no reports of economic devastation due to the lack of access to cute, silly, badly focussed and irreligious videos.

**More Information**

Pakistan blocks YouTube
PCCW blacks out YouTube
Insecure routing redirects YouTube to Pakistan
Pakistan lifts the ban on YouTube

# Malaysia funds F-Secure ICT Research

*<web-link for this article>*

Strengthening the ties between Malaysia and Finland, Malaysia's Multimedia Development Corporation (MDeC) has provided F-Secure with a research grant of approximately US$1.7million establishing special projects with MSC Malaysia. The purpose of the R&D projects funded by the grant is to further Malaysia's development as one of the world's best environments for multimedia and ICT (Information, Communication, and Technology).

Left to right: F-Secure's Ingvar Fröiland, Finnish Ambassador Mr. Lauri Korpinen, MDeC Senior VP Dato' Narayanan Kanan

A special signing ceremony took place in F-Secure's Kuala Lumpur Security Lab, with Finnish Ambassador Mr. Lauri Korpinen, MDeC Senior VP Dato' Narayanan Kanan and F-Secure's Ingvar Fröiland.

**More Information**

MDeC Signing Ceremony
The Multimedia Development Corporation (MDeC)

# Kaspersky is first AV Certified on Win 2008 Server

Kaspersky Lab has announced that its antivirus solution Kaspersky Anti-Virus 6.0 for Windows Server Enterprise Edition is the first to earn a Windows Server 2008 software certification. Windows Server 2008 certification guarantees that Kaspersky Anti-Virus 6.0 for Windows Server Enterprise Edition is fully compatible with this platform and provides the highest level of integration with its technologies. Kaspersky Anti-Virus 6.0 for Windows Server Enterprise Edition was one of more than 300 applications that were eligible for certification based on participation in the Microsoft Early Access Program (EAP) for Windows Server 2008 Software Certification.

"Microsoft is very pleased that Kaspersky Labs is a leading innovator, developing solutions that take advantage of the advanced security and core functionality of Windows Server 2008," said Steve Bell, senior product manager of Windows Server marketing at Microsoft. "By certifying their anti-virus solution, Kaspersky Lab is helping customers deploy their solutions on Windows Server 2008 with confidence." Kaspersky Anti-Virus 6.0 for Windows Server Enterprise Edition supports the Server Core installation mode and utilizes new and advanced Windows Server 2008 technologies such as Terminal Services, Remote Applications and Terminal Services Gateway, allowing for further optimization of malware scanning processes.

"Today Windows Server 2003 is the most popular operating system for servers in the world. We believe that Windows Server 2008 will eventually surpass its predecessor and become the

new common standard for corporate servers," says Alexey Kalgin, deputy product marketing director at Kaspersky Lab. "And we are proud that we are the first IT-security company in the world to offer its clients a solution which is certified for Windows Server 2008."

Windows Server 2008 software certification consists of approximately 100 tests that independently confirm an application's compliance with best practices for compatibility, security, reliability, and availability on the new platform, while ensuring the software performs in a 64-bit environment. The certification identifies top-performing technologies that are ready to deploy in mission-critical environments. Details about Windows Server 2008 software certification, its test framework, and the Early Access Program are available at www.innovateonwindowsserver.com.

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/