(For hearing on 26 February 2019 at 10 am before the Court of Final Appeal)

FACC No. 22 of 2018

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	Appellant
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

Case for the Appellant

TABLE OF CONTENTS

A. Overview 1

B. The Proceedings 3

B.1 Facts of the Case 3

B.2 The Magistrate's Findings 4

B.3 The CFI Judgment on Case Stated 5

B.4 Application for a certificate under s32(2) of HKCFAO 8

C. Point of Law of Great and General Importance 8

C.1 Approach to statutory interpretation and construction 8

C.2 Legislative history of the provision 9

C.3 Interpretation of the phrase "obtaining access to a computer" 13

C.3.1 Purposive Approach 14

C.3.2 Comparison with other provisions in the Bill 18

C.3.3 Existing state of law & Technological changes 20

C.3.4 Absurdity 26

C.4 Conclusion 30

D. Substantial and Grave Injustice 31

E. Conclusion 34

("A[3]/p.2§3" = Part A Record, Tab 3, p. 2, para.3)

A. Overview

1. On 2 November 2018, the Appeal Committee granted leave to appeal for the Appellant to appeal on the following point of law: - A[7]/p.133-134

> "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?"

2. Leave is also granted on the substantial and grave injustice basis 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.

3. In summary, the Appellant submits that:

On Point of law

(1) From the legislative history and the purpose of s.161 of the Crimes Ordinance (Cap 200) ("CO"), the *actus reus* of the offence is broad and covers both "Computer-as-target" offences and "Computer-as-tool" offences.

(2) Access to a computer under s.161 is irrespective of whether the access was unauthorized or not, and

irrespective of the means of access. Unauthorized extraction and use of information from a computer is only one mode of committing an offence under s161(1)(c). The *actus reus* of the offence is not so restricted.

(3) The criminalization of wrongdoings or misconducts (which of themselves are not criminal offences) through the use of information and communications technology ("ICT") as a tool is neither illogical nor absurd – s161 only bans one mode of perpetration of such misconducts.

<u>On Substantial and grave injustice</u>

(4) The nature and the circumstances of the intended use, distribution, collection and return of the interview questions and marking scheme must mean that, according to the ordinary standards of the reasonable and honest people, the documents and the information contained therein are confidential in nature – thus disclosure of the contents of the questions must be objectively dishonest.

(5) The WhatsApp messages and the Respondents' cautioned statements prove that the Respondents were indeed dishonest both objectively and subjectively. The learned Judge's confirmation of the magistrate's determination that the Respondents were not objectively dishonest was perverse and a departure from accepted norms.

B. The Proceedings

4. The Respondents were each charged with 1 count of "Obtaining access to a computer with a view to dishonest gain for another", contrary to s.161(1)(c) of the CO.

B.1 Facts of the Case

5. The Respondents were at the material times primary school teachers. R1 to R3 were teachers of the same school ("Primary School"). For the academic year of 2014-2015, there were 290 applications competing for 28 places of primary one class in the Primary School, and candidates had to attend a selection interview. During a briefing session held the day before the interview, R1 to R3 were provided with the interview questions and marking scheme. The questions and the marking scheme were collected and returned to PW1 who was the teacher in charge of the admission selection at the end of the briefing. A[1]/p.4 §13

6. It was not disputed that: A[1]/p.9 §15(4)-(6)

(1) R1 used her mobile phone to take photos of the interview questions and marking scheme during the briefing and she transmitted the photos to a church mate by WhatsApp (Charge 1).

(2) R2 also used her mobile phone to take photos of the interview questions and she sent the photos to R3 during the briefing (Charge 2).

(3) R3, after receipt of the photos of the questions from R2, used the school's computer to type the interview questions into a word document, and she sent it by email to R2 (with the school's computer) and a friend (with her mobile phone) (Charge 3).

(4) R4, a teacher of a different primary school and a former classmate of R2, received the word document from R2. She used her mobile phone to take photos of the questions and transmitted the photos to two friends by WhatsApp (Charge 4).

7. On the day of interview, when PW2 presented the English and Chinese vocabulary cards to Child B, Child B excitedly said that his mother had revised those words with him the night before. PW2 then marked on the assessment form that "*the questions are compromised and the result is not accurate*", and reported the matter to PW1. The interview performance counted for 75% of the marks. A[1]/p.10 §15(7)-(8) A[1]/p.6 §13(8)

8. Relying on the evidence of PW1, the various WhatsApp messages, and the Respondents' cautioned statements, the prosecution submitted at trial that the Respondents knowingly leaked confidential information to persons connected to the candidates and they were dishonest both objectively and subjectively in terms of the *Ghosh* test. A[1]/p.10 §17-26

B.2 The Magistrate's Findings

9. On 25 February 2016, the Respondents were acquitted by Ms Veronica Heung, Permanent Magistrate ("the Magistrate"). The Magistrate had doubts as to A[1]/p.58 §27-30

whether the teachers were reminded of the confidentiality, and found the prosecution had failed to prove beyond reasonable doubt the **objective** limb of the *Ghosh* test against the Respondents.

