

## Contents

Contents.....	1
UK Government to Allow Remote Searches.....	1
Wireless Reminder .....	2
Views on the Control of Obscene and Indecent Articles Ordinance .....	2
Introduction .....	2
Copyright, Privacy, Obscenity and Free Speech .....	2
Control of the Internet .....	3
ISP Responsibility .....	3
Provision of Blocking Lists.....	4
Community Standards .....	5
The Human Body is Not Indecent.....	5
Depictions of Legal Activities are Not Obscene .....	5
Conclusion.....	5
References .....	6

## UK Government to Allow Remote Searches

[<web-link for this article>](#)

The British newspaper, the Sunday Times has [reported](#) that the Home Office has quietly adopted a new plan to allow police across Britain routinely to hack into people's personal computers without a warrant. Under the rules, a remote search can be permitted if a senior officer says he "believes" that it is "proportionate" and necessary to prevent or detect serious crime — defined as offences punishable by a jail sentence of over three years.

The police could use many of the techniques currently used by criminals - such as exploiting vulnerabilities, installing keyloggers or enticing the suspect to execute a trojan sent by email. Such attempts could trigger protection software, such as anti-virus and firewalls, which would be unable to distinguish between criminal and police unauthorised access attempts. This issue was [raised by Sophos](#) in 2001 when information about the FBI "Magic Lantern" Trojan horse was revealed.

Yui Kee Chief Consultant Allan Dyer commented, "I think this is a dangerous proposal. Law enforcement should justify their actions to a competent authority before, and their actions subject to open review afterwards. There will be circumstances where covert surveillance is necessary, but the officers concerned will have reasons, and be able to explain them to a magistrate. What is the justification for not requiring a warrant? What will the next stage be? If access is blocked by security software, will the Police then demand powers to arrest users of anti-virus software and firewalls on the grounds they are 'preventing a legal Police search'?"

### More Information

[Police set to step up hacking of home PCs](#)

[As if warrantless wiretapping wasn't bad enough](#)  
[Police look to hack citizens' home PCs](#)  
[UK police plan to increase remote searching of home computers](#)  
[Police set to step up hacking of home PCs](#)  
[Eye spy with my piggy eye](#)  
[Sophos voices concern about FBI's Magic Lantern e-bug](#)  
[FBI Spy Software: "Magic Lantern"](#)  
[Home Office denies remote snooping plan](#)  
[Euro-Police Hacking Goes Out of Control](#)

## Wireless Reminder

[<web-link for this article>](#)

Cartoonist J. D. "Iliad" Frazer has a [reminder](#) for anyone setting up a wireless access point, particularly in crowded, high-rise environments.

### More Information

[Cartoon for Jan 05, 2009](#)

## Views on the Control of Obscene and Indecent Articles Ordinance

Personal Submission by Allan G. Dyer

### Introduction

This submission addresses the review of the Control of Obscene and Indecent Articles Ordinance (COIAO), announced by the Hong Kong Government on 3 October 2008. The areas covered include the limited scope of the review, and the consequential problems; the challenge of a media-rich world; and the standards that should be applied.

### Copyright, Privacy, Obscenity and Free Speech

It is clear that different people hold a wide range of views on what personal information (including images) they want to record and, optionally, make public, and the view might change according to the circumstances. Similarly, there are many views on public decency and obscenity, and the location can change the standards. In the current situation, laws intended for other purposes are sometimes used to try to address these emerging issues. In the early stages of the Edison Chen scandal, it was suggested that websites publishing the photos should be prosecuted under the COIAO, despite the fact that the images were of a similar nature to many erotic images on the internet. Should an obscenity law be used to protect privacy? Now, copyright law is being used against the perpetrators, but copyright was originally intended as a trade: creators get exclusive rights for a limited period and Society benefits from the creations when copyright expires and they pass into the public domain. Why should that be used for images that were intended solely for private enjoyment?

