

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

FINAL APPEAL NO. 22 OF 2018 (CRIMINAL)
(ON APPEAL FROM HCMA NO. 466 OF 2017)

BETWEEN

SECRETARY FOR JUSTICE

Applicant

and

CHENG KA YEE (鄭嘉儀)

1st Respondent

TSANG WING SHAN (曾詠珊)

2nd Respondent

WONG PUI MAN (黃佩雯)

3rd Respondent

U LENG KOK (余玲菊)

4th Respondent

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

Date of Hearing: 26 February 2019

Date of Judgment: 4 April 2019

J U D G M E N T

Chief Justice Ma:

1. I agree with the judgment of Mr Justice Robert French NPJ.

Mr Justice Ribeiro PJ:

2. I agree with the judgment of Mr Justice Robert French NPJ.

Mr Justice Fok PJ:

3. I agree with the judgment of Mr Justice Robert French NPJ.

Mr Justice Cheung PJ:

4. I agree with the judgment of Mr Justice Robert French NPJ.

Mr Justice French NPJ:

Introduction

5. It is an offence against s 161(1)(c) of the Crimes Ordinance (Cap 200) for a person to obtain access to a computer with a view to dishonest gain for that person or for another. Primary school teachers and a friend who used phones and a computer to transmit to third parties questions to be used in competitive admission interviews were charged under the provision. They were acquitted of the charges. The question on which this appeal turns is whether or not a person can commit the offence when the only computer being used belongs to that person. For the reasons that follow, the answer is no and the appeal by the Secretary for Justice must be dismissed.

Factual Background

6. The respondents to this appeal were three teachers at the Church of Christ in China Heep Woh Primary School (the first three named respondents) and a teacher in another school (the fourth respondent) who had been a classmate of the second respondent.

7. Children could seek admission to the school, which was government subsidised, through an open admission process involving a competitive interview-based assessment. The first three respondents were among teachers at the school who were to conduct the open admission interviews on 14 June 2014. They were briefed on the day before the interview by the teacher in charge of the process for the 2014/2015 academic year.

8. Each of the teachers being briefed, including the three respondents, was provided with a plastic folder containing a copy of the Interview Questions and the Marking Scheme. The first and second respondents used their mobile phones to take photographs of the contents of the folders at the briefing and sent the photographs to third parties using WhatsApp. The first respondent sent the photographs to a friend in her church. The second respondent sent her photographs to the third respondent in the course of the briefing. The third respondent used a school computer to type up the interview questions into a Word document which was then sent by email on the school computer to the second respondent and, using her mobile phone, to a friend. The second respondent sent the Word document by email to the fourth respondent and a friend. The fourth respondent used her mobile phone to take photographs of the questions and transmitted them to two friends by WhatsApp.

9. Each of the respondents was charged with an offence against s 161(1)(c) of the Crimes Ordinance (Cap. 200). The charges against each were in common form, namely:

“Obtaining access to a computer with a view to dishonest gain for himself or another, contrary to s 161(1)(c) of the Crimes Ordinance, Cap 200.”

The brief particulars of the offences differed slightly between the respondents and were as follows:

- “• [The first respondent] on 13 June 2014, in Hong Kong, obtained access to a computer, namely, a Xiaomi smartphone with a view to dishonest gain for another.
- [The second respondent] on 13 June 2014, in Hong Kong, obtained access to a computer, namely, a Samsung smartphone, with a view to dishonest gain for another.
- [The third respondent] on 13 June 2014, in Hong Kong, obtained access to a computer, namely, a desktop computer of the Church of Christ in China Heep Woh Primary School, with a view to dishonest gain for another.
- [The fourth respondent] on 13 June 2014, in Hong Kong, obtained access to a computer, namely, an iPhone, with a view to dishonest gain for another.”

10. The events of 13 June 2014 and the conduct of the respondents as set out above were not in dispute at trial, which proceeded before Permanent Magistrate, Ms Veronica Heung. On 25 February 2016, the Magistrate acquitted all four respondents. She did so on the bases that:

- (i) She had a reasonable doubt that the teacher in charge had ever mentioned at the briefing seminar the need for confidentiality in relation to the Interview Questions.
- (ii) In each case she was not satisfied beyond reasonable doubt that the necessary element of dishonesty had been made out.

