立法會
Legislative Council

LC Paper No. CB(2)580/20-21(03)

Ref : CB2/PL/SE

Panel on Security

Updated background brief prepared by the Legislative Council Secretariat for the meeting on 15 January 2021

Results of Study of Matters Raised in the Annual Report to the Chief Executive by the Commissioner on Interception of Communications and Surveillance

Purpose

This paper summarizes past discussions by the Panel on Security ("the Panel") on the results of study of matters raised in the annual reports to the Chief Executive ("CE") by the Commissioner on Interception of Communications and Surveillance ("the Commissioner").

Background

2. The Interception of Communications and Surveillance Ordinance (Cap. 589) ("ICSO"), which came into force on 9 August 2006, provides a statutory regime to regulate the conduct of interception of communications and covert surveillance by designated law enforcement agencies ("LEAs"). Under section 49 of ICSO, the Commissioner shall, for each report period, submit a report to CE. The report is to be submitted within six months after the expiry of the report period. CE shall cause a copy of the report to be laid on the table of the Legislative Council ("LegCo").

3. In the course of examination of the Interception of Communications and Surveillance Bill in 2006, the Administration undertook, inter alia, to report to the Panel the results of the Administration's study of matters raised in the Commissioner's annual report to CE.

Deliberations of the Panel

4. Since the commencement of ICSO on 9 August 2006, annual reports had been submitted by the Commissioner to CE. The results of the

Administration's study of matters raised in the annual reports have been discussed at a number of Panel meetings and the deliberations are summarized below.

Compliance with the statutory requirements among officers of the law enforcement agencies

5. Some members were concerned that LEA officers were unfamiliar with the rules and procedures of the ICSO regime. Some members were of the view that sufficient training on the requirements in ICSO should be provided to newly appointed as well as existing staff, including those at supervisory level. Concern was also raised as to whether any reviews or assessment had been conducted to ensure that frontline officers were familiar with ICSO requirements.

6. According to the Administration, in response to the recommendations in the reports of the Commissioner, numerous revisions had been made to the Code of Practice ("CoP"). Although relevant officers were not required to undergo assessment on the requirements in ICSO, LEAs concerned considered training to be important, and had provided diversified training to relevant officers, including induction and refresher training, briefings, seminars, workshops, practical training, theoretical and case-sharing sessions, which particularly covered issues on legal professional privilege ("LPP") and journalistic material ("JM"). All officers newly assigned to ICSO work would receive training, while existing officers would also receive refresher training. Notably, LEAs invited the Commissioner to a forum in January 2019 to speak to frontline officers on the requirements under ICSO. The forum was useful and had active participation among officers. The Administration would liaise with the Commissioner as to whether similar forum should be held again, considering in particular whether there were any specific issues arising from the Commissioner's inspections that had not been raised before.

7. To prevent recurrence of technical mistakes and avoid human errors when performing ICSO duties, members were advised that corresponding computer systems in LEAs were enhanced to streamline some manual work processes. Supervisory process had also been strengthened with additional levels of report and assessment.

Prevention of abuse of power by law enforcement officers

8. While noting that interception of communications and covert surveillance was critical to the combating of serious crime, some members expressed concern about the possibility of abuse of power by LEAs.

9. Members were advised that under ICSO, all interception required the prescribed authorization of a panel judge. When making an application for a prescribed authorization, an LEA applicant had to submit with his application an affidavit or written statement on his assessment of the likelihood of involvement of LPP to a panel judge for issue of a prescribed authorization. Whenever there were any subsequent changes which might affect the assessment, LEA concerned had to notify the panel judge, who would determine whether the prescribed authorization should continue and if so, whether any additional conditions needed to be imposed. LEAs were required to submit reports within specified time limits to the Commissioner, who monitored the compliance of LEAs with ICSO. Where there were cases of non-compliance or irregularity, follow-up actions were taken by LEAs in accordance with the established mechanisms having regard to the Commissioner's advice and recommendations. Where disciplinary actions were to be taken against the officers concerned, LEAs concerned would take into account the views of the Commissioner, if any, before actions were taken against the officers concerned.

10. Some members were of the view that more information on cases of non-compliance and irregularities should be disclosed in the Commissioner's annual reports. Members were advised that the Commissioner had highlighted in his annual reports his continued practice of providing the utmost transparency of his work, while taking care not to divulge any information the disclosure of which might prejudice the prevention or detection of crime or the protection of public security.

11. Some members expressed concern about the possibility of LEAs carrying out interception of communications or covert surveillance for political purposes. Members were advised that the Commissioner had stated at his briefing on 5 December 2017 on his Annual Report 2016 that he had not identified any interception of communications or covert surveillance carried out for such purposes. The Commissioner had also stated that applications of such a nature, if any, would not be approved by panel judges.