10. The Magistrate confirmed the decision to acquit the Respondents upon a section 104 review of the acquittal on 2 September 2016. A[1]/p.66 §31-45

B.3 The CFI Judgment on Case Stated

11. The Appellant appealed by way of case stated. The questions of law in the Case Stated for the opinion of the Court of First Instance ("CFI") are:- A[1]/p.80 §46

(1) Did the Magistrate err in finding that R1-R4 might not be aware that the questions distributed at the briefing were the actual questions to be asked at the interview;

(2) Did the Magistrate err in finding that R1-R4 might not be aware that the questions distributed at the briefing were confidential in nature;

(3) Did the Magistrate err in finding that R1-R4 might not have the requisite *mens rea* to dishonest gain for another;

(4) Did the Magistrate err in acquitting each of R1-R4 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* [2003] 6 HKCFAR 466; and

(5) Did the Magistrate err in failing to give proper consideration to the evidence of this case and in taking irrelevant matters into account in maintaining her decision to acquit R1-R4 in the review hearing.

12. The appeal was heard before Deputy High Court Judge C P Pang ("Judge") on 20 March 2018. Subsequent to the hearing, by a letter dated 6 June 2018, the Judge raised his concern on the appropriateness of the charges. By a second letter dated 14 June 2018, the Judge directed the parties to file written submissions on whether the Respondents obtained access to a computer under s.161(1) of the CO.

13. On 6 August 2018, Judgment was handed down ("Judgement") and the Court dismissed the appeal on the grounds that the *actus reus* of the offence was not made out and the findings of the Magistrate were not perverse.

14. In holding that the acts of Respondents were not "obtaining access to a computer" under s.161 of the CO, the Court said:

(1) the obiter statement by the Court of Final Appeal in ***Li Man Wai v SJ*** (2003) 6 HKCFAR 466 at para. 26 sets out the ambit of the offence under s.161(1)(c). The prosecution must prove "*the unauthorized extraction and use of information from a computer*" A[2]/p.101 §68

A[2]/p.97 §53

(2) there is no logic and legal basis in converting improper acts which are not otherwise offences under established legal principles into an offence under s.161 simply because a computer was involved in the commission of such misconducts. This would result in the anomalies inconsistent with the established legal principles in criminal law; and A[2]/p.97 §54

(3) there is a difference between "obtaining access to a computer" ("取用電腦") and "using a computer" ("使用電腦").

15. As to the 5 questions posed, the Judge found that:

(1) the Respondents "*should know the need and importance of keeping school's information and material for school admission selection as confidential*". A[2]/p.103 §77

A[2]/p.103 §78

(2) the overall evidence in the case suggests that, while the Respondents might not know that they were committing a crime, they "*knew that their conducts were improper and they did not want their conducts to be discovered*". Their conducts were "*wholly inappropriate and disgraceful which no doubt deserved to be condemned*". A[2]/p.104 §79

(3) the Magistrate correctly applied the *Ghosh* test for dishonesty and her findings of facts were not plainly wrong or perverse.

B.4 Application for a certificate under s32(2) of HKCFAO

16. On 6 September 2018, the Judge granted the Appellant's application for a certificate under s.32(2) of the Hong Kong Court of Final Appeal Ordinance (Cap 484) that a point of law of great and general importance was involved in the Judgment. A[3]/p.109-111

C. <u>Point of Law of Great and General Importance</u>

C.1 Approach to statutory interpretation and construction

17. In relation to statutory interpretation and construction, the applicable principles are the following:

(1) Statutory interpretation should be purposive, contextual and holistic: ***B v Commissioner of ICAC*** (2010) 13 HKCFAR 1 (at 9D-F). The proper starting point is to look at the relevant words or provisions having regard to their context and purpose.

(2) The context of a statutory provision should be taken in its widest sense and includes the other provisions of the statute and the existing state of the law: ***Cheung Kwun Yin*** (2009) 12 HKCFAR 568 (at 575B-D).

(3) The object of the exercise is to ascertain the objective intention of the legislature as expressed in the language of the statute, rather than the

subjective intention of the lawmaker: ***B v Commissioner of ICAC*** (2010) 13 HKCFAR 1 (at 9F-10B). The court is bound to give effect to the clear meaning of the language and will not depart from that clear meaning and give the language a meaning which the language cannot bear: ***HKSAR v Cheung Kwun Yin*** (at 574 D-F), ***T v Commissioner of Police*** (2014) 17 HKCFAR 593 (§194-198).

(4) The circumstances in which the court can imply words which do not appear on the face of the statute are strictly limited: ***R (Quintavalle) v Health Secretary*** [2003] 2 AC 687 (at 690 A-C).

(5) A statute is taken to be "*always speaking*". The court will construe a statutory provision to take into account changes, in particular technological changes, that have taken place subsequent to the passing of the statute: ***HKSAR v Wong Yuk Man*** (2012) 15 HKCFAR 712, (at 726 §27), ***Royal College of Nursing v Department of Health and Social Security*** [1981] AC 800 (at 822A-B). An updating construction of legislation is generally to be preferred: ***R (on the application of ZYN) v Walsall Metropolitan Borough Council*** [2015] 1 All ER 165 (at 174G-176H).

