



香港個人資料私隱專員公署  
Office of the Privacy Commissioner for Personal Data, Hong Kong

專員用箋

*From the desk of the Commissioner*

Our Ref. PCO(O)115/156 pt.12

28 March 2006

By Hand

Clerk to the Bills Committee  
Panel on Security  
Legislative Council  
Legislative Council Building  
8 Jackson Road, Central  
Hong Kong

Dear Sir,

**Interception of Communications and Surveillance Bill ("the Bill")**

I refer to the Bill gazetted on 3 March 2006.

In discharge of my function under section 8(d) of the Personal Data (Privacy) Ordinance, Cap 486 to examine any proposed legislation that may affect the privacy of individuals in relation to personal data, I have to-day sent my comments on the Bill to the Permanent Secretary for Security. A copy of my letter is enclosed. For members' information and reference, a copy of my previous letter dated 9 February 2006 responding to the proposed legislative framework when it was first presented by the Security Bureau is also enclosed.

I hope members of the Bills Committee will give due consideration to the comments given.

Yours sincerely,

(Roderick B WOO)  
Privacy Commissioner for Personal Data

Encl. letters to the Secretary of Security dated 9 February and 28 March 2006



香港個人資料私隱專員公署  
Office of the Privacy Commissioner for Personal Data, Hong Kong

Our Ref.: PCO(O)115/156 pt.12

Your Ref.: SBCR 3/2/3231/94

9 February 2006

By Fax & By Post

Mr Stanley Ying, JP  
Permanent Secretary for Security  
Security Bureau  
Government Secretariat  
Lower Albert Road  
Hong Kong

Dear *Stanley*

Interception of Communications and Covert Surveillance  
Proposed Legislative Framework

In respect of the proposed legislative framework to regulate interception of communications and covert surveillance, we have the following comments to make:

Non-government parties

While there are good reasons for the Government to devote the present legislative proposal concerning interception of communications and covert surveillance engaged in or practiced by law enforcement agencies ("the LEAs") in order to allay public concerns, it is equally important that legislative proposals governing these activities which are carried out by private individuals or organisations should not be left in abeyance. Sophisticated technological devices easily available in the market has now made it possible for personal data to be collected without the data subject's knowledge or consent. Legislation specifically regulating these acts and practices will protect the personal data privacy to which Hong Kong residents are entitled under Article 30 of the Basic Law and enhance the limited application of the Personal Data (Privacy) Ordinance, Cap 486 ("the PDPO").

It is agreed that consultation exercise soliciting views from the public and

different sectors is imperative and I expect a concrete time frame for the second phase of the exercise.

#### Authorization

In order to avoid the carrying out of interception of communications and covert surveillance by LEAs indiscriminately, the criteria for determining the application of the following conceptual terms are important and should be spelt out in no uncertain terms so as to prevent abuse. Any grey areas in applying the criteria should be removed as far as practicable:

- (i) Different definitions of "serious crime" is applied to interception of communications (offences punishable with a maximum imprisonment of not less than 7 years) and covert surveillance (offences punishable with a maximum imprisonment of not less than 3 years or a fine of not less than \$1,000,000). What is the rationale for making the distinction?
- (ii) The definition of "public security" needs clear boundary so as not to become a purpose that is subject to easy abuse;
- (iii) How is the test of "proportionality" and hence necessity to be applied and what factors are to be taken into account? The test has to be clearly spelt out in the proposed legislation;
- (iv) In the area of covert surveillance, careful consideration should be given over the selection criteria in determining what is the "more intrusive" and what amounts to the "less intrusive" surveillance. The argument that when surveillance is carried out by a party participating in the communications will make it "less privacy intrusive" does not sound convincing in particular when surveillance device is employed by such party to the communications;
- (v) For surveillance where there is no infringement of the reasonably expected privacy of individuals, no authorization is required. This raises the question as to the yardstick to be applied in determining the perimeters of reasonable expectation of privacy which is a matter to be properly addressed in the proposed legislation.

As for the period of authorization which initially lasts for three months and subject to renewals, intrusion of the intended target as well as innocent third parties' personal data privacy would be aggravated as a result of prolonged surveillance activities being carried out. Hence, criteria for granting any

renewal application should be more stringent than those used to consider the original application.