11. The appellant applied to the Magistrate asking her to review her decision to acquit pursuant to s 104 of the Magistrates Ordinance (Cap 227). On 26 September 2016, the Magistrate confirmed her decision. The appellant then applied to the Magistrate to state a case on a point of law pursuant to s 105 of the Magistrates Ordinance (Cap 227). Under that section where it is desired to question by way of appeal any order or determination on the ground that it is erroneous in point of law, a party to the charge or the Secretary for Justice may apply to the magistrate to state and sign a case setting forth the facts and the grounds upon which the order or determination was granted for the opinion of a judge.

12. The Magistrate stated a case setting out the questions arising from it for the opinion of the Court of First Instance. Despite the requirement for a point of law, the questions largely went to the Magistrate's factual conclusions. They were as follows:

Question 1: Did I err in finding that D1-4 might not be aware that the questions distributed at the briefing were the actual questions to be asked at the Interview?

Question 2: Did I err in finding that D1-4 might not be aware that the questions distributed at the briefing were confidential in nature?

Question 3: Did I err in finding that D1-4 might not have the requisite *mens rea* to dishonest gain for another?

Question 4: Did I err in acquitting each of D1-4 on the facts and the evidence of this case in that such verdicts were against the evidence properly considered and assessed, and were perverse in the sense as recognized in *Li Man Wai v Secretary for Justice*?¹

Question 5: Did I err in failing to give proper consideration to the evidence of this case and in taking irrelevant matters into account in maintaining my decision to acquit D1-4 in the review hearing?

13. The appeal came on for hearing before Deputy High Court Judge C P Pang, who delivered judgment on 6 August 2018.² As appears from the Stated Case none of the questions raised any issue of the proper construction of s 161(1)(c). However, after the oral hearing the Judge raised with counsel the legal question whether the charges against the four respondents were appropriate and, in particular whether their acts amounted to the *actus reus* of “[obtaining] access to a computer” within the meaning of s 161(1)(c). The parties made further written submissions on that point. The appellant’s submission on the law as to the scope of the *actus reus* of the offence was quoted by the Judge:

“A person can commit the *actus reus* of obtaining access to computer in infinite ways, such as using a smartphone [which is now settled law a

¹ (2003) 6 HKCFAR 466.

² *Secretary for Justice v Cheng Ka Yee & Others* [2018] HKCFI 1809.

computer] to take upskirt photos of females or using it to send confidential information to others. Unauthorized extraction of information from a computer is but one way of obtaining access to it.”³

The Judge rejected that proposition as one which could lead to absurd consequences.

14. In delivering his decision, which is the subject of the appeal to this Court, Deputy Judge Pang referred to *Li Man Wai v Secretary for Justice* and the statement in that judgment that:

“...the law as it now stands does not punish all kinds of unauthorized access to computers, it only prohibits the unauthorized and dishonest extraction and use of information ...”⁴

He held that to prove the commission of the offence, the prosecution must prove the unauthorized extraction and use of information from a computer.⁵ The use by the first, second and fourth respondents of their own smartphones to take photographs and to receive/send them by WhatsApp were not unauthorized extractions and use of information from the computer.⁶ The use by the third respondent of the desktop computer to create the Word file was not unauthorized and she did not obtain or extract the Word file from the school’s computer system.

15. The Judge’s conclusions on the question of law he had raised made consideration of the five questions in the Stated Case moot. However, he went on to consider them briefly. He held that the magistrate had correctly applied the test for dishonesty in *R v Ghosh*.⁷ While the Judge might have come to a different

³ *Secretary for Justice v Cheng Ka Yee & Others* [2018] HKCFI 1809 [50].

⁴ (2003) 6 HKCFAR 466 [26].

⁵ *Secretary for Justice v Cheng Ka Yee & Others* [2018] HKCFI 1809 [68].

⁶ *Secretary for Justice v Cheng Ka Yee & Others* [2018] HKCFI 1809 [69].