C.2 Legislative history of the provision

18. s.161 of the CO was introduced in 1992 pursuant to the Computer Crimes Bill 1992 ("Bill"). The Bill

sought to create two new offences[1] and broaden the coverage of existing offences[2] through amending the Telecommunications Ordinance (Cap 106) ("TO"), CO and Theft Ordinance (Cap 210).

19. The Explanatory Memorandum of the Bill states that:-

> "This Bill amends 3 Ordinances in order to make certain forms of computer misuse criminal offences." (underline added)

20. s.27A of the TO and s.161 of the CO were created to target at "access to computer" offences. The proposed s.161 offence is as follows :-

> "**Crimes Ordinance**
>
> **161. 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) -
>
> (a) a person obtains access to a computer if (and only if) he causes a computer to perform any function;

[1] s.27A of the TO and s.161 of the CO.

[2] ss.59, 60, 85 of the CO, ss.11 and 19 of the Theft Ordinance (Cap 210).

(b) "gain" and "loss" are to be construed as extending only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and -

(i) "gain" includes a gain by keeping what one has, as well as a gain by getting what one has not; and

(ii) "loss" includes a loss by not getting what one might get, as well as a loss by parting with what one has.". (underline added)

21. The Bill was introduced to the Legislative Council on 1 April 1992. When the Secretary for Security moved that the Bill be read the second time in the Legislative Council, he 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.
>
> Firstly, the Bill will tackle what is known as 'hacking', by making unauthorized access to a computer by means of telecommunication an offence.
>
> Secondly, 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**." (underline added)

22. A subcommittee was formed in October 1992 to study the Bill. It is important to note the following

discussions in the subcommittee:

(1) The term "*computer*" should be left undefined because "*the speed of new development in computer technology will quickly cause any definition to become outdated*".

(2) s.27A of TO was created to protect the privacy of legitimate computer users and should be regarded as a regulatory offence for which a custodial sentence would be inappropriate. By contrast, s.161 of the CO was a more serious offence and would warrant a custodial sentence.

(3) The offences introduced by the Bill were "*essentially offences of dishonesty or criminal damage*". By fitting computer misuse into existing criminal legislation, the existing case law could be applied.

23. Significantly, at the committee stage, there were proposed amendments to s.161(2) of the CO by deleting the definition of "*obtaining access*" in para.(a) and adding "*not*" after "*extending*" where it first appeared. The amended s.161 (2) thus read:-

> (2) For the purposes of subsection (1) -
> ~~(a) a person obtains access to a computer if (and only if) he causes a computer to perform any function;~~
> ~~(a)~~ "gain" and "loss" 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 -

(i) "gain" includes a gain by keeping what one has, as well as a gain by getting what one has not; and

(ii) "loss" includes a loss by not getting what one might get, as well as a loss by parting with what one has.". (underline added)

24. In moving the said proposed amendments, the Secretary for Security said:-

> "The amendment to clause 6 of the Bill concerning access to a computer with criminal or dishonest intent will modify this provision so that it covers access to obtain data in transit in any part of a computer system, with dishonest or criminal intent." (underline added)

25. In April 1993, the Computer Crimes Ordinance was enacted.

C.3 Interpretation of the phrase "obtaining access to a computer"

26. The Bill had been examined in the light of the Computer Misuse Act 1990 of the United Kingdom. However, s.161 is peculiar to Hong Kong and it has no direct equivalent in other jurisdictions[3].

[3] The "access offences" in the United Kingdom (ss.1 and 2 of the Computer Misuse Act 1990), Australia (s.477.1(1)(a) of the Criminal Code Act 1995 (Cth)) and the United States (Computer Fraud and Abuse Act of 1986 (CFAA)) prohibit "unauthorized" access to computers, while Canada (s.342.1(1) of the Criminal Code (Can)) focuses on unauthorized use of a computer. ss.1 and 2 of the Computer Misuse Act 1990 of the United Kingdom stipulate directly the act of causing a computer to perform any function with intent to secure access to any program or data held in any computer as the offences. s.17 (2)(c) provides that a person "secures access" to any program or data held in a computer if by causing a computer to perform any function he uses it. In New Zealand, "access" is defined under s.248 of the Crimes Act 1961 as "in relation to any

C.3.1 Purposive Approach

27. As can be seen from the above summary of the legislative history, the legislative purpose of the Bill was to remedy "misuse of computer" and "computer-related crimes" given the widespread use of computers in Hong Kong. The Secretary for Security made it clear in his speech on 1 April 1992 that the offence would apply irrespective of whether the access to a computer was unauthorized or not, and irrespective of the means of access, save that it was not designed to tackle copyright related activities which were regulated under another separate legislation.

28. "Computer-related crimes" is a broad descriptive term which emphasizes the role of technology in the commission of crime. To this end, two principal categories can be identified and they are "cyber-dependent" and "cyber-enabled" crimes[4]:

    (1) Cyber-dependent crimes are those that can only be committed using computers, computer networks, or other forms of ICT. Typically, this relates to modes of offending where the technology is the target of the criminal activity, such as hacking, malware and Distributed

---

computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system."

