Lim Siong Khee v Public Prosecutor
[2001] SGHC 69

Case Number : MA 256/2000

Decision Date : 09 April 2001

Tribunal/Court : High Court

Coram : Yong Pung How CJ

Counsel Name(s) : Heikel Bafana and Isreal Louis Ismail (Alexander Charles Louis) for the appellant; David Khoo and April Phang (Deputy Public Prosecutors) for the respondent

Parties : Lim Siong Khee — Public Prosecutor

Criminal Law – Offences – Computer Misuse – Access to free web-based email account without authority – Whether consent of email account holder or system provider is determinative – ss 2(2), (5), 3(1), 8(1) Whether authorisation to relate to kind of access in question to data-Computer Misuse Act (Cap 50A, 1998 Ed)

Words and Phrases – "Without authority" – s 2(5) Computer Misuse Act (cap 50A, 1998Ed)

: This was an appeal against the decision of District Judge Siva Shanmugam, where he convicted the appellant, Mr Lim Siong Khee (`Mr Lim`), on the following charge:

> *You, Lim Siong Khee are charged that you, in the month of May 1999, in Singapore did knowingly cause Mailcity`s e-mail server to perform a function for the purpose of securing access without authority to the electronic mailbox of a Mailcity account holder with the user name `chongyc`, via remote dial-up access to the said server using the said user name and password without the consent of the account holder and you have committed an offence under section 3(1) of the Computer Misuse Act, Chapter 50A (Revised Edition 1998).*

The facts

Ms Chong Yan Cheng (`Ms Chong`) first met Mr Lim in December 1998. They went on a trip to Europe sometime in April 1999. Upon their return to Singapore, Ms Chong ended the relationship as she felt that they were incompatible. From April 1999 onwards, she started having problems logging into her email account, `chongyc[commat]mailcity.com` (`the email account`). She suspected that someone was tampering with her account. During this period, Mr Lim knew her movements and he made this known to her. He knew, for example, that she had stayed at Mariott Hotel with two of her friends on 8 and 9 May 1999.

On 9 May 1999, an email was sent out from the email account to three of Ms Chong`s friends. The email was titled `Special Relation`. The contents in the email were addressed to Ms Chong and they contained lurid details of her purported intimate relations with Mr Lim during their European trip. Ms Chong testified that when she confronted Mr Lim, he admitted that he had accessed the email account by guessing correctly that her password was her birthdate. He was also able to find out the new password even after she changed it by answering the hint question correctly. The answer to the hint question was also Ms Chong`s birthdate.

In his defence, Mr Lim admitted that he did access the email account, but claimed that he had Ms Chong`s consent to do so, as she had given him the password while they were in Europe.

Decision of the judge

The judge found that, on the forensic evidence, Mr Lim had accessed the email account on at least two occasions: when he sent the email titled `Special Relation` on 9 May 1999 and subsequently when he retrieved an email from one Ms Iris Tang to Ms Chong dated 10 May 1999, wherein she offered consolation and advice.

The judge found Mr Lim to be an unreliable witness. His explanations were inconsistent and far from satisfactory. In contrast, Ms Chong withstood the cross-examination and established herself as a truthful witness. Mr Lim`s claim that Ms Chong had given him the password was rejected. He was convicted and sentenced to five months` imprisonment.

The appeal

The offence involves s 3(1) of the Computer Misuse Act (Cap 50A, 1998 Ed) (`the Act`), which states:

> *Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access* ***without authority*** *to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both. [Emphasis is added.]*

Mr Bafana, who appears for Mr Lim, makes two main submissions. First, he submits that the legislative intent of the Act is that in determining whether access is `without authority`, it is the authorisation of the computer system owner or provider that is material. On the facts, Mailcity.com would be the party to determine whether access was authorised. There was no evidence at the trial that Mailcity.com did not authorise the appellant`s access. Instead, the focus was on the lack of consent from the email account holder, Ms Chong. Consequently, a key requirement of s 3(1) had not been proved.

The phrase `without authority` receives legislative attention at s 2(5) of the Act:

> *For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if -*
>
> *(a) he is not himself entitled to control access of the kind in question to the program or data; and*
>
> *(b)* ***he does not have consent to access*** *by him of the kind in question to the program or data* ***from any person who is so entitled*** *. [Emphasis is added.]*

Thus, the consent must come from a person who is entitled to access the data in question. In the case of free web-based email systems, the general understanding of both consumers and industry is

that it is the account holder who is entitled to access the data contained in the emails. This can be seen from the agreements of the major free web-based email systems. Mailcity.com is part of the Lycos Network, and [para] 8 of the Lycos Network Privacy Policy states:

> *The Lycos Network has security measures in place to attempt to protect against the loss, misuse and alteration of* ***your data under our control****. Only authorized employees have access to the information you provide us. Lycos has implemented strict rules on employees who have access to either the databases that store user information or to the servers that host our services ... [Emphasis is added.]*

The later part of the same paragraph also suggests that the account holder is the one who is responsible for and in control of the access to his account:

> ***You are ultimately responsible for the security of your Lycos Network ID and password****. Please take care when using and storing them. Lycos recommends that you do not divulge your password to anyone. You should log out of your browser at the end of each computer session to ensure that others cannot access your personal information and correspondence, especially if you share a computer with someone else or are using computer in a public place like a library or Internet cafS. [Emphasis added.]*