⁷ [1982] EWCA Crim 2; [1982] QB 1053.

view, the magistrate, deciding on the facts as she found them, could not be criticised for her ruling that the prosecution had failed to prove the element of dishonesty beyond reasonable doubt. The Judge answered all five questions in the negative. The appeal from the magistrate's decision was dismissed.⁸

16. The appellant subsequently applied to Deputy Judge Pang for a certificate under s 32 of the Hong Kong Court of Final Appeal Ordinance (Cap 484) that a point of law of great and general importance was involved in his judgment to enable the appellant to appeal to this Court. The Judge, by an Order dated 6 September 2018, certified that the following point of law of great and general importance was involved in the case:

“Is the *actus reus* of the offence under section 161(1)(c) of the Crimes Ordinance, Cap 200 restricted to the unauthorized extraction and use of information from a computer?”

17. On 2 November 2018, the Appeal Committee of this Court granted leave to appeal from the Judge's decision on the basis that a point of law of great and general importance was involved in the case, namely:

“What is the scope of the *actus reus* of the offence under section 161(1)(c) of the Crimes Ordinance (Cap 200)? In particular, is it restricted to the unauthorized extraction and use of information from a computer?”

The Court also granted leave on the substantial and grave injustice ground, under s 32, for the appellant to contend, subject to the conclusion reached as to the foregoing point of law, that it is reasonably arguable that the finding as to lack of dishonesty was perverse.

⁸ *Secretary for Justice v Cheng Ka Yee & Others* [2018] HKCFI 1809 [82]-[83].

The Statutory Framework

18. The process of statutory construction begins with the text to be construed, identification of the relevant constructional choices it presents, a predisposition to choose an ordinary meaning, and a choice always informed by context and purpose. The statutory text in this case is s 161(1)(c) of the Crimes Ordinance (Cap 200), the provision under which the respondents were charged. Its immediate context is the section read as a whole and its location in the Ordinance.

19. The section appears as the last substantive offence-creating provision in the last part of the Ordinance, Part XIII entitled “Miscellaneous Offences”. There are only two offence-creating sections, namely s 160 which covers “loitering” and s 161 entitled “Access to computer with criminal or dishonest intent”. Section 161 provides:

“Access to computer with criminal or dishonest intent

- (1) Any person who obtains access to a computer—
 - (a) with intent to commit an offence;
 - (b) with a dishonest intent to deceive;
 - (c) with a view to dishonest gain for himself or another; or
 - (d) with a dishonest intent to cause loss to another,whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.
- (2) For the purposes of subsection (1) **gain** (獲益) and **loss** (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and—

- (a) **gain** (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and
- (b) **loss** (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has.”

20. The part of the text which is directly applicable to this appeal and defines the offence with which each of the respondents was charged therefore reads as follows:

“Any person who obtains access to a computer ... with a view to dishonest gain for himself or another ... whether on the same occasion as he obtains such access or on any other future occasion, commits an offence ...”

The Legislative History

21. The legislative history, including the Memorandum for Legislative Council and the Second Reading Debate, are referred to in order to ascertain the context and purpose of the provision under which the respondents were charged.

22. Section 161 was introduced into the Crimes Ordinance (Cap 200) by the Computer Crimes Ordinance No 23 of 1993. That Ordinance was described in its long title as:

“An Ordinance to clarify and amend the criminal law relating to the misuse of computers, and for related matters.”

It created new offences and broadened the range of existing offences.

23. In addition to s 161, the 1993 Ordinance enacted a new s 27A in the Telecommunications Ordinance (Cap 106), which relevantly provided:

“Unauthorized access to computer by telecommunications

- (1) Any person who, by telecommunication, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine...
- (2) For the purposes of subsection (1)—
 - ...
 - (b) access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and—
 - (i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;
 - (ii) he does not believe that he has been so authorized; and
 - (iii) he does not believe that he would have been so authorized if he had applied for the appropriate authority.”⁹

24. The Computer Crimes Ordinance No 23 of 1993 amended s 59 of the Crimes Ordinance (Cap 200), which is an interpretive provision for Part VIII relating to “Criminal Damage to Property”. The relevant parts of the new s 59(1) and (1A) were:

“(1) In this Part, **property** means:

...

⁹ Subsections (3) and (4) of the new s 27A are not material for present purposes.

- (b) any program, or data, held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature.