[4] Jonathan Clough, Principles of Cybercrime, (2nd ed, 2015), p.11, see also the Cybercrime Convention which provides for 4 broad categories of cybercrime offences: offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences and offences relating to copyright infringement and related rights.

Denial-of-Service [5] ("DDoS") attacks ("Computer-as-target").

(2) Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. For example, child pornography, stalking, criminal copyright infringement and fraud ("Computer-as-tool").

29. In the light of what s.161 of the CO seeks to remedy, adopting a purposive approach to statutory interpretation, it is submitted that "obtaining access to a computer" under s.161(1)(c) of the CO should be given an appropriate wide meaning so that it could properly cover "Computer-as-target" and "Computer-as-tool" wrongdoings which can result in either dishonest gain or loss.

30. The Shorter Oxford English Dictionary defines "obtain" as "*come into the possession or enjoyment of; secure or gain as the result of request or effort; acquire, get*". "Access" is defined as "*coming into the presence of or into contact with; approach, entrance; admittance (to the presence or use of)*".

31. Webster's Collegiate Dictionary defines "access" as "*permission, liberty, or ability to enter, approach, or pass to and from a place or to approach or communicate with a person or thing; freedom or*

[5] DDoS is a form of denial of service performed by simultaneously sending large numbers of packets to the same host or network from many computers in different locations on the Internet, with the aim of flooding a network connection or other services.

ability to obtain or make use of something".

32. It is submitted that the natural and ordinary meaning of "obtain access to a computer" clearly encompasses situations where a person gains access to a computer remotely through electronic means, as well as via coming into contact with a computer as an object. There is no requirement that the access must be "unauthorized" or confined to "other's computer". The reference to "*a* computer" means that the computer to which access is obtained can be any computer, be it one's own computer or a computer of other person, and there is no need for a second computer to be involved: ***Attorney General's Reference (No.1 of 1991)*** [1993] QB 94 (at 99D-100G).

33. The above notwithstanding, considering the context and purpose of the Bill, the Appellant submits that a mere "touching" or similar way of "mere coming into contact with" a computer should not constitute "obtaining access" under s.161. It requires a person to, for example, cause a computer to perform any function or obtain data in transit in any part of a computer system.

34. While it is accepted that in strict literal terms, "obtaining access to a computer" ("取用電腦") and "using a computer" ("使用電腦") can be accorded different meanings (para.68 of the Judgment), the Appellant submits that the former is clearly broader in scope than the latter. One can "obtain access to" a

computer without "using" it, but "access to a computer" is a prerequisite of "using" a computer because one will invariably cause the computer to perform a function when using it.

35. In this connection, the Chinese text "取用" ("obtaining access to"), which is equally authentic and presumed to have the same meaning as the English text, also carries a connotation of "使用" ("use") given the plain meaning of the word "use".

36. It is submitted that an obvious form of computer misuse is where a person uses a computer as a tool to commit some serious wrongdoing. Therefore, when one causes a smartphone, which has been held to be a "computer" (***Secretary for Justice v Wong Ka Yip Ken*** [2013] 4 HKLRD604, ***R v Woodward*** 2011 ONCA 610, ***US v Kramer*** 631 F 3d 900 (8th Cir.2011)), to perform a function such as taking photographs of confidential information, his act should constitute "obtaining access to a computer" under s.161. This construction is in line with the legislative intent of s.161 which was enacted to remedy and sanction computer misuse and computer-related crimes.

37. Access to information, or data held in a computer is just one of the many purposes one may harbor in obtaining access to a computer. It is submitted that the statement in para.26 by the Court of Final Appeal in *Li Man Wai*, in the context of its specific facts, was simply to highlight that mere

unauthorized extraction and use of information [as constituting only the *actus reus* of the offence on the specific facts of that case] was insufficient, but it must also be proved [for the *mens rea* of the offence] that the act was dishonest. It was not a statement of law to define and restrict the ambit of s.161(1)(c).

38. The restrictive view adopted by the Judge does not accord with the legislative intention properly ascertained. It has the effect of unduly narrowing the scope of "obtaining access to a computer" to only one specific mode of offending, namely by "*unauthorized extraction and use of information*", which is contrary to the clear wording in s.161.

C.3.2 Comparison with other provisions in the Bill

39. It is worth comparing s.161 of the CO with s.27A of the TO[6] as both provisions were introduced by the same Bill targeting at "access offences".

40. s.27A(1) of the TO reads as follows:

> "**27A 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.

[6] The proposed s.27A of the TO was also amended at the committee stage, see Resumption of the Second Reading of the Computer Crimes Bill dated 21 April 1993, Hong Kong Legislative Council, Official Record of Proceedings of 21 April 1993 at 2930-2934, 2949-2952.

