

**IN THE COURT OF FINAL APPEAL OF THE
HONG KONG SPECIAL ADMINISTRATIVE REGION**

FINAL APPEAL NO. 20 OF 2018 (CRIMINAL)
(ON APPEAL FROM HCMA NO. 454 OF 2016)

BETWEEN

HKSAR

Respondent

and

CHU TSUN WAI (朱峻瑋)

Appellant

Before: Chief Justice Ma, Mr Justice Ribeiro PJ,
Mr Justice Fok PJ and Mr Justice Cheung PJ,
Lord Hoffmann NPJ

Date of Hearing: 17 January 2019

Date of Judgment: 1 February 2019

JUDGMENT

Chief Justice Ma:

1. I agree with the judgement of Lord Hoffmann NPJ.

Mr Justice Ribeiro PJ:

2. I agree with the judgement of Lord Hoffmann NPJ.

Mr Justice Fok PJ:

3. I agree with the judgement of Lord Hoffmann NPJ.

Mr Justice Cheung PJ:

4. I agree with the judgement of Lord Hoffmann NPJ.

Lord Hoffmann NPJ:

5. On 12 October 2014 the appellant took part in a Distributed Denial of Service (“DDoS”) attack on the website of the Shanghai Commercial Bank. When you call up a website, your computer sends a “request” to the website server, i.e. the computer which supports the website, calling up the website page. If it is available, the website server will respond to the request by transmitting the page. When it appears on your screen, you may click on some service you want to access, for example, your bank account, and your computer will send another request, and so on. The capacity of the server to deal with requests at any given time (its “bandwidth”) is finite. The method of a DDoS attack is for a number of co-ordinated computers to send a very large number of requests at more or less the same time to exhaust the server’s bandwidth, thereby denying access to persons wishing to transact their ordinary business through the website and possibly causing the overloaded system to crash. In the present case the server received 504,592 requests within the space of an hour, of which 6,652 came within a space of 16 seconds from the appellant’s computer. But the attack was a failure because

the server had enough surplus capacity to prevent the attack from having any effect upon its other operations.

The Charge

6. The appellant was charged with criminal damage, contrary to section 60(1) of the Crimes Ordinance Cap 200, namely that he without lawful excuse damaged property belonging to another intending to damage such property or being reckless as to whether such property would be damaged. It is an offence punishable by a maximum of ten years imprisonment. The meaning of “damage any property” was given an extended meaning by a definition inserted into section 59 by the Computer Crimes Ordinance 1993 (Ordinance No 23 of 1993). A new subsection 59(1A) provided that in relation to a computer, damage to property included “misuse of a computer”. This phrase was in turn defined to mean:

- “(a) To cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
- (b) to alter or erase any program or data held in a computer or in a computer storage medium;
- (c) to add any program or data to the contents of a computer or of a computer storage medium...”

The Issue

7. The principal issue in this appeal is whether the appellant had caused the computer “to function other than as it has been established to function by or on behalf of its owner” within the meaning of paragraph (a) of section 59(1A).

The prosecution says that the bank, as owner, established its server to receive and respond to genuine requests for its services. Causing the computer to respond to requests which were sent only for the purpose of using up its bandwidth was causing it to function other than as the bank had established it to function. The appellant, on the other hand, said that the computer was established to receive and respond to requests. During the attack it responded to the appellant's and other requests exactly as it had been programmed to do. The attack caused no difference to the way it functioned.

The 1993 Ordinance

8. The Computer Crimes Ordinance 1993 created a number of crimes under various Ordinances in relation to computers. The simplest was the offence of unauthorised access to a computer by telecommunications (“hacking”), punishable by a fine and inserted into the Telecommunications Ordinance Cap 106 as section 27A. The offence is committed by a person who (1) by telecommunications (2) knowingly causes a computer to perform any function (3) to obtain unauthorised access to any program or data held in a computer. The offence is committed simply by obtaining unauthorised access through the internet (“by telecommunications”), whether on account of curiosity, malice or dishonest intent. It protects the privacy of ordinary computers. Websites, on the other hand, invite the public to access them. There may of course still be unauthorised access to a particular “program or data” on the websites contrary to section 27A but websites also require a different form of protection.

9. The new section 161 of the Crimes Ordinance dealt with obtaining access with intent to commit an offence, with a dishonest intent to deceive or with a view to dishonest gain or with a dishonest intent to cause loss.

10. Against this background, one can see that the extension of the concept of criminal damage in the Crimes Ordinance to misuse of computers was particularly important for the protection of websites. The definition of the offence does not require access as such to have been unauthorised. So it applies to computers which, through their websites, offer open access to the world. If the access was with dishonest intent, that is covered by section 161. The offence under section 60 is committed when, having obtained access to the computer through the website, one causes it to “function other than as it has been established to function by or on behalf of its owner”. The question therefore is how one describes the way in which it has relevantly been established to function by its owner. Mr Randy Shek, for the appellant, says it was established to, among other things, receive and respond to requests. Mr Ned Lai, for the prosecution, says it was established to provide banking services.