The repeated or frequent surveillance of the same targeted individual also needs vigilant control and additional safeguards may be imposed by requiring such act to be sanctioned by Court. For renewal applications made to designated authorized officer, one of the safeguards that could be used to lessen the risks of abuse is to limit the granting of only one renewal application and that such application has to be supported by good reasons including reasons to show why if the previous attempt was not fruitful the surveillance should continue. Any further renewal application has to be authorized by the Court.

#### Independent oversight authority and complaints handling

The Commissioner welcomes the setting up of an independent oversight authority to be charged with the duty of regularly monitoring the compliance of the requirements of the proposed ordinance as well as providing a channel for redress to complainants whose privacy right may have been wrongly invaded.

The power to order payment of compensation gives teeth to effective enforcement. The oversight authority should also be equipped with other incidental powers such as the power to summon witnesses, to search and seize, to conduct hearing and to publish reports, etc. in facilitating the exercise of its functions and powers. In addition to the power to order payment of compensation, the oversight authority should also be given power to order cessation of the ongoing surveillance act or practice and the destruction of the information gathered in order to abate the wrongful act.

By virtue of the covert nature of the activities, it would be difficult for a data subject to be aware of the act and to lodge a complaint, especially when no prosecution ensues. No matter how frequent or regular sampling audits are going to be undertaken, it could not substitute the protection afforded the data subjects of their being notified that surveillance activities had been taken place against him. In this respect, it is noted that section 7(5) of the Interception of Communications Ordinance confers powers on Court to notify the person in question that his communications have been intercepted where no charge is laid against the person. The proposed legislation should give due regard to this notification requirement unless otherwise justified.

The oversight authority should also be empowered to oversee the propriety of those surveillance activities which apparently do not require authorization in order to prevent abuse of powers. It is unclear from the present proposal

whether the oversight authority will have such jurisdiction.

The PDPO as it presently stands confers powers upon the Commissioner to handle complaints of acts or practices that contravene the requirements of the PDPO. There may therefore be situations that the powers of the oversight authority now proposed and the Commissioner would overlap, such as in dealing with complaints against the LEAs concerning the conduct of covert surveillance. A clear distinction of the functions and powers of the oversight authority is called for so that the public is not misled as the proper channel through which they can seek assistance or redress.

#### Other privacy safeguards

The security and safekeeping of the personal data collected through interception or covert surveillance should be seriously addressed. All such personal data should be securely kept and locked, to be accessible only on a "need to know" basis by authorized staff so as to prevent unwarranted or accidental access. The staff in charge should possess the requisite integrity, prudence and competence in complying with the requirements of the ordinances, applicable guidelines, practice directions and code of practices that are in force.

The personal data collected should be properly disposed of when the purpose of collection has been fulfilled so that they are not excessively retained. Where authorization is revoked or the original purpose has been fulfilled, the materials collected or generated through interception or covert surveillance should be safely and irreversibly destroyed.

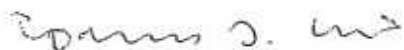
Regular review of the personal data management practice is to be carried out by the respective LEAs to ensure that their act or practice is privacy compliant.

#### Code of practice

It was proposed that a Code of Practice be drawn up by the Secretary for Security in providing guidance to law enforcement officers. For more effective implementation of the Code of Practice, the oversight authority may assume a more proactive role in its drafting stage. It should also recommend amendments to the code whenever it considers appropriate. The proposed legislation may also explicitly provide that a breach of the Code of Practice will give rise to a rebuttable presumption of contravention of the relevant requirements under the proposed legislation in proceedings brought before any court, magistrate or tribunal. A similar provision is found in section 13 of the PDPO.

I hope the above will give food for thoughts from the perspective of personal data privacy protection when the Bill is introduced in LegCO.

Yours sincerely,

A handwritten signature in dark ink, appearing to read "Roderick B. Woo". The signature is fluid and cursive, with a distinct loop at the end.