(2) For the purposes of subsection (1)—

(a) the intent of the person need not be directed at—

(i) any particular program or data;

(ii) a program or data of a particular kind; or

(iii) a program or data held in a particular computer;

(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." (emphasis added)

41. s.27A(1) of the TO criminalizes "*obtaining unauthorized access*" "*by telecommunication*" to "*any program or data*" "*held in a computer*". In contrast, s.161 contains no such limiting or definitive words which restrict the scope of the *actus reus*. This is an important distinction. The focus of s.161 is an act of obtaining access to a computer with the specific intent under any of the four limbs in subsection (1)(a) to (d), rather than obtaining access to ultimately the program or data in the computer. It echoes the legislative intent that s.27A is to protect the privacy of legitimate computer users, and s.161 is essentially

an offence of dishonesty.

42. It is submitted that the scope of s.161 is wide, and intended to be so, given the context and purpose of the Bill. The general words employed under s.161 were not the result of any oversight or inadvertence of the Draftsman, but a deliberate decision to not limit the scope of s.161. If the intention of the Draftsman or Legislature were to prohibit only "unauthorized extraction and use of information" from a computer, the Draftsman could and should have stated it expressly.

C.3.3 Existing state of law & Technological changes

43. The Computer Crimes Ordinance 1993 is the only piece of legislation in Hong Kong expressly directed at computer-related crimes. Several legislations were amended or made to address other wrongdoings which took advantage of the advancement of Internet technology, such as:

(1) the Copyright Ordinance (Cap 106) – pertaining to illegal copies of Internet material[7];

(2) the Control of Obscene and Indecent Articles Ordinance (Cap 390) – concerning the distribution of pornographic material on the Internet[8];

(3) the Gambling Ordinance (Cap 148) – prohibiting

[7] Offences in relation to making or dealing with infringing articles etc. under s.118 of the Copyright Ordinance (Cap 106).
[8] Offences to publish an obscene, indecent or classified article under ss.21-23 of the Control of Obscene and Indecent Articles Ordinance (Cap 390).

gambling on the Internet other than under the auspices of the Hong Kong Jockey Club[9];

(4) the Prevention of Child Pornography Ordinance (Cap 579) – concerning the dissemination of online and electronic child pornography[10].

44. It is trite that technology has advanced considerably since the enactment of the Bill. A computer provides a new and faster mode to commit old crimes as well as novel means of committing crimes unknown to any criminal justice system in the pre-digital era. A computer can now perform countless tasks. It is much easier to capture images, and the images can be reproduced and distributed easily via internet almost instantly, and they are effectively irretrievable. The convenience of electronic banking and online sale and purchase transactions also provide fertile ground for fraud. Social networking sites may now be used to stalk and harass. The internet facilitates new modes of offending at a scale that can hardly be achieved in the offline physical environment.

45. As a matter of fact, s.161(1)(c) has been invoked in prosecuting cases such as:

(1) Using private email account to forward a company email to another by using the copy and paste method (e.g. *HKSAR v Siu Pui Yiu* FAMC

[9] The definition of "bookmaking" under s.3 includes bookmaking by "online medium".
[10] Offences relating to child pornography under s.3 of the Prevention of Child Pornography Ordinance (Cap 579).

47/2012).

(2) Using a mobile phone to take clandestine images in private places (e.g. *HKSAR and Ho Siu-hei Jason* [2018] HKCFI 974).

(3) Uploading sex videos onto the internet (e.g. *HKSAR v Wong Ngai Sang* DCCC200/2017).

(4) Sending an email which contained false information (e.g. *HKSAR v Yip Kim Po & 5 ors* CACC 353/2010).

(5) Using a computer to make an application on the internet for a credit card for some fraudulent scheme (e.g. *HKSAR v Lai Mei Yuk, Candy* CACC427/2003).

46. At the time when the Bill was introduced in Hong Kong, all such new forms of offending could not have been foreseen. However, all the acts in question involved undoubtedly misuse of computer and they fall squarely within the language of s.161, which is essentially an offence of dishonesty and was specifically created and added to the CO under Part XIII of Miscellaneous Offences to proscribe computer misuse. The application of s.161 in those situations is simply a matter of giving the words their natural meaning and giving effect to the legislative intent.

47. Moreover, s.161 should be a provision that is intended to be "always speaking" – the term "computer" was intentionally left undefined so that

it could withstand the test of time, and the definition of "*obtain access*" was deleted at the committee stage because "*causing a computer to perform any function*" was considered not wide enough. Applying the principle that a legislation is "always speaking" and the mischief that s.161 seeks to remedy, there is no justification to restrict the application of s.161(1)(c) and render it incapable of sanctioning offences of computer misuse and computer related crimes: ***B v Commissioner of ICAC*** (2010) 13 HKCFAR 1 (at 10A-B), ***Bennion on Statutory Interpretation*** (7th ed., 2017) (at 409-424).

48. Although this case is concerned with accessing and using a computer to capture and disseminate confidential information for dishonest gain by other persons, it is worth considering the impact of the Judgment on a range of conducts which may broadly be described as "voyeurism". It is accepted that as an offence, voyeurism involving use of a computer falls within the definition of "cybercrime": ***Principles of Cybercrime*** (2nd ed, 2015), p.27. While digital technology has not created this phenomenon of voyeurism, technology makes it much easier to capture the so-called "up-skirt" and "down-blouse" images, and have them replicated and disseminated rapidly, at minimal cost and to a potential audience of millions, thus making the offending substantially more serious than with the use of a traditional camera or other means.