(1A) In this Part, ***to destroy or damage any property*** in relation to a computer includes the misuse of a computer.

In this subsection ***misuse of a computer*** means—

- (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,

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it.

25. The Ordinance also amended s 85 of the Crimes Ordinance (Cap 200) in relation to making false entries in a bank book etc by extending the definition of “books” to include “any disc, card, tape, microchip, soundtrack or other device on or in which information is recorded or stored by mechanical, electronic, optical or other means.” Section 19 of the Theft Ordinance (Cap 210) relating to false accounting was amended by including, in s 19(3), a definition of “record” as including “a record kept by means of a computer”.

26. Section 11 of the Theft Ordinance (Cap 210), relating to burglary was amended by adding a new interpretive provision (s 11(3A)) in the following terms:

“The reference in subsection (2)(c) to doing unlawful damage to anything in a building includes—

- (a) unlawfully causing a computer in the building to function other than as it has been established by or on behalf of its owner to function, notwithstanding that the unlawful action 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) unlawfully altering or erasing any program, or data, held in a computer in the building or in a computer storage medium in the building; and
- (c) unlawfully adding any program or data to the contents of a computer in the building or a computer storage medium in the building.”

27. In a memorandum to the Legislative Council submitted with the Computer Crimes Bill reference was made to a Working Group on Computer Related Crime which was established in 1984 to report to the Attorney-General and did so in March 1988. Its recommendations were considered by the Legal Affairs Policy Group which, as quoted in the memorandum to the Legislative Council, agreed:

- “(a) Although there is little evidence that computer-related crime has become a major problem, appropriate legal sanctions should be put in place given the widespread use of computers in Hong Kong.
- (b) The present law is inadequate in areas where computers have been accessed dishonestly. Most of the preparatory work for a computer-related crime can be performed without committing any existing offence. Such preparatory work, which could include gaining access to a computer with an intent to deceive or to cause loss to another or gain for the wrongdoer should be specifically punishable without the need to prove the ultimate criminal act has been committed. A new offence of [‘dishonest accessing’] should therefore be created to

make it unlawful to gain access to computers with intent to deceive, cause loss to another or gain for the offender.”

The recommendation in that paragraph gave rise to s 161. Other recommendations explain the other amendments made in the Bill.

28. In the Second Reading Speech for the Bill in the Legislative Council, the Secretary for Security said:

“Although there is no evidence at present that computer-related crime is widespread, the Government believes it is necessary to put in place appropriate legal sanctions against computer misuse, which can result in dishonest gain for the wrongdoer or loss to others.”

He went on to say:

“...the Bill will create a new offence of gaining access to a computer with dishonest intent or with intent to commit an offence. This would apply irrespective of whether the access was unauthorized or not, and irrespective of the means of access.”

29. A Subcommittee of the Legislative Council was established to study the Bill. It came up with a number of conclusions. Its work and recommendations were set out in the speech of Mr Steven Poon in the Second Reading Debate. The Committee had actively pursued the question of what constituted “unauthorized access”. Mr Poon said:

“The subcommittee holds the view that unauthorized access to computers should not include accidental access such as dialing [sic] a wrong number or mistyping a key scenario. To address the subcommittee’s concern the Administration has agreed to amend the relevant section by building in an element of intent to the effect that only a person who intentionally obtains access to a programme or data held in a computer *without authority* will be

penalized. The necessary amendment will be moved by the Administration at the Committee stage.”¹⁰

30. The Secretary for Security also referred, in the Second Reading Debate, to the Subcommittee’s conclusions and added:

“There was also discussion in the subcommittee of the intention behind the new offence of access to a computer with criminal or dishonest intent proposed in clause 6 of the Bill. This offence is aimed at penalizing access to a computer for acts preparatory but falling short of the commission of a fraud. Examples would include someone obtaining access to computerized bank records to obtain details of credit balances for later fraudulent use or an employee writing instructions to a computer that will result in due course in the computer making automatic payments to his account. Currently such activity would not amount to an offence. Once the fraud is put into effect this section would no longer be relevant as other provisions of the Theft Ordinance will apply.”