(Roderick B. WOO)  
Privacy Commissioner for Personal Data





香港個人資料私隱專員公署  
Office of the Privacy Commissioner for Personal Data, Hong Kong

Our Ref. : PCO(O)115/156 pt.12

Your Ref.: SBCR 3/2/3231/94

28 March 2006

By Fax & By Post

Mr Stanley Ying, JP  
Permanent Secretary for Security  
Security Bureau  
Government Secretariat  
Lower Albert Road  
Hong Kong

Dear *Stanley*

**Interception of Communications and Surveillance Bill ("the Bill")**

I refer to the captioned Bill gazetted on 3<sup>rd</sup> instant. Having perused the Bill and in addition to the comments we raised before on the proposed legislative framework, I have the following observations:

**I. Cases of reasonable expectation of privacy**

The definition of "*covert surveillance*" under Clause 2(1) of the Bill has been qualified by reference to cases where the subject is entitled to a **reasonable expectation of privacy**. Apart from the elaboration made in Clause 2(2) that there is no reasonable expectation of privacy in activities carried out in public place, it leaves open the meaning of reasonableness. The determination of what is reasonable apparently rests with goodwill and judgment of the law enforcement agencies ("the LEAs") in carrying out the surveillance activities. Without precision, it may give rise to a potential conflict of interest situation and is susceptible to abuse.

Hence, it is imperative to devise a clear definition or benchmark to determine the reasonable expectation of privacy of the data subject. Reference in this respect can be drawn to the recommendations made by the Law Reform Commission's recently issued report on *Privacy: the Regulation of Covert Surveillance* ("the LRC Report") in taking into account factors such as the place where intrusion occurred, the object and occasion of the intrusion, the means of intrusion employed and the nature of any device used, etc. in determining the reasonable privacy expectation of an individual. It is advisable for the issue to be covered by the Bill itself, and if not, by the Code of Practice to be prepared by the Secretary for Security under Clause 59. As an additional safeguard, the Commissioner on Interception of Communications and Surveillance ("the Commissioner") should also be informed of the cases where the LEAs have carried out

covert surveillance activities without prescribed authorizations so as to enable the Commissioner to assess whether the decision is properly made and to decide whether to exercise his powers under other parts of the Bill.

## II. Type 2 surveillance

I understand that this term as defined under Clause 2(1) is intended to cover those “*less privacy intrusive*” surveillance activities that are carried out by the LEAs. However, given the relatively wide scope of application proposed under (a)(i)(B) and (ii) of its definition to allow for surveillance being carried out by persons other than the participating party insofar as the latter intends or reasonably expects the words or activities to be heard or seen or has given the express or implied consent to monitoring or recording the words or activity in question, it gives rise to privacy concerns as to loopholes for abuse. This is particularly so when the participating party is an undercover agent who no doubt would consent to the surveillance works being carried out by some third parties. The target individual’s words or activities though expected to be heard or seen by the participating party, are rendered more privacy intrusive, for them to be heard or monitored by unexpected third parties.

The same concern arises in the scenario put forward in (b) thereof when the surveillance does not involve entry onto any premises without permission ((b)(i) thereof refers). Examples are found in surveillance devices being installed in adjacent premises with the permission of the neighbour to facilitate the monitoring or recording of words and activities of the target subject(s) that took place next door (for example, by using long lenses, etc.). The fact that the surveillance is undertaken by persons other than the participating party or in premises with permission of owners or occupiers other than the target subjects has rendered the act more privacy intrusive and judicial authorization appears to be better safeguard.

## III. Conditions for issue, renewal or continuance of prescribed authorization

Clause 3(1) spells out the proportionality test to be relied upon by the prescribed authorities. It is however noted that the term “*operational terms*” (Clause 3(1)(b)(i) refers) is used as qualifying benchmark in considering the intrusiveness of the interception or covert surveillance. Since “*operational terms*” is an elusive concept, the balance may be easily tipped in favour of carrying out the interception or covert surveillance.

In applying the proportionality test, due regards should be given to the factors recommended by the LRC Report, such as the gravity of the crime, the place where intrusion will occur, the means of intrusion employed, the nature of any device used, the extent to which privacy of individuals will be affected by the interception or covert surveillance.



#### IV Notification to be given to data subjects

The Bill does not impose a notification requirement to individuals who had been subjects of interception or surveillance especially those cases that no prosecution action ensues. It is also noted that Division 4 of Part 3 empowers the head of department to issue emergency authorization for any interception or Type 1 surveillance when there is an immediate need to resort to such action. Notwithstanding that the emergency authorization is to be confirmed by the panel judge within a period of not longer than 48 hours and the power of the judge to revoke the authorization, wide powers are conferred on the executive arm to give initial approval. From a personal data privacy perspective, the absence of notification given to the data subjects, in particular, in cases where there is no ensuing prosecution or where the authorization was subsequently revoked does not accord sufficient protection to data subject whose privacy rights might have been wrongfully infringed upon without his knowledge. The review and redress channel afforded under Part 4 of the Bill does not have meaningful application if data subject is always kept in the dark and so is deprived of his right to proper legal protection.

