MAYER·BROWN JSM

Article

Controversy Continues Over Singapore Licensing Requirements for Online News Site

Gabriela Kennedy
Karen Lee

Gabriela Kennedy
Partner
+852 2843 2380
gabriela.kennedy@mayerbrownjsm.com

Karen Lee
Associate
+852 2843 4452
karen.hf.lee@mayerbrownjsm.com

This article first appeared in the 2014 Issue 1 of *Computer and Telecommunications Law Review.*

The new Singapore online licensing requirements that came into force on 1 June 2013, has led to a number of protests against this perceived threat to freedom of speech. For example, in June 2013, 162 websites staged a twenty-four hour online "black out" and about 1,500 people attended a rally in Hong Lim Park. Lately, however, the protesters are taking a more "cyber" approach to their protests, with several news and government websites being hacked and messages posted on their webpages.

The question is, why are people protesting against the new online licensing requirements, what websites have been hacked in protest, and what actions have or could the government take in response to these cyber attacks? This article attempts to address each of these questions.

The New Licensing Requirements

Online news sites must now apply to Singapore's Media Development Authority (**"MDA"**) for a new individual licence, if they report regularly on matters relating to Singapore and are accessed by a significant number of Singapore readers. What constitutes "regular" and "significant" has been quantified by the MDA, so that online news sites which meet the following criteria will need to obtain a new licence on an annual basis:

1. They publish a minimum of one article per week in respect of Singapore's news and current affairs over a 2 month period; and
2. They have a minimum of 50,000 visitors per month from unique IP addresses located in Singapore, over a 2 month period.

What amounts to Singapore news and current affairs has been described by the MDA as broadly including any programme (whether or not it is presenter-based or whether or not it is provided by a third party) that contains "any news, intelligence, report of occurrence, or any matter of public interest, about any social, economic, political, cultural, artistic, sporting, scientific or any other aspect of Singapore in any language (whether paid or free and whether at regular interval or otherwise) but does not include any programme produced by or on behalf of the Government"[1].

[1] "Fact Sheet – Online news sites to be placed on a more consistent licensing framework as traditional news platforms" published by the MDA on 28 May 2013.

The applicant for a new individual licence must put up a performance bond of SG$50,000 (about US$ 40,116) and must remove within twenty-four hours any content that is found by the MDA to be in breach of its standards.

According to the MDA, if it determines that a website meets the above criteria then it will formally notify and work with the operator to move it to a new individual licence. Prior to such notification, these websites will be automatically class-licensed under the Singapore Broadcasting Act. So far, the MDA have only listed 10 websites that require a new individual licence, which includes channelnewsasia.com, businesstimes.com.sg and sg.news.yahoo.com. However, many believe that these 10 websites are just the beginning. It will essentially be up to the MDA's discretion to determine whether or not a news site falls within the scope of the new licensing regime.

The Concerns

The MDA insists that the new licensing requirements are merely intended to provide greater clarity on existing requirements and to bring online news sites in line with other news platforms.

However, major concerns have still been raised regarding the following:

1. The potential broad scope of the new licensing requirements, which may theoretically apply to a wide range of sites, such as a popular blog run by an individual that regularly reports on upcoming social and entertainment events in Singapore;
2. The ability to afford the SG$50,000 performance bond, which may effectively mean the shutting down of popular news sites or blogs run by small organisation or individuals that are required to obtain a new individual licence, but which are unable to do so due to their inability to pay the large performance bond; and
3. The requirement to remove any material that the MDA finds "objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws[2]", within the tight deadline of twenty-four hours, failing which the MDA may impose fines or may suspend or revoke the website's licence.

The Protests

The above concerns, and the alleged impact they may have on freedom of speech, has resulted in recent hackings on government and news websites.

The first "attack" occurred against the website of Ang Mo Kio Town Council on 28 October 2013, where a message and an image of the Guy Fawkes mask (the image associated with the activist group, Anonymous) was posted by a person calling himself the "Messiah".

A few days later, the Straits Times was also hacked, and a message posted by the "Messiah" on the Straits Times blog of one of its journalists, alleging that she had misled the Singapore people regarding her report on the YouTube video posted on 31 October 2013 by the "Messiah". In the YouTube video, the "Messiah", wearing the Guy Fawkes mask, claimed that he was linked to the activist group, Anonymous, and threatened cyber attacks against the government if it did not reconsider the new licensing requirements.

The Singapore Prime Minister's official website was also hacked several days later, and an image of the Guy Fawkes mask was posted with the words "it's great to be Singaporean today". Other alleged incidents of hacking were also reported.

On 4 November 2013, James Raj Arokiasamy was arrested and later charged under the Computer Misuse and Cybersecurity Act (**"CMCA"**) (and also faced separate drug charges), for allegedly hacking into the Ang Mo Kio Town Council's website and operating under the name the "Messiah". The case against him is set to be heard on 26 November 2013.

James Raj Arokiasamy is also suspected of being responsible for hacking the Straits Times website, the People's Action Party Community Foundation website and the website for the co-founder of the City Harvest Church. The other hacking incidents are believed to have been carried out by other unrelated individuals, also adopting the same moniker of the "Messiah". Several other suspects have been brought in for questioning, and are apparently assisting the police in their investigations.

[2] MDA's Internet Code of Practice.

The Government's Powers Against Hackers

The main legislation that the government can rely on against hackers is the CMCA (formerly the Computer Misuse Act). Under Section 5(1) of the CMCA, a hacker can be arrested and charged with the criminal offence of making an unauthorised modification to the contents of a computer. If found guilty, the hacker may be liable to a maximum fine of SG$10,000 (about US$8,000) and/or up to 3 years imprisonment or, in the case of a second or subsequent conviction, a maximum fine of SG$20,000 (about US$16,000) and/or up to 5 years imprisonment. James Raj Arokiasamy was charged with such an offence.

To assist in the police investigations into the hackings, the Minister of Home Affairs may also choose to exercise its new powers under the CMCA. On 14 January 2013 an amendment to the CMCA was passed, which gave the Minister additional powers to prevent, detect and counter cyber attacks on critical infrastructures (i.e. essential information systems and assets, which includes telecommunication networks, banking infrastructure, water, electricity, gas and public transportation systems). The threat must relate to Singapore's national security, essential services, defence or foreign relations.

The government can now require a person or organisation (e.g. telecommunications companies, website operators, etc.) to take specific steps towards preventing, detecting or countering cyber threats, where it relates to computers, computer services, or class of computers or computer services. Such steps may include requiring a specified person to:

i. Direct another person to provide information necessary to identify, detect or counter any threat;
ii. Provide information obtained from a computer controlled or operated by the specified person, which is necessary to identify, detect or counter any threat;
iii. Provide a report on any cybersecurity breaches or attempted breaches that match the description specified by the Minister; and
iv. Exercise the powers granted under Sections 39(1) and (2) and 40(2) of the Criminal Procedure Code, which includes accessing any computer that the specified person has reasonable cause to suspect has been used in connection with an offence for the purpose of investigating an offence.

The specified person will be granted immunity from any civil or criminal liability that it may incur when complying with the Minister's order. However, failure to comply may result in a maximum fine of SG$50,000 and/or a maximum of 10 years imprisonment.