He went on to say that an amendment to be made to clause 6 of the Bill (ie s 161), concerning access to a computer with criminal or dishonest intent, would modify the provision as it appeared in the Bill so that it covered access to obtain data in transit in any part of a computer system with dishonest or criminal intent.¹¹

31. In the Bill submitted to the Legislative Council the proposed interpretive provision in s 161(2) had contained a paragraph (a) which read:

“a person obtains access to a computer if (and only if) he causes a computer to perform any function”.

That paragraph was deleted by amendment moved by the government.

¹⁰ Hong Kong Legislative Council *Debates*, 21 April 1993, 2931 (emphasis added).

¹¹ Hong Kong Legislative Council *Debates*, 21 April 1995, 2934

The Constructional Question

32. There are a number of constructional questions which could arise in this case. One is whether a smartphone or an iPhone is a computer for the purposes of s 161(1)(c)? Another is whether, assuming such a device is a computer, its use to take photographs and transmit them to another involves “access to a computer”? The answers to those questions are not straightforward and do not fall to be determined in this appeal. The ground of importance on which this Court granted leave to appeal was narrowed, in argument, to a constructional question, sufficient, if decided adversely to the appellant, to dispose of the appeal. That question is whether the offence created by s 161(1)(c) of the Crimes Ordinance covers a use by a person of their own computer with the requisite intent?

33. As the particulars of the offences indicate, each of the respondents except for the third respondent, was charged on the basis of their use of a mobile phone. It was not suggested that the phones belonged to anyone other than those respondents. The third respondent was charged in relation to a desktop computer provided by the school. Given the absence of any evidence of a limit on her authority to use it, including use for private purposes, the appellant conceded that for the purposes of this appeal her position was the same as that of the other respondents. That is to say, the school computer could be treated, for the purposes of the law, as though it were her own. We are not concerned with the correctness of that concession and our acceptance of it does not create a precedent for future cases involving the use by a person of a computer allocated to them by their employer. In such cases, questions of private use rights might be raised distinct from authorized use in the course of employment.

The Approach to Construction

34. This Court has stated in numerous judgments the principles which it applies to the task of statutory construction. It looks to the text of the provision to be construed, its context, including the statute of which it is part and its legislative history, and its purpose. As Ma CJ said in *Town Planning Board v Town Planning Appeal Board*:¹²

“The purpose may be clear from the provision itself or it may be necessary to look at the Explanatory Memorandum to the bill introducing the provision or a ministerial or official statement may be utilised for this purpose.”

35. In this case the context includes the amendments to a number of statutes which were made by the Computer Crimes Ordinance 1993. There is little history of s 161 itself, as it was a new creation although the amendment made, in the course of debate in the Legislative Council, to the clause which became s 161 can be seen as part of the legislative history.

36. The Memorandum for Legislative Council, the Second Reading speech of the Secretary, the recommendations of the Legislative Council Subcommittee, and the government’s adoption of those recommendations all go to indicate the purpose of the provision which is discussed below.

The Constructional Choice

37. The term “ambiguity” is often used to indicate that a word or statutory term or provision has more than one possible meaning, but that word itself has more than one meaning. It can refer to “doubt or uncertainty”. It is also

¹² (2017) 20 HKCFAR 196 at [29].

attributed to words with more than one meaning. It sometimes suggests a deficiency in drafting. However, it is not an unusual occurrence that even well drafted statutes offer choices of construction relevant to their application to a particular class of facts. That is the present case in relation to the words with which s 161(1) opens, namely “any person who obtains access to a computer ...”. On one construction, relevant to the present case, a person “obtains access to a computer”, within the meaning of s 161(1) if he or she uses any computer, whether their own or somebody else’s. The alternative construction applies the section only to the use by a person of a computer belonging to somebody else.

38. The ordinary meaning of the words which open s 161 are indicative of “unauthorized” use of a computer as suggested in *Li Man Wai v Secretary for Justice*.¹³ The word “obtain” is relevantly defined in the Sixth Edition of the Shorter Oxford English Dictionary as “come into the possession or enjoyment of; secure or gain as the result of request or effort, acquire, get.”¹⁴ “Obtain” so defined, is not a word which sits easily with the use by a person of their own device. Nor is the word “access” which, used as a noun, ordinarily means “admittance (to the presence or use of) ... [the] action or process of obtaining stored documents, data etc.”¹⁵ As a verb, it includes in its usage “gain access to (spec. data etc held in a computer-based system, or such a system)”.¹⁶ As a matter of language one always “obtains” access to something to which one did not have access before.