Reference is drawn to section 7(5) of the Interception of Communications Ordinance, Cap 532 of the power of the court to require notification to persons affected by the interception. In order to tip a proper balance, it is recommended that similar approach be adopted at least for cases (i) that no prosecution ensues; (ii) where the authorization was revoked under Clause 24(3) of the Bill; and (iii) of non-compliance reported by the LEAs under Clause 52 of the Bill.

Although there is argument against the giving of notification on the ground that it conflicts with the basic principle that the unused or disallowed intercepted or covertly obtained materials be destroyed as soon as possible in order to lessen the risk of unauthorized or accidental access or usage of these materials (Clause 56(1)(c) refers), it should not be construed as a valid excuse for overriding the right of the data subjects to seek for redress. The notification requirement is also in alignment with the right conferred upon an aggrieved person to apply for examination under Clause 42 of the Bill. This is also consistent with the obligation imposed on the LEAs under Clause 57 to keep proper records of the applications and the related materials. The LRC Report has also expressed views on the need to give proper notification in certain circumstances, such as where the warrant or internal authorization have not been properly issued, etc. 24 hours (as opposed to 48 hours as proposed in the Bill) is recommended by the LRC Report to be the maximum period for initial authorization by a law enforcement officer in emergency situation. We share the notion that the shorter period is preferred to lessen the impact on intrusion on personal data privacy.

#### V. Cases of emergency application

Clause 20(1) provides for emergency application when there is an immediate need for interception or Type 1 surveillance. The criteria set out in Clause 20(1)(a) is drafted in vague terms by using words such as “*imminent risk*”, “*substantial damage*”, “*vital*

*evidence*” which are easy subjects of abuse. It is proposed that either they are defined in clearer terms in the Bill or alternatively, that the Code of Practice should give clear and detailed guidance to prevent abuse. Although confirmation of emergency authorizations is provided under Clause 23, damage has already been done for the interception or Type 1 surveillance that was wrongly carried out. There also seems to be insufficient safeguards being in place to prevent deliberate delay on the part of the LEAs to bring upon themselves the occurrence of an urgent situation justifying emergency application. The LEAs should also be obliged to furnish report to the Commissioner covering refusal for applications for confirmation by panel judge for emergency authorizations (Clause 24(5)), for oral application cases (Clause 27) and discontinuance of interception or covert surveillance cases where the conditions for continuance of the prescribed authorization under section 3 are not met (Clause 55).

#### VI. Limitation on number of renewals and approval criteria

The Bill has provided for unlimited number of applications for renewal under both judicial authorization (Clause 12(4) refers) and executive authorization (Clause 18(4) refers). The damages on personal data privacy, especially those owed to innocent third parties will be aggravated as a result of prolonged periods of surveillance or interception of communications being undertaken. It is therefore advisable that a ceiling be set, in particular, to those cases approved under executive authorization, as to the maximum number of renewal applications allowed for or alternatively, that judicial authorization be sought instead on the renewal application as safeguard against abuse of executive powers. In this respect, the LRC Report also adopts similar line of thoughts that application for a second or subsequent renewal of an internal authorization should be made to the Court of First Instance before its expiration, as should any application for renewal of a warrant.

The grounds in support of the renewal application as laid down in Part 4 of Schedule 3 of the Bill do not include the giving of supporting reasons to show why the interception or surveillance activities engaged in that were futile in collecting the intelligence is still justified. Apart from the general consideration under Clause 3(1), the Bill should as far as practicable set out more stringent criteria and factors to be taken into account before the authorizing officer (under Clause 17) and the panel judge (under Clause 11) should grant the renewal application. Such factors include, for example, the proof of the efficiency or utility of such interception or surveillance exercise, etc. In the LRC Report, it is recommended that information such as the particulars of any previous application involving the same person, the reasons why the covert surveillance continues to be considered proportionate to what it seeks to achieve should be put forward on an application for renewal. I support that recommendation.