49. Some jurisdictions have already enacted specific

anti-voyeurism statutes [11] . Each jurisdiction expresses the offence in terms that are sufficiently broad to encompass new technologies. For example, "observing" under the Canadian provision includes by "mechanical or electronic means"[12], while "visual recording" is defined to include a "photographic, film or video recording made by any means"[13].

50. Presently, there is no specific legislation in Hong Kong dealing with an act of voyeurism involving observation or visual recording for a sexual purpose. The usual charges brought for taking under-the-skirt photograph in public places are Disorderly conduct in public places, Loitering and Outraging public decency under the common law. Although there is criticism that these charges are not entirely satisfactory because they are just general offences, it is nonetheless accepted that the acts satisfy the *actus reus* required of these offences[14].

51. s.161 is a computer-specific provision and voyeurism with use of a computer is a culpable cybercrime conduct. It is submitted that applying s.161 to voyeurism offences is simply giving effect to the legislative intent and is within the ordinary meaning of the words in the provision.

52. A restricted interpretation of the ambit of s.161

---

[11] For example, Canada, the United Kingdom and the United States of America.
[12] s162(1) Criminal Code (Can).
[13] s.161(2) Criminal Code (Can).
[14] For example, *HKSAR v Cheng Siu Wing [2003] 4 HKC 471*, *香港特別行政區 訴 陳智文* HCMA 772/2004, *SJ v Yeung Wing Hong* [2013] 3 HKLRD 800.

would significantly undermine and defeat the purpose and efficacy of s.161 in combating computer-related crimes. If the restrictive view of the Judge is adopted, the following wrongdoings (which are just non-exhaustive real case examples) will fall within a legal lacuna and can be committed with impunity:

(1) Hacking without "Extraction and Use of Information" / Hacking Overseas ICT devices

– Cybercriminals use their own devices in Hong Kong to hack into computer system of an overseas company and install malware / commit crimes.

(2) Phishing[15]

– Cybercriminals create websites with appearances and web addresses closely resembling websites of banks or send faked emails to deceive and obtain personal data and credit card details of the victims.

(3) DDoS Attacks Launched from Hong Kong against Overseas Targets

– Cybercriminals launch DDoS attacks from Hong Kong against web servers hosted overseas (even if the web servers are owned by Hong Kong companies).

[15] Disguising as a trustworthy entity in an electronic communication, for example, using faked email addresses to communicate or enclosing a fake hyperlink in the email.

(4) Misuse of Personal / Corporate Information (Identity Theft)

– A criminal syndicate operates in Hong Kong and uses stolen personal data to register stored value facility accounts of overseas companies with a view to money laundering (e.g. misusing Alipay and WeChat Pay in the Mainland).

(5) Clandestine Photos / Videos taken in public[16] or private places

C.3.4 Absurdity

53. It is accepted that the court should endeavor to not adopt a construction that will produce an absurd, irrational or illogical result, since this is unlikely to have been intended by the Legislature.

54. However, if the meaning of a provision is otherwise clear, the existence of anomalies should not displace that clear meaning unless the anomalies amount to an absurdity which the Legislature could not have intended: ***Stock v Frank Jones (Tipton) Ltd*** [1978] 1 WLR 231 (at 238), ***Bennion on Statutory Interpretation*** (7th ed., 2017), pp.359-363, 375-384, ***R (on the application of R (on the application of AA Sudan)) v Secretary of State for the Home Department*** [2017] 1 WLR 145.

[16] Where the available evidence does not satisfy the offences of Outraging public decency, Loitering or Disorderly conduct in a public place.

55. In doubting whether "using a computer" should constitute "obtaining access to a computer" under s.161(1) of the CO, the Court states that it "*fail [s] to see the logic and legal basis in converting improper acts which are not otherwise offences under established legal principles into an offence under section 161 simply because a computer was involved in the commission of such misconducts*", and it considers that "*the scope of section 161(1)(c) based on the use of a computer*" "*is infinitely wide*" and "*would result in the anomalies inconsistent with the established legal principles in criminal law*" (paras. 53 and 67 of the Judgment).

56. It is submitted that the starting point in statutory interpretation should be the language of the statute, and not a retrospective view as to whether a particular act has previously constituted an offence or not. s.161 has prescribed four situations where access to a computer is made a crime: ***HKSAR v Tsun Shui Lun*** [1999] 3 HKLRD 215.

57. There is nothing that defies logic or legally objectionable in sanctioning **one mode** of offending conduct committed in a specific way which is considered condemnable by the Legislature. One may draw an analogy with acts of desecration of the National flag. In the context of exercise of one's right to freedom of speech and freedom of expression (a fundamental human right), the Court of Final Appeal in ***HKSAR v Ng Kung Siu and another*** (1999) 2 HKCFAR 442 held that s.7 of the National Flag and National Emblem Ordinance and s.7 the

Regional Flag and Regional Emblem Ordinance were constitutional as they only prohibit one mode of expression – desecration of either flag. Any other mode of expression is not prohibited.