In the words of the Review website, "The policy intention of the COIAO is to preserve the free flow of information and safeguard the freedom of expression enjoyed by Hong Kong people on the one hand, and to reflect standards of public decency as they should apply particularly to articles intended for young and impressionable people on the other", unfortunately, in limiting the scope of the review to the COIAO, the complexity and inter-relatedness of the issues cannot be addressed, and the result will be failure.

A new Review should be launched, with a scope that covers all the closely related areas: Telecommunications and the role of ISPs, Privacy, Copyright, and Obscene and Indecent articles.

## Control of the Internet

On the one hand, the internet is a morass of pornography, misinformation and rubbish and we need to protect vulnerable members of our society; on the other hand, a number of Hong Kong ISPs are imposing terms and conditions on their users that stifle free speech and freedom of expression. On the gripping hand<sup>viii</sup>, the internet is, without doubt, the largest and most powerful information resource in the world, a society that cripples it will cripple its own development and position on the world stage.

I present my letter<sup>vii</sup>, published in the South China Morning Post, 7<sup>th</sup> November 2008:

As a parent, I adopt a two-fold approach to protecting my children from obscene matter on the internet: first, the computer is in the lounge, discouraging deliberate attempts to access such material; second, I have filtering software installed, preventing accidental access. Time and willingness to discuss what they have seen or read is also vital... one child-friendly website encouraged children to report "bad language", I had to explain this did not include misspellings.

However, we cannot blindly delegate our responsibilities to commercial companies, whether that is the developers of filtering software or ISPs. The software might be developed in, and therefore reflect the views of, a country that considers violence less damaging than sex, that has no gun control, and consequently a high level of gun crime and that fears other religious views. Hong Kong ISPs are already attempting to censor their customers: one ISP, Pacnet, in its terms and conditions prohibits content that "denounce religious or political beliefs". In a Democratic Society we have another phrase for that, "free speech, debate and discussion".

We need the technical expertise of software developers and ISPs to help us control harmful material, but the decisions about what is harmful is a matter for Society to decide. Therefore, the Control of Obscene and Indecent Articles Ordinance should establish a mechanism whereby the blocking lists used by ISPs and filtering software can be reviewed, challenged and modified in accordance with our standards of public decency.

To expand on the two areas: ISP responsibility; and provision of blocking lists:

### ISP Responsibility

ISPs are Telecommunications Service Providers, licensed under the Telecommunications Ordinance (TO). At present, they have free rein to set whatever terms and conditions they like. In some cases, possibly because of the concerns of their legal teams, they have set very restrictive conditions, the following examples are from Pacnet's Terms and Conditions<sup>1</sup>:

7.9 The Subscriber warrants and undertakes to Pacnet that: -

...

7.9.3 no part of the Subscriber Content, the Subscriber Equipment (if applicable) or the Subscriber Service is or will be in breach of any Applicable Law;

...

7.9.5 no part of the Subscriber Content or the Subscriber Service or the Subscriber Website denounces or will denounce religious or political beliefs;

7.9.6 no part of the Subscriber Content or the Subscriber Service or the Subscriber Website is or will be indecent, obscene, seditious, harassing, abusive, threatening, harmful, vulgar, pornographic, offensive or of doubtful propriety, likely to

encourage crime, public disorder, violence or hatred or likely to damage public health, safety or morals;

Clause 7.9.3 is, surely, sufficient to protect Pacnet against unreasonable responsibility for their user's content. The additional clauses, 7.9.5 and 7.9.6 are attacks on freedom of expression.

Clause 7.9.5 is a direct attack on free speech. If you prohibit denouncements, then you are implicitly declaring there to be only ONE TRUE point of view. In fact, many religions inherently denounce other religions (e.g. "there is no God but Allah", "none shall come to the Father except through me"). Please note that, in the extent that it offers a viewpoint on public policy, and criticises other views, this submission itself is a "political denouncement", and therefore, under a strict reading of the clause, could not be published via Pacnet's service. Clause 7.9.6 unreasonably restricts users' freedom to express themselves through indecent and vulgar content.

Of course, these clauses are not generally enforced. This is no reason to claim that they do not restrict free speech, quite the reverse, as an unknown, unaccountable group selectively applies them, they can be used to control and direct "free" speech in Hong Kong.