#### VII. The device retrieval warrant

Where a prescribed authorization ceases to have effect, Clause 32(1) provides that the LEAs **may** apply to a panel judge for issue of a device retrieval warrant authorizing the retrieval of any of the devices authorized to be used under the prescribed authorization.

Given the permissive rather than mandatory duty on the part of the LEAs, it raises privacy concerns in the event that the LEAs fail to apply for removal of the device which may still be left deliberately or inadvertently functioning and thereby collecting personal data. In order to prevent this from happening, it is advisable that the application for device retrieval warrant be made mandatory so that the panel judge can oversee that (i) there is no undue delay on the part of the LEAs in making the application for device retrieval warrant when the period of prescribed authorization expires; and (ii) to ensure that all the surveillance or interception devices are properly removed, preventing unauthorized or prolonged usage of these devices.

According to Clause 34(b), the duration of the device retrieval warrant is not to be longer than the period of 3 months. While valid reasons might exist for the granting of a 3 months' judicial authorization for installing the interception and surveillance devices in order to gather intelligence, we fail to see the same need applies to justify the giving of a 3 months' period for removing the devices. Such prolonged period is likely to give room for abuse and aggravate the damages, if any. A shorter period for retrieval should be considered.

#### VIII. Powers of the Commissioner

Clause 42(2) provides that the application for examination to be made in writing. To assist those who may not be able to put the application in writing, the Commissioner should provide assistance to the applicant in completing the complaint procedures so as not to deter or discourage the making of applications for examination. Reference can be drawn from similar provisions under section 37(4) of the Personal Data (Privacy) Ordinance ("the PDPO") whereby the Privacy Commissioner and his prescribed officers shall provide appropriate assistance to an individual who wishes to make a complaint and requires assistance to formulate the complaint.

It is provided under Clause 43(2)(b) that the Commissioner may order for the payment of compensation. The LRC Report recommends that where appropriate, punitive damages may be awarded. In order to protect the privacy of individuals, the Commissioner should also be vested with the powers to order for immediate cessation of the on-going interception or surveillance activities in order to abate the damages to privacy, if any, that is being incurred. There is also the need to provide the Commissioner with such incidental powers such as the power to summon and examine witnesses (with penal sanction imposed on non-compliance) which are imperative for the efficient discharge of his functions.

Clause 43(1) provides the power of the Commissioner to carry out an examination to determine whether or not the interception or covert surveillance alleged has taken place and if so whether or not a prescribed authorization should have been, but has not been, issued or renewed under the Ordinance in relation to the interception or covert surveillance as alleged. Clause 43(2) goes on to say that if the Commissioner determines that a prescribed authorization should have been, but has not been issued or renewed

under the Ordinance, he shall rule the case in the applicant's favour. Otherwise, he shall rule against the applicant pursuant to Clause 43(3). By using the words "should have been ...issued or renewed", it presupposes that the conditions for carrying out the interception or covert surveillance under Clause 3 are fulfilled but only that no prescribed authorization has been obtained. It is not clear whether the Commissioner has power to examine cases in a situation where interception or covert surveillance was wrongly carried out without fulfilling the conditions under Clause 3 (in which case prescribed authorization, even having been applied for, should not have been issued). Will you clarify the situation or amend the wording under Clause 43 to cover the situation?

With respect to the power of examination under Clause 45, it appears that the restriction on the Commissioner to carry out the examination on the basis of written submission only as laid down in Clause 45(1)(b) is overly restrictive.

Clause 51(1) of the Bill as it presently stands in giving powers to the Commissioner to require public officer to answer any question and provide information, etc. lacks teeth in the absence of corresponding provision of sanction for non-compliance.

In view of the legislative proposal under Clause 59(5) that non-compliance with the Code of Practice issued under Clause 59(1) is not to be regarded as failure to comply with the provisions of the Bill and does not affect the validity of any prescribed authorization or device retrieval warrant, the aggrieved parties are likely to be left without remedies. This absolute exoneration overkills the effectiveness of the Code of Practice and therefore needs careful re-consideration. It is therefore suggested that the Commissioner be vested with powers that notwithstanding the provisions of Clause 59(5), to award damages against the LEAs upon finding of a breach of the Code of Practice when reviewing or examining cases before him. In addition, in all legal proceedings brought against the LEAs, the breach of a Code of Practice should be admitted as a rebuttable presumption for the party seeking to prove the matter to invoke. Reference in this respect is drawn to section 13 of the PDPO.