39. There is a degree of redundancy in the statutory language to the extent that the verb “obtain” is a synonym for “access” when used as a verb. That overlap, however, merely emphasizes the oddness of applying s 161 to the use by

¹³ (2003) 6 HKCFAR 466.

¹⁴ Shorter Oxford English Dictionary (6th ed, 2007).

¹⁵ Ibid.

¹⁶ Ibid.

a person of their own computer. The section could have been framed with the opening words “[a]ny person who uses a computer ...” on which wording a constructional choice limiting the provision to the use of somebody else’s computer would be unlikely.

40. As noted above, the Bill as presented to the Legislative Council was amended to delete an interpretive provision in the proposed s 161(2)(a) which would have provided:

“A person obtains access to a computer if (and only if) he causes a computer to perform any function.”

This was evidently made on the suggestion of the Legislative Council Subcommittee that it would have a limiting effect as it would not cover communications between computers to obtain or tap data in transit. It may be observed that had that provision remained, there might have been a stronger textual case for a construction extending s 161 to the use of the offender’s own computer. That would have flowed from the generality of the phrase “causes a computer to perform any function”. It would have accorded textually with the reference in the Secretary’s Speech to the section applying “irrespective of whether the access was authorized or not” which was relied upon by the appellant. But that generality is not reflected in the text of the provision as enacted. As a matter of background the Working Group referred to earlier had produced an interim report which recommended the creation of the offence of “dishonest accessing” under the Theft Ordinance (Cap 210) which began with the words:

“Any person who dishonestly accesses a computer, with or without due authority with intent to deceive or with a view to gain for himself or another...”

It does not appear from the available record what became of that draft or the reason that the words “with or without due authority” did not appear in the Bill. Their inclusion might have strengthened the appellant’s argument. Their omission is neutral as the primary point of reference is the text as it was enacted.

41. The statutory context in which s 161 was enacted is suggestive but not determinative of its appropriate construction. For the most part the other provisions enacted by the Computer Crimes Ordinance 1993 appear to define offences by reference to access to or misuse of a computer other than the offender’s own computer. The “hacking” offence created by s 27A of the Telecommunications Ordinance (Cap 106) was directed to a person who “by telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer”¹⁷. Not only is the section clearly directed at a computer other than the offender’s own, but it uses the term “access”. The word “unauthorized” is comprehensively defined in s 27A(2). It does not appear in s 161(1). The appellant pointed to that difference in support of a submission that s 161(1) covered the use of one’s own computer, which could not be described as ‘unauthorized’. The difference does not overcome the inference to be drawn from the use of the words “obtain” and “access” in s 161 and the removal of the definition of “access” during the Second Reading Debate.

42. The purpose of s 161 emerges with reasonable clarity from the Legislative Council Brief. As the law stood prior to the amendment, a computer might be accessed by way of preparation for the commission of a substantive offence where the access of itself would not constitute an offence. The stated

¹⁷ *HKSAR v Chu Tsun Wai* [2019] HKCFA 3 at [8].

purpose of the new section set out as quoted in Legislative Council Memorandum was to create:

“[a] new offence of ‘dishonest accessing’ ... to make it unlawful to gain access to computers with intent to deceive, cause loss to another or gain for the offender.”¹⁸

43. The language of the Memorandum itself, using as it did the term “gaining access”, indicates a purpose directed at conduct by an offender involving access to somebody else’s computer. That limitation is explicable as a matter of policy. The definition of inchoate offences presents challenges particularly in relation to their *mens rea* elements which are necessarily directed to the commission of a future offence. The practical difficulty of establishing a preparatory *mens rea* may be lessened where it is connected to an *actus reus* involving the wrongful use of somebody else’s computer.

44. All in all, text, context and purpose in this case point in the direction of a construction of s 161 that does not extend to the use of the offender’s own computer, unless that use involves getting access to another computer in which case the conduct is also likely to be covered by one of the other offences created or extended by the Computer Crimes Ordinance 1993. It was not suggested that the present case involved any of the respondents using their own devices to access another’s device.