12. Some members were concerned about the credibility of police officers in performing ICSO duties. The Administration stressed that police operations were conducted strictly adhering to the relevant laws and regulations. Members were further advised that the Commissioner did not find any deliberate disregard of the statutory provisions or CoP, or any ulterior motive or ill will on the part of the officers involved in the Annual Report 2018. The Commissioner also observed that LEAs had adopted a very cautious approach in handling ICSO cases.

<u>Inadequacy of the Interception of Communications and Surveillance Ordinance</u>

13. Having regard to the proliferation of use of social media and instant message applications among members of the public, some members expressed concern about the inadequacy and possible loophole of ICSO. They considered that there was a genuine need to review ICSO as electronic messages/digital contents transmitted via these types of applications were within seconds and difficult, if not impossible, to be intercepted, and those records stored in mobile phones or other similar devices after transmission were beyond the scope of regulation under the existing ICSO.

14. The Administration pointed out that as defined in ICSO, "interception" meant "in relation to any communication, means the carrying out of any intercepting act in respect of that communication; or when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of any communication." It did not explicitly stipulate the means of communication to be regulated, and was sufficiently broad so as not to be circumvented by specific technologies. ICSO also specified the types of information that the Commissioner needed to disclose in the Annual Reports. Such regime and practice were similar to those in many overseas jurisdictions, and considered suitable for the situation in Hong Kong and should continue to operate. As such, it was considered not necessary for a review of or amendments to ICSO.

15. Some members, however, expressed concern about the limitations of ICSO during the performance of enforcement actions given the current technological environment. According to the Administration, the requirements under ICSO were necessary to strike a balance between combating serious crime and privacy protection. It was further pointed out that difficulties in verifying the identity of offenders upon intelligence gathering were in fact a global challenge faced by LEAs worldwide. Nevertheless, it was noteworthy that some 200 persons were arrested in 2018 pursuant to ICSO, and around 4 000 persons were arrested since ICSO came into force. It was believed that ICSO would continue to operate effectively in the coming years.

<u>Compensation for unauthorized interception of communications or covert surveillance</u>

16. Some members pointed out that the Apology Ordinance (Cap. 631), which had just come into operation in 2017, sought to, among other things, promote and encourage the making of apologies in order to prevent the escalation of disputes. These members sought clarification as to whether making of apology for the purpose of the Apology Ordinance was applicable to cases of unauthorized interception of communications or covert surveillance.

17. According to the Administration, ICSO had provided for a person to apply in writing to the Commissioner for an examination, if he suspected that he

was the subject of an interception of communications or covert surveillance operation. If the Commissioner, after an examination, determined that the suspected interception of communications or covert surveillance had been carried out by an LEA without the authority of a prescribed authorization, he would notify the applicant concerned, provided that it would not be prejudicial to the prevention or detection of crime or the protection of public security, and initiate the procedure for awarding payment of compensation to the applicant by the Administration. Members were further advised that according to the Commissioner's Annual Report 2016, 15 applications for examinations had been received in 2016 and the Commissioner had found all 15 cases not in the applicants' favour.

Protection of information subject to legal professional privilege and privacy of members of the public

18. Some members expressed the view that LEA officers should under no circumstances be allowed to listen to any communication between a client and a law firm. LEA officers who listened to such communication should be prosecuted under ICSO.

19. According to the Administration, LPP was protected by the common law and Article 35 of the Basic Law, which guaranteed that "Hong Kong residents shall have the right to confidential legal advice". ICSO did not preclude LEAs from intercepting the communications of a lawyer provided that the interception was carried out pursuant to a prescribed authorization in accordance with the requirements in ICSO. In relation to the protection of LPP in ICSO, section 3 of ICSO required the consideration of all relevant circumstances and the balancing of competing interests, including the protection of privacy and LPP, in the issue, renewal or continuance of a prescribed authorization. Schedule 3 to ICSO also required LEAs to assess the likelihood of obtaining LPP information when making an application for interception. Under ICSO, no prescribed authorization might contain terms that authorize the interception of communications by reference to any telecommunications service used at an office or other relevant premises, or a residence, of a lawyer unless exceptional circumstances existed. Section 62 of ICSO further guaranteed that "Any information that is subject to legal professional privilege is to remain privileged notwithstanding that it has been obtained pursuant to a prescribed authorization". Administrative measures were in place supplementing the statutory safeguards.

Cases involving journalistic material

20. Some members were concerned whether a prescribed authorization would be granted, if an LEA applicant indicated at the time of application that JM would be obtained. Concern was also raised about the possibility of cases

where an application for a prescribed authorization was submitted without informing the panel judge that JM would likely be obtained.

21. According to the Administration, there was no question of an LEA submitting an application for a prescribed authorization without informing the panel judge if JM would likely be obtained. ICSO required an applicant to set out, at the time of applying for a prescribed authorization, the likelihood that any information which might be the contents of any JM would be obtained by carrying out the interception or covert surveillance sought to be authorized. LEAs were required to notify the panel judges of cases where information which might be the contents of any JM had been obtained.