58. On the same vein, s.161 criminalizes one mode of improper conduct (which does not involve exercise of any fundamental human right) when a computer was involved and accessed by the accused with criminal or dishonest intent.

59. Moreover, one can always point to some anomalies in the legislation. For instance, "gain" under s.8 of the Theft Ordinance (Cap 210) is limited to financial or proprietary benefits whereas "gain" under s.161 of the CO was held to include "*information which the person obtaining access to the computer did not have before the access*". Anomaly would also arise as taking confidential information without authorization from a manual record is not an offence under the law[17], but if the same information is taken from a computer with dishonest intent, it would constitute an offence under s.161(1)(c).

60. It appears there is no valid distinction between information taken from a computer and information taken from a manual record. However, the seemingly different treatment can be justified by the inherent nature peculiar to a computer which is widely available nowadays, and increasingly easy to use. Computers can process and transmit information/

[17] "Information" does not fall within the meaning of "property" under s.5 of the Theft Ordinance, Cap 210.

data/ images at high speed, with no physical boundaries and at negligible costs to potentially millions of recipients. One can take a digital image with a mobile phone and upload it to a website within seconds. This presents novel opportunities for abuse and exploitation, and the consequences are wide-ranging and serious. There is every good reason to sanction wrongdoings which are committed using computer as a tool with criminal or dishonest intent. It is submitted that that was what the Legislature should have intended and the provision (which is always speaking) should be construed accordingly.

61. Applying these principles to the present case, there is nothing illogical or absurd for criminalizing leaking confidential information with a view to dishonest gain by the candidates of the information before the interview with the use of a computer while no crime would have been committed if the Respondents copied the information on a piece of paper instantly or from memory and then handed it over or mailed it. It is the speed, accuracy and the scope of the recipients to whom the information can be leaked through the use of ICT before the interview that makes the difference.

62. Although the conduct element of the offence is broad in its scope, it does not endow the offence an unduly wide application. Obviously, one can envisage frivolous or even ridiculous examples of minimal technical contraventions for every offence. Taking a government pencil home for work and giving it to a child afterwards is technically stealing it under the

Theft Ordinance. However, the fact that the elements of an offence can be satisfied by fairly trivial circumstances does not mean the offence itself is wrongly conceived.

63. For the offences under s.161, what is sought to be proscribed is an access to computer with the relevant intent or purpose as set out in the provision. Using a computer *per se* in an ordinary way would not fall foul of the law and caught by s.161. It would only constitute an offence under s.161 when such access is obtained with criminal or dishonest intent, which is a high threshold in terms of standard of proof by the prosecution in criminal proceedings. If a computer user simply wishes to tell a "white lie" about his age, that would unlikely be regarded as dishonest either in the user's own eyes or by the community standard. It is the mental element that determines the criminality of the conduct and helps avoid over-breath of the offence.

C.4 Conclusion

64. It is submitted that R1, R2 and R4 in using their own smartphones to take photographs of the interview questions or to send them by WhatsApp, and R3 in using the desktop computer of the school to create the Word file and transmitting it to R2 by email, they had caused the respective computers to perform a function, and thereby had obtained access to a computer. The acts of the Respondents fall within the ordinary meaning of the words of s.161(1)(c) and this interpretation gives effect to the legislative intent

with no absurdity resulting.

D. Substantial and Grave Injustice

65. The main issue at trial and appeal (by way of Case Stated) is whether the Respondents were dishonest in terms of the *Ghosh* test. At trial, the Respondents were acquitted because the Magistrate found *inter alia* that the prosecution had failed to prove the objective limb of *Ghosh* test beyond a reasonable doubt. A[1]/p.60§30

66. In relation to the 5 questions in the Case Stated, the Judge stated that the Magistrate had "*correctly applied the Ghosh test for dishonesty*" in holding that the prosecution failed to prove beyond reasonable doubt that the Respondents were dishonest on the objective limb. A[1]/p.104§79

67. For the objective limb under the *Ghosh* test, it must be decided whether what was done in a particular case is regarded as dishonest according to the ordinary standards of reasonable and honest people. The question for the jury is not whether *they* themselves regard the defendant's conduct dishonest but whether they consider most *other* people would. It is ordinary people's standards that must be applied: ***Arlidge and Parry on Fraud*** (5th ed, 2016), paras.2-019-020.

68. In the present case, the Respondents were all teachers by profession. The Primary School did impose the strict requirement that the teachers had

to return the materials after the briefing. It is submitted that even if the Respondents were not reminded of the need of confidentiality, it would be clear to any ordinary and reasonable person that interview questions should not be disclosed beforehand to a candidate, or the purpose of the interview, which was to obtain spontaneous answers to unrehearsed questions, would be ruined: ***HKSAR v Law Hay-Chung & Ors*** CACC 628/1998.