The same approach is taken by two of the most popular free web-based email systems: Hotmail (which is owned by Microsoft) and Yahoo! Mail. The user agreement between Microsoft and the Hotmail user states that the user agrees `to notify Microsoft immediately of any unauthorized use of your account or any other breach of security`. The onus is thus on the account holder to inform Microsoft if the account holder finds that there has been use of the account which has been unauthorized by the account holder. The Yahoo! Mail user agreement takes the same approach at [para] 5:

> *You are responsible for maintaining the confidentiality of the password and account, and are fully responsible for all activities that occur under your password or account. You agree to (a)* ***immediately notify Yahoo of any unauthorized use of your password or account*** *or any other breach of security, and (b) ensure that you exit from your account at the end of each session. [Emphasis is added.]*

Mr Bafana`s argument that it is Mailcity.com`s authorisation that is determinative faces a further obstacle in the form of s 8(1) of the Act. This provision makes it an offence for a person to knowingly and without authority disclose any password for the purpose of wrongful gain. In the speech of the Minister for Home Affairs, Mr Wong Kan Seng, at the Second Reading of the Computer Misuse (Amendment) Bill 1998, the Minister said in relation to s 8(1):

> *Clause 7 will introduce a new section ... to make it an offence for unauthorised disclosure of passwords by any person if he does so for any wrongful gain or for unlawful purpose or to cause wrongful loss.* ***It is possible for a system administrator to sell passwords to unauthorised users to enable free access and usage*** *... The proposed penalties for such offences are similar to the penalties applicable to interference or obstruction of lawful use of computer. [Emphasis is added.]*

The legislative intent is clear from the above speech. For the purposes of s 8(1), the system administrator is not the person who determines who is authorised to access accounts. Indeed, the system administrator himself can be criminally culpable if he sells passwords to other persons without the consent of the account holder. Whether access by a user is `without authority` under s 8(1) depends on the account holder, not the computer system owner or provider. The phrase `without authority` in s 3(1) must be similarly construed.

Mr Bafana`s second submission is that, in any event, there was a reasonable doubt whether Mr Lim lacked Ms Chong`s consent to access the email account. He relies mainly on Mr Lim`s allegations that he had intimate relations with Ms Chong, and that she gave him the password for him to help, when she had problems accessing her account in Europe. However, as the Public Prosecutor points out, first, there is no affirmative evidence that Ms Chong was in an intimate relationship with Mr Lim. Second, Ms Chong denied ever giving Mr Lim her password. Her story is that, after she discovered that her account had been accessed, she confronted Mr Lim, who confessed that he gained access by correctly guessing her password. The judge found Ms Chong a more credible witness than Mr Lim and held that consent had not been given. Nothing has been raised in this appeal which justifies overturning this finding of fact.

Even if Ms Chong had consented, I have serious doubts that this would have made a difference. In **R v Bow Street Metropolitan Stipendiary Magistrate, ex p Government of the United States of America** [1999] 4 All ER 1, the House of Lords held in respect of s 1 of the Computer Misuse Act 1990, which is substantially similar to our s 3(1), that on its true construction, s 1 is not concerned with authority to access per se, but rather with authority to access the actual data involved.

The language of our Act leads to the same conclusion. Section 3(1) of the Act states:

> *Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of **securing access without authority** to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both. [Emphasis is added.]*

The relevant interpretative provisions for s 3(1) are the following:

> *2(2) For the purposes of this Act, a person **secures access** to any program or data held in a computer **if** by causing a computer to perform any function he -*
>
> *(a) alters or erases the program or data;*
>
> *(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;*
>
> *(c) uses it; or*
>
> *(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner),*

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

...

2(5) For the purposes of this Act, ***access of any kind*** *by any person to any program or data held in a computer is unauthorised or done* ***without authority*** *if -*

(a) he is not himself entitled to control ***access of the kind in question to the program or data*** *; and*

(b) he does not have consent to ***access by him of the kind in question to the program or data*** *from any person who is so entitled. [Emphasis is added.]*

Section 2(2) defines the phrase `access` by listing four different kinds of access. Section 2(5) defines access `without authority` as access of any kind where the person either does not have control of or consent to the access `of the kind in question to the program or data`. In other words, the authorisation must relate to the kind of access in question to the program or data. Thus, even if Mr Lim was given Ms Chong`s password to help her access her email account while they were in Europe, he had no authority whatsoever to access that account to send off lurid emails or to check on her personal movements and affairs.

In view of the above reasons, I dismissed Mr Lim`s appeal against his conviction.

Sentence

Mr Lim was sentenced in the court below to five months` imprisonment. At the appeal, it was submitted that this was manifestly excessive. In particular, Mr Bafana asked the court to take into consideration the fact that Mr Lim was a spurned lover who could not accept that the relationship was over. That he may be, but it does not mean that he can consistently enter into her email account to uncover every intimate detail of her personal life and use that information to stalk her or harass her, or to use the email account to send out contemptible emails, of such lurid details, that serve no other purpose than to totally destroy a young lady`s reputation. In my view, he was completely malicious and vindictive. I cannot imagine anything more despicable than what he did. Far from being excessive, I found the sentence of five months` imprisonment to be sorely inadequate and enhanced it to 12 months` imprisonment.

Outcome:

Appeal dismissed.