LCQ20: Acts relating to clandestine photography

Following is a question by the Dr Hon Elizabeth Quat and a written reply by the Secretary for Security, Mr John Lee, in the Legislative Council today (May 8):

Question:

Last month, the Court of Final Appeal handed down a judgment on an appeal case, ruling that as the acts of the respondents clandestinely taking photographs of interview questions with their own mobile phones and divulging them to other people had not involved access to another person's computer, the respondents had not committed the offence under section 161(1)(c) of the Crimes Ordinance (Cap. 200) (i.e. the offence of obtaining access to a computer with a view to dishonest gain for himself or another person). In this connection, will the Government inform this Council:

(1) as the Government indicated, subsequent to the handling down of the aforesaid judgment, that the Police were discussing with the Department of Justice ways to deal with nine other cases of a similar nature, of the details of those cases and the approach for dealing with them;

(2) as there are comments that following the handing down of the aforesaid judgment, it will be difficult for the Police to invoke any legislation to institute prosecutions against those persons who take photographs clandestinely with their own mobile phones in a private place, of the Government's measures to curb such acts before any legislation is enacted to plug the loophole;

(3) as the Review of Sexual Offences Subcommittee of the Law Reform Commission proposed the creation of a new offence of voyeurism and conducted public consultation on the proposal in May last year, whether the Government will immediately commence the relevant legislative procedure; if so, of the details and the timetable; if not, the reasons for that;

(4) whether it will immediately conduct a study on enacting legislation against acts of clandestine photo-taking of confidential documents or information; if so, of the details and the timetable; if not, the reasons for that; and

(5) given that at present, the non-compliance of a data user with the Data Protection Principles stipulated in the Personal Data (Privacy) Ordinance (Cap. 486) does not directly constitute a criminal offence, and the data user commits a criminal offence only if he or she contravenes an enforcement notice served on him or her by the Privacy Commissioner for Personal Data in connection with such non-compliance, and that the offence only carries a maximum fine of $50,000 and an imprisonment of two years, whether the

Government will amend Cap. 486 to enhance the deterrent effects against acts of privacy intrusion such as clandestine photo-taking; if so, of the details; if not, the reasons for that?

Reply:

President,

Section 161 of the Crimes Ordinance (CO) (Cap. 200) on "access to computer with criminal or dishonest intent" stipulates that 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.

The above provision aims at combating acts of "access to computer with criminal or dishonest intent", such as technology crimes like illegal access to a computer system. The maximum penalty is five-year imprisonment on conviction upon indictment.

On April 4, 2019, the Court of Final Appeal (CFA) held in Secretary for Justice v CHENG Ka Yee & 3 Others [2019] HKCFA 9 that the text, context, and purpose of section 161(1)(c) of CO pointed towards construing the provision so that it does not extend to the use of the offender's own computer. In other words, on its proper construction, section 161(1)(c) of CO does not apply to the use by a person of the person’s own computer, not involving access to another's computer.

The Government respects CFA's ruling. The judgment helps clarify the relevant statutory provisions and legal viewpoints. Having consulted the Constitutional and Mainland Affairs Bureau, the Department of Justice (DoJ) and the Secretariat of the Law Reform Commission (LRC), our reply to the various parts of the question is as follows:

(1) & (2) As at April 30 this year, the Police had eight cases related to the offence of "access to computer with criminal or dishonest intent" under section 161 of CO pending handling. As regards the other case, the charge has already been amended to the offence under the Hospital Authority Bylaws concerning the taking photograph of a patient in a hospital without consent, and legal proceedings are still on-going. The Police will continue to maintain close liaison with DoJ to ensure that the relevant cases are handled appropriately, such as examining whether to proceed with prosecution with the charge of "access to computer with criminal or dishonest intent" in light of the circumstances of individual cases, or considering the feasibility of laying alternative charge(s).

Given that the facts of every case are different, there is no hard-and-fast rule on how to handle the relevant cases. In considering each case, DoJ will make relevant prosecutorial decisions based on the actual facts, evidence, applicable law and the Prosecution Code. Most legislation targeting the real world (such as theft, deception, etc.) also applies to crimes committed through the Internet or by means of technology. Focusing on obtaining access to a computer with criminal or dishonest intent, section 161 of CO remains effective against unlawful acts such as illegal computer intrusion and obtaining access to another's computer for committing other offence(s).

We understand the public's concern about acts such as clandestine upskirt-photography. Depending on the actual circumstances and evidence of the case, the acts may constitute the offence of "loitering" under section 160 of CO (Cap. 200) with a maximum penalty of imprisonment for 2 years; "disorder in public places" under section 17B of the Public Order Ordinance (Cap. 245) with a maximum penalty of a fine at level 2 and imprisonment for 12 months; or "outraging public decency" under the common law with a maximum penalty of imprisonment for seven years.

If the photo-taking activities involve "personal data" as defined in the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486), and the collection or handling of such personal data contravenes the data protection principles as set out in Schedule 1 to PDPO, the Privacy Commissioner for Personal Data (PCPD) may issue an enforcement notice to relevant persons. A person who contravenes an enforcement notice will, on first conviction, be liable to a maximum penalty of a fine at level 5 and imprisonment for two years plus a daily fine.

(3) & (4) With regard to the impacts brought about by CFA's judgment handed down on April 4, 2019 in respect of section 161 of CO, the Security Bureau (SB) is looking into the judgment with relevant departments and proactively examining the legislative amendment on the crime concerned, with a view to introducing the relevant legislative proposal as soon as possible.

In that regard, in respect of the offence of voyeurism, LRC released a report on "Voyeurism and Non-consensual Upskirt-photography" on April 30 recommending the introduction of a new and specific offence of voyeurism to deal with acts of non-consensual observation or visual recording of another person for a sexual purpose; and a new and specific offence in respect of non-consensual upskirt-photography. SB welcomes LRC's recommendations and will carefully study and follow up the report. We suggest discussing with the Panel in July, to be followed by a consultation, with a view to introducing a bill for the Legislative Council's scrutiny as soon as possible.

On the other hand, in light of the rapid development associated with information technology, computer and the Internet, coupled with the potential for them to be exploited for carrying out criminal activities, an LRC sub-committee commenced its study on the topic of cybercrime in January this year. SB will continue to closely monitor the progress of the study.

(5) Given the rapid development in information technology and online communications, technological advancement has brought new challenges to the protection of personal data privacy. The Government is highly concerned about how to improve the regulation on personal data and maintains an open mind on amending and improving the PDPO. Currently, the Constitutional and Mainland Affairs Bureau, jointly with the Office of PCPD, has commenced reviewing the relevant regulations and penalties of PDPO, including studying issues such as the establishment of a mandatory data breach notification mechanism, retention period of personal data and regulation of data processors. Having regard to the findings of the Office of PCPD's investigation on recent personal data breaches and its recommendations, the Government will decide how the PDPO should be improved to enable the Office of PCPD to effectively strengthen the regulation on protection of personal data.