In relation to the power of reporting and making recommendations by the Commissioner under Clause 41(3) and Clause 50(3), please explain why there is discretion being conferred to reporting also to the Secretary for Justice given that there is no criminal sanction for breach of Bill.

#### IX. Data subject stripped of his data access request right

Clause 45(2) provides that the applicant for examination is not entitled to have access to "*any information, document or other matter compiled by, or made available to, the Commissioner in connection with the examination*". Coupled with the further powers given under Clause 51(3) on general non-disclosure, it is read and interpreted that the applicant as data subject is deprived of his data access right conferred under section 18 of the PDPO. We therefore have reservation on the aptness of Clause 45(2) having the effect of depriving the data subject of his statutory right under the PDPO.

Currently, Part VIII of the PDPO provides for specified circumstances exempting access to personal data. For instance, when the personal data are held for the purpose of prevention or detection of crime (section 58(1)(a)) or the prevention, preclusion or remedying of unlawful or seriously improper conduct or dishonesty or malpractice by persons (section 58(1)(d)), they are exempt from the provisions of data protection principle 6 (i.e. the principle governing access to and correction of personal data) if compliance of the principle would be likely to prejudice the exempted purpose or directly or indirectly identify the person who is the source of the data. Given that Part VIII of the PDPO already provides for exemption to be relied upon and invoked by the data user in appropriate cases, we find Clause 45(2) granting outright denial of access to personal data not necessary and conflicting provisions under different ordinances will cause problem in future.

#### X. Immunity from suit

Clause 61 confers immunity on persons from all civil and criminal liability of any conduct carried out pursuant to a prescribed authorization and performance of function and compliance with requirement under the Bill. The effect of granting this immunity means that the civil remedy on claim for damages under section 66 of the PDPO is virtually taken away. In the absence of strong reasons justifying the abrogation of other civil rights, the provisions of the PDPO shall operate in parallel with other statutes and the civil remedy provided for under section 66 shall continue to apply. Further thoughts should be given on this apparent inconsistency with the rights conferred under section 66.

#### XI. Consequential amendments to the PDPO : section 58A

Consequential amendments were proposed for exempting from the provisions of the PDPO personal data system used for the collection, holding, processing or use of personal data which are, or are to be contained, in protected product or relevant records. Sub-paragraph (2) thereof specifically exempts those personal data that are, or are to be contained, in the protected product or relevant records from the provisions of the PDPO. Attention is drawn to the fact that exemption is only a defence under Part VIII of the PDPO and the Privacy Commissioner is still charged with the duty to carry out an investigation under section 38 when complaints are brought to him to determine if the exemption provision has been properly invoked. Investigation would inevitably entails the examination of the intercepted materials or covertly obtained information.

Thus, if the legislative intent is clear that there should be no overlap of jurisdiction under the Bill and the PDPO and that all data protection principles and other provisions of the PDPO are not to be applicable, the proposed amendment should not be put under Part VIII of the PDPO but should be made an independent provision so that members of the public are made fully aware that those matters do not fall within the purview of the PDPO and that the Commissioner has assumed the oversight role instead. This has the benefit of defining in sufficient clarity the different functions and roles to be played by the relevant

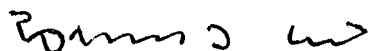
regulatory bodies to avoid any overlap of duties and powers. The present case, as it stands, is still pending the outcome of further deliberations by members of the Bills Committee on the inclusion of this proposed consequential amendment which if implemented, our comments expressed in the preceding sections IX and X of this letter would become academic.

Although the Commissioner may at the end of the day be vested with the exclusive jurisdiction to deal with matters concerning personal data in relation to the Bill, I would nevertheless emphasize the importance of following the fundamental data protection principles laid down in the PDPO by the LEAs and the Commissioner so that the Bill expounds the concept of personal data privacy protection and their proper management.

I urge you to give serious consideration to the above comments.

With kind regards,

Yours sincerely



(Roderick B. WOO)  
Privacy Commissioner for Personal Data

c.c. Department of Justice (Attn.: Mr Ian Wingfield, Law Officer (International Law))

c.c. Clerk to Bills Committee, Panel on Security, Legislative Council