45. The appellant argued for the wider construction of s 161 and did so largely on the ground that such a construction secured a beneficial public policy. The appellant pointed out that technology had moved on considerably since the enactment of the Computer Crimes Ordinance 1993. He gave as examples the

¹⁸ Security Branch, *Legislative Council Brief* (25 March 1992) para 3(b), enclosed in *Memorandum for Legislative Council* (26 March 1992).

use of computers in an age of electronic banking and online sales and purchase to commit fraud. Reference was made to the use of social networking sites to stalk and harass. The internet, it was said, “facilitates new modes of offending at a scale that can hardly be achieved in the offline physical environment.”¹⁹ Examples were given of the application of s 161(1) in the prosecution of cases, involving:

- (i) use of a private email account to forward a company email to another by using the copy and paste method;²⁰
- (ii) use of a mobile phone to take clandestine images in private places;²¹
- (iii) uploading sex videos on to the internet;²²
- (iv) sending an email which contains false information;²³
- (v) use of a computer to make an application on the internet for a credit card for some fraudulent scheme.²⁴

Those forms of offending, it was submitted, could not have been foreseen at the time of the enactment of the Computer Crimes Ordinance 1993. However they all involved misuse of a computer and, according to the appellant, “fall squarely within the language of s 161, which is essentially an offence of dishonesty and was specifically created and added to the [Crimes Ordinance (Cap 200)] under Part XIII of Miscellaneous Offences to proscribe computer misuse.”²⁵ The

¹⁹ Case for the appellant para 44.

²⁰ *HKSAR v Siu Pui Yiu* FAMC 47/2012.

²¹ *HKSAR v Ho Siu-Hei, Jason* [2018] HKCFI 974, unreported.

²² *HKSAR v Wong Ngai Sang* DCCC 200/2017, unreported.

²³ *HKSAR v Yip Kim Po and Five Ors* CACC 353/2010, unreported.

²⁴ *HKSAR v Lai Mei Yuk, Candy* CACC 427/2003, unreported.

²⁵ Case for the appellant para 46.

appellant argued that the application of s 161 in these cases is simply a matter of giving the words their natural meaning and giving effect to the legislative intent.

46. It was further argued that a restrictive interpretation of s 161 would significantly undermine its purpose and efficacy in combating computer-related crime. The appellant offered what was called a real case list of wrongdoing which would fall under a legal lacuna and could be committed with impunity on the narrow construction of s 161(1). The list included hacking, phishing – ie sending false emails to obtain credit card details, distributed denial of service attacks launched from Hong Kong against overseas targets, identity theft and clandestine photographs.

47. There are two short comments to be made about the appellant's submissions. The first submission seeks a construction of s 161 which creates substantive offences beyond the scope of its purpose which was to create preparatory offences. The second submission appears to offer a desirable public policy and urges the Court to adopt a construction that advances that policy. But that is not the function of the Court in statutory construction. The Court seeks to ascertain the purpose of the statute to inform its construction. It does not identify a purpose which it thinks would be beneficial and then construe the statute to fit it.²⁶

Conclusion

48. For the reasons set out above, s 161(1)(c) on its proper construction does not apply to the use by a person of his or her own computer, not involving access to another's computer. For that reason, and in light of the concession made

²⁶ *China Field Ltd v Appeal Tribunal (Buildings) (No 2)* (2009) 12 HKCFAR 342 at [36].

by the appellant in relation to the third respondent, the appeal must be dismissed against all of the respondents.

(Geoffrey Ma)
Chief Justice

(R A V Ribeiro)
Permanent Judge

(Joseph Fok)
Permanent Judge

(Andrew Cheung)
Permanent Judge

(Robert French)
Non-Permanent Judge

Mr David Leung, SC, DPP, Mr Robert Lee, SADPP and Ms Kasmine Hui, SPP,
of the Department of Justice, for the Appellant

Mr David Boyton, instructed by T K Tsui & Co., for the 1st and 4th Respondents

Mr Duncan Percy, instructed by Kenneth W Leung & Co., for the 2nd Respondent

Mr James Tze, instructed by Raymond Luk & Co., for the 3rd Respondent