69. More importantly, there was overwhelming evidence to prove the Respondents knew that what they did were dishonest:

(1) R1, who had once worked as a Discipline Mistress, admitted under caution that they had to use the materials given in the briefing to test the candidates in the interview. When R1 sent the photos of interview questions and marking scheme to her church mate, she said categorically that those were "*the questions for tomorrow*", "*the competition is very keen*", "*the performance in the interview really counts*" and "*the better the performance, the higher the marks, the bigger the chance to be admitted*". A[1]/p.19-20 A[1]/p.16-18 A[1]/p.23-24, 27 A[1]/p.26-29

(2) R2 admitted under caution that she knew the file distributed in the briefing contained the interview questions and marking scheme which would be used in the interview. When asked whether an interviewing teacher was required to keep these questions confidential, R2 responded "*of course it was required*". She denied having A[1]/p.32 A[1]/p.35,37-41

sent the questions to any person other than R3 and her family members. However, WhatsApp messages showed that on the day before the interview, R2 told R4 and another friend that she would have the details of the interview after the meeting, and she sent the questions to them later on.

(3) R3 admitted under caution that a friend asked her if she "*had the contents of the questions (to be put in the) interview*". R3 admitted that when R2 took photographs of the interview questions, she was sitting next to her. After she received the images from R2, she typed the questions into a Word file because she did not want the recipients to see "*exactly what that document would look like*" or "*exactly the same thing on this sheet of paper the kid would see by that time*". A[1]/p.45-47 A[1]/p.47-51

(4) The WhatsApp messages showed that R4 repeatedly prompted R2 to give her the "*interview questions*" as soon as they were available. R4 sent a message to her friends that the "*interview questions*" would be available the following day because the "*panel head*" (*R2*) would give the questions to her after the meeting. When R4 sent the interview questions to her friends, she warned them not to disclose the matters to others, not to practise or flip through the questions on the spot, or it would "*cause death*" and "*someone will lose her job*".

70. The Respondents deliberately leaked the interview

questions to confer an unfair advantage to some candidates who had a connection with them. What they did would destroy the fairness and integrity of the admission interview. It is submitted that what the Respondents did was obviously dishonest both objectively and subjectively. To acquit the Respondents on the basis that an ordinary reasonable and honest person would not consider the Respondents' acts dishonest is demonstrably perverse. The Magistrate had clearly misdirected herself and applied a wrong test.

71. The Judge found that the Respondents "*should know the need and importance of keeping school's information and material for school admission selection as confidential*", and "*the overall evidence in the case suggested that while they [the Respondents] might not know that they were committing a crime, D1-4 knew that their conducts were improper and they did not want their conducts to be discovered. In my view, their conduc*ts *were* w*holly inappropriate and disgraceful which no doubt deserved to be condemned*".

72. It is submitted that the Judge has effectively found the acts of the Respondents dishonest, both objectively and subjectively. The finding that the Magistrate had correctly applied the *Ghosh* test is demonstrably perverse.

E. Conclusion

73. The scope of the *actus reus* of the offence under

s.161(1)(c) of the CO covers all types of access to a computer, irrespective of (a) whether the access is authorized or not and (b) whether the access is to one's computer or that of another person. It is not restricted to the unauthorized extraction and use of information from a computer.

74. It is respectfully submitted that the appeal should be allowed on the basis that the acts of the Respondents constituted the *actus reus* of the offence under s.161(1)(c) and their conducts, in light of the evidence of this case, were dishonest both objectively and subjectively.

75. Although the procedural history of this case cannot be attributed to the Respondents, the seriousness of the offending warrants the remittance of the present case to the Magistrate with a direction to convict and the imposition of an appropriate sentence on each of the Respondents, taking into consideration the said procedural history and such other mitigating factors.

All of which is respectfully submitted.

Dated this 11th day of December, 2018.

(David Leung SC)
Director of Public Prosecutions

(Robert Lee)

Senior Assistant Director of Public Prosecutions

(Kasmine Hui)
Senior Public Prosecutor

To: The Registrar of the Court of Final Appeal

And to: 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

Messrs T.K. TSUI & Co., Solicitors for R1 & R4
Room 502, 5/F., HSBC Building Yuen Long,
150-160 Castle Peak Road, Yuen Long,
New Territories, Hong Kong

Messrs Kenneth W. LEUNG & Co., Solicitors for R2
Suite 1601, 16th Floor, Chinachem Tower,
34-37 Connaught Road Central,
Hong Kong

Messrs Raymond Luk & Co, Solicitors for R3
Unit A2, 2/F, Eton Building,
288 Des Voeux Road Central,

Hong Kong

FACC No. 22 of 2018

IN THE COURT OF FINAL APPEAL OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION
FINAL APPEAL NOS. 22 OF 2018 (CRIMINAL)
(On appeal from HCMA No. 466 of 2017)

BETWEEN

SECRETARY FOR JUSTICE	Appellant
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

Case for the Appellant

Filed this day of December, 2018.

Department of Justice
6th Floor, High Block
Queensway Government Offices
66 Queensway
Hong Kong
Tel: 2867 2265
Fax: 3105 1387