Therefore, the TO should be amended to:

- i. Prevent ISPs, as licensed telecommunications service providers, from restricting the content they carry, other than by requiring it to be legal.
- ii. Provide for, and require, technical cooperation between law enforcement authorities and ISPs so that illegal material can be investigated and taken down efficiently.
- iii. Give ISPs immunity from prosecution for content where they have merely acted as a carrier.

These changes should provide ISPs with the legal environment to do their job as a carrier without the pernicious Terms and Conditions they currently consider necessary for their own protection.

### **Provision of Blocking Lists**

As indicated in my letter to the South China Morning Post, as a parent I use blocking software to assist in controlling the content my children access, but I am aware that the software, and the lists of restricted sites, are developed by a privately-held company in a foreign country. I have limited information on how they research their lists, and there is no accountability – if I object to a classification, there is no transparent appeal mechanism. This is not a groundless fear; there are reports that some blocking software companies introduce a religious bias<sup>ix,x,xi</sup>.

A Blocking List for Hong Kong could be developed without unnecessarily duplicating research work:

- Blocking software providers are invited to submit their lists to the HK Government (perhaps TELA or OAT would be the appropriate body)
- The HK Government consolidates the lists, packages the consolidated list using tools provided by each software provider, and publishes them for download by the public.
  - If a list shows an obscene site located in Hong Kong, it can be referred to the Police for immediate investigation
- Members of the public can download the HK list, and use it with the blocking software of their choice.
- If they find "misclassifications", members of the public can submit sites to the Government, for review according to HK's standards. The results of the reviews are used to update the lists.
- When enforcement results in objectionable material being removed from an otherwise non-objectionable site (e.g., removal of offensive posts from a forum), the Government can report the removal to the software developers so that access to non-objectionable material is not unnecessarily restricted.

This scheme depends on the willingness of at least one software developer to cooperate with the HK Government. The HK list, and the software that permits its use, could be promoted to HK users, and it should become the recommendation of the Education Department for school use. Even so, Hong Kong's population might seem too small to be attractive to marketers. However, software developers are aware of their apparent lack of accountability, those who are not trying to push their own agenda might welcome the chance to prove their impartiality, and use their cooperation with the HK Government in their worldwide marketing. In any case, it would be premature to dismiss this proposal without discussing it with the software developers.

## **Community Standards**

The OAT has made a number of controversial decisions in recent years, including forcing the cover-up of a copy of Michelangelo's David, conflicting decisions in the Edison Chen scandal, and the Chinese University student newspaper incident. It is easy to perceive the OAT as out-of-touch with the general public, particularly when comparing their decisions to material that is freely available online, and the posts of Hong Kong people in 'racy' forums. Surely the behaviour of Hong Kong people on the internet is part of our community standards?

To make the OAT more relevant, its membership must be expanded. The people participating in adult forums are adults participating in adult activities, they would not want children involved and the public-spirited among them should be willing to contribute to the ongoing discussion on the boundaries between unrestricted, indecent and obscene articles.

About the standards themselves, I offer two principles:

### **The Human Body is Not Indecent**

The human body is a beautiful thing; it is not, in itself, indecent. The failure of the OAT to appreciate this was the cause of the controversy in the Michelangelo incident. Children do not need to be protected from seeing people; young children are not attracted to naked images. Young people entering puberty do become interested, but by that stage, they should be learning about human reproduction. Banning minors from seeing naked bodies gives it the lure of the forbidden, hampers mature discussion, and, in the rare worst case, allows perverts to manipulate young victims.

Particularly paradoxical is the treatment of breasts. We do not require babies to be blindfolded while feeding, so why are images of breasts deemed indecent?

Nakedness and sexuality are different. Parents know that toddlers have a strong defence against adult sexual behaviour: a toddler might get quite upset by two adults hugging, fully-clothed, particularly if they are parents. There is also the apocryphal story that, in Victorian times, a young man might get quite excited by a glimpse of a lady's ankle. Minors should be protected against depictions of sexual activity that are beyond their level of psychological development and biological education, but defining that is a difficult problem.