Proceedings in the lower courts

11. The principal issues before the magistrate (Mr Raymond Wong) and on appeal to the judge (Deputy High Court Judge Stanley Chan) were whether the appellant was the user of the computer at the time, and whether the appellant had participated in the attack intentionally or by accident. Both tribunals found that he was the user of the computer and had done so intentionally. These findings are not challenged. The magistrate dealt briefly with the construction of section 59(1A). He said (paragraph 70) that the appellant had added information to the bank’s computer within the meaning of paragraph (c). As to the question of intent, he said (paragraph 72) that the appellant had the intent to damage the bank’s computer, and also held (paragraph 73) that the appellant was at least “reckless” as to whether the bank’s computer would be damaged.

12. The reasons of the judge are likewise mainly given over to the question of whether the appellant intended to participate in the attack. He also dealt briefly with the question of construction. He said of paragraph (a) of section 59(1A) “obviously, over 500,000 ‘requests’ within 11 minutes would not be the established way of functioning of the computer under attack”. As to paragraph (c), he said that the requests had added data “even when they were of such minute amount”.

Paragraph (a)

13. I do not think that it is sufficient to say that the computer functioned as it had been established to do because it dealt with the attackers’ requests in accordance with what it had been programmed to do. Generally speaking, computers can only do what they have been programmed to do and such a narrow construction would deprive paragraph (a) of any effect. This conclusion is reinforced by the words “notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer”. Mr Shek was hard put to offer an example of an act which came within his construction of “other than as it has been established to function by ... its owner” which was not excluded by the following words. In my opinion the functions for which the computer is established to do are not so much concerned with the way it works (or fails to work) but what it was intended to *do*. The way it works depends upon how it was constructed by its manufacturer. But the statute is concerned with what the owner has set it up to do. The website and its server were established to provide banking services, not to deal with a multitude of requests made for no purpose except to inconvenience the bank and its customers and generate publicity for the attackers.

14. Although it is a decision on a different statute, there is some analogy with the decision of the English Divisional Court in *DPP v Lennon* [2006] EWHC 1201 (Admin) on the question of whether the owner of a computer consented to receive the equivalent of a DDoS attack in the form of a torrent of e-mails. The court said that his general consent to receiving emails -

“plainly does not cover emails which are not sent for the purpose of communication with the owner, but are sent for the purpose of interrupting the proper operation and use of his system.”

15. In my view, a DDoS attack is very appropriately described as a misuse of the bank’s computer. Mr Shek said that it was wrong to have regard to the use of the term “misuse of a computer” in construing the meaning of paragraph (a). “Misuse of a computer” is a defined expression. It means, and means only, what is stated in paragraphs (a), (b) and (c). I agree that the defined term cannot be used to enlarge the meanings of paragraphs (a), (b) and (c) but there is no reason why it cannot be considered when construing them. A defined expression is not usually an arbitrarily chosen word but intended as a broad description of a concept more precisely defined in the ensuing paragraphs. (See *Chartbrook v Persimmon* [2009] 1 AC 1101, 1112-1113). In such case, it may be used to elucidate any ambiguities in those paragraphs. Furthermore, paragraph (a) itself describes the offence as a “misuse” of the computer.

16. Mr Shek suggested that so broad a definition of the offence could cause injustice. But one must take into account the general defences to a charge of criminal damage and in particular the requirement that the “damage” must have been caused “without lawful excuse”. In particular, section 64(2)(a) of the Crimes Ordinance provides that it is a lawful excuse honestly to believe (whether reasonably or not) that the owner had consented or, if he had known, would have

consented, to the act in question. It seems to me that the Legislature was content to rely upon such general provisions to prevent any injustice being caused by the breadth of the definition of misuse of a computer.

17. I would therefore uphold the decision of the judge on paragraph (a).

Paragraph (c)

18. The appellant submitted that prosecution based its case before the magistrate solely upon paragraph (a). (Appellant's case paragraphs 86-87). There was no mention of paragraph (c) and the appellant adduced no evidence upon the question of whether data was added to the bank's computer or whether he could be said to have intended or been reckless as to whether this would happen. This objection appears to me well founded (see *HKSAR v Hau Tung Ying* (2011) 14 HKCFAR 453, 470). I therefore consider that reliance upon paragraph (c) would be unjust to the appellant. But for the reasons I have given in relation to paragraph (a), I would dismiss the appeal.

Chief Justice Ma:

19. For the above reasons, the appeal is dismissed.

(Geoffrey Ma)
Chief Justice

(R A V Ribeiro)
Permanent Judge

(Joseph Fok)
Permanent Judge

(Andrew Cheung)
Permanent Judge

(Lord Hoffmann)
Non-Permanent Judge

Mr Randy Shek and Mr Geoffrey Yeung, instructed by Eric Yu & Company, for
the Appellant

Mr Ned Lai, SADPP, Ms Mickey Fung, SPP and Mr Ivan Cheung, SPP, of the
Department of Justice, for the Respondent