### **Depictions of Legal Activities are Not Obscene**

If an activity is legal, why should a recording, image or other depiction of that activity, made with the consent of the participants, be deemed illegal?

## **Conclusion**

Information technology has, and still is, changing how we create and disseminate information, presenting new challenges to old laws. That people wish to create material that may be indecent or obscene is not new (see the Cerne Abbas Giant<sup>xiv</sup>, for example), but the ease with which such material can be created, distributed and misused is changing beyond recognition. The review of the COIAO is overdue, but to consider it, and the effects on freedom of expression, without also reviewing the Personal Data Privacy Ordinance and the Telecommunications Ordinance is unwise.

## References

- i. Pacnet's General Terms and Conditions  
[http://corporate.pacific.net.hk/en/terms/general\\_tc\\_v3.php](http://corporate.pacific.net.hk/en/terms/general_tc_v3.php)
- ii. Copyright, Privacy, Obscenity and Free Speech in a Media-Rich World  
<http://articles.yuik.com.hk/newsletter/2008/12/b.html>
- iii. Topless in Tai Po, in this weather?  
[http://www.thestandard.com.hk/news\\_detail.asp?pp\\_cat=21&art\\_id=75615&con\\_type=1&d\\_str=20081211](http://www.thestandard.com.hk/news_detail.asp?pp_cat=21&art_id=75615&con_type=1&d_str=20081211)
- iv. Pacnet Refuses to Discuss its Censorship  
<http://articles.yuik.com.hk/newsletter/2008/11/a.html>
- v. Why Should the Government Curtail Free Speech When ISPs Will Do It?  
<http://articles.yuik.com.hk/newsletter/2008/10/f.html>
- vi. An obscene threat to all  
[http://www.thestandard.com.hk/news\\_detail.asp?pp\\_cat=15&art\\_id=45019&sid=13727795&con\\_type=1](http://www.thestandard.com.hk/news_detail.asp?pp_cat=15&art_id=45019&sid=13727795&con_type=1)
- vii. How can children be protected from obscene material online?  
[http://articles.yuik.com.hk/published/scmp/protectchild\\_0811.html](http://articles.yuik.com.hk/published/scmp/protectchild_0811.html)
- viii. Gripping hand [http://en.wikipedia.org/wiki/Gripping\\_hand](http://en.wikipedia.org/wiki/Gripping_hand)
- ix. eSN Exclusive: Report cites possible religious bias in school web filters  
<http://www.eschoolnews.com/news/top-news/index.cfm?i=34293&CFID=5235322&CFTOKEN=31246683>
- x. Benjamin Edelman's lawsuit FAQ  
<http://www.aclu.org/privacy/speech/14911res20020725.html>
- xi. Filtering Software: The Religious Connection  
<http://www.cyberbully.org/onlinedocs/documents/religious1.php>
- xii. Ethics, Safety, and Security in the IT Curriculum for Schools  
<http://articles.yuik.com.hk/conferences/HKICC/EthicsSafetySecurity/>
- xiii. Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal  
<http://articles.yuik.com.hk/newsletter/2008/02/a.html>
- xiv. Cerne Abbas Giant  
[http://maps.google.com/maps?f=q&source=s\\_q&sll=37.0625,-95.677068&sspn=28.114729,55.107422&ie=UTF8&ll=50.813592,-2.474708&spn=0.001366,0.003363&t=h&z=18](http://maps.google.com/maps?f=q&source=s_q&sll=37.0625,-95.677068&sspn=28.114729,55.107422&ie=UTF8&ll=50.813592,-2.474708&spn=0.001366,0.003363&t=h&z=18)



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@yuik.com.hk](mailto:info@yuik.com.hk)  
<http://www.yuik.com.hk/>

<http://www.yuikee.com.hk/>

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

**E-Learning**

- Content & Curriculum Development
- Training

**Security**

*Your  
Peace of Mind  
Is Our  
Commitment*

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

**Education**

- Project Development & Management
- Educational Software Distribution

<http://education.yuikee.com.hk/>