Pressure experienced by frontline law enforcement officers

22. Some members were concerned that frontline LEA officers were under heavy pressure when carrying out covert surveillance operations under ICSO, as any error in procedures or records could result in disciplinary actions. Hence, some frontline LEA officers were reluctant to submit surveillance applications in order to avoid making mistakes. This explained the substantial drop in the number of applications for Type 1 and Type 2 surveillance from 134 and 126 in 2007 to eight and three in 2017 respectively, which represented a drop of about 94% and 97% respectively. These members were concerned that the law enforcement capability of LEAs would be undermined.

23. The Administration advised that applications for conducting Type 1 and Type 2 surveillance under ICSO were made on a need basis having regard to the nature of individual cases, and the grant of a prescribed authorization would expressly be based on the necessity and proportionality principles under ICSO. Statistics on Type 1 and Type 2 surveillance under ICSO thus varied from year to year. For instance, there were only six applications for Type 1 surveillance in 2012. There was no question of LEA officers avoiding the submission of surveillance applications under ICSO in order to avoid regulation under ICSO.

Documentation requirement on cases of non-compliance

24. Noting from a non-compliance case in which three officers involved did not remember the exact date of discovering the mistake, some members raised queries over the absence of any written records of the internal communications among different ranks regarding the case. Information was sought on whether there was any requirement within LEAs on the keeping of records in government departments to facilitate internal monitoring and checking by the Commissioner.

25. According to the Administration, the Government Records Service had formulated records management procedures and guidelines to ensure proper

management of government records. Policy bureaux and government departments, including LEAs, should create and capture adequate but not excessive records to meet operational, policy, legal and financial purposes. While CoP provided a general overview on record management, under the ICSO regime, LEAs were further required to follow the Commissioner's more stringent requirements in reporting on cases of irregularity or non-compliance. All written documents and file records of such cases would need to be preserved for inspection by the Commissioner, in addition to a full investigation report on each of such incidents.

Commissioner's power and authority to listen to interception product

26. The Panel noted the recommendation of the first Commissioner for empowering him and staff designated by him to examine intercept and covert surveillance products. The Commissioner considered that the provision of such power for himself and his designated staff to listen to and inspect intercept and surveillance products would serve as a strong deterrent against malpractice or concealment.

27. Members noted that the Interception of Communications and Surveillance (Amendment) Bill 2015, which proposed, among other things, empowering the Commissioner to require LEAs to provide protected products for his checking, was passed at the Council meeting of 16 June 2016. Some members expressed concern about how such examination would be conducted, whether there were measures to prevent the leakage of information in the process and whether relevant training were provided to the Commissioner's staff designated for carrying out examination of protected products.

28. Members were advised that the examination of protected products was carried out at the premises of LEAs. The Commissioner had drawn up confidentiality requirements, internal guidelines and procedures as well as provided training to relevant staff on the examination of protected products.

Relevant papers

29. A list of relevant papers on the LegCo website is in the **Appendix**.

Council Business Division 2
Legislative Council Secretariat
31 December 2020

Appendix

Relevant papers on
Results of Study of Matters Raised in the Annual Report
to the Chief Executive by the Commissioner
on Interception of Communications and Surveillance

Committee	**Date of meeting**	**Paper**
Panel on Security	6.11.2007 (Item V)	Agenda Minutes
Panel on Security	6.12.2007 (Item I)	Agenda Minutes
Panel on Security	16.2.2009 (Item I)	Agenda Minutes
Panel on Security	3.3.2009 (Item IV)	Agenda Minutes
Panel on Security	7.12.2009 (Item I)	Agenda Minutes
Panel on Security	6.7.2010 (Item III)	Agenda Minutes
Panel on Security	29.11.2010 (Item I)	Agenda Minutes
Panel on Security	5.12.2011 (Item I)	Agenda Minutes
Panel on Security	3.1.2012 (Item VI)	Agenda Minutes
Legislative Council	18.1.2012	Motion on "Annual Report 2010 to the Chief Executive by the Commissioner on Interception of Communications and Surveillance"
Panel on Security	4.12.2012 (Item IV)	Agenda Minutes

Committee	**Date of meeting**	**Paper**
Panel on Security	2.7.2013 (Item III)	Agenda Minutes
Panel on Security	3.12.2013 (Item III)	Agenda Minutes
Panel on Security	2.12.2014 (Item IV)	Agenda Minutes
Panel on Security	1.12.2015 (Item IV)	Agenda Minutes
Panel on Security	6.12.2016 (Item IV)	Agenda Minutes
Panel on Security	5.12.2017 (Item IV)	Agenda Minutes
Panel on Security	4.12.2018 (Item IV)	Agenda Minutes
Panel on Security	7.1.2020 (Item IV)	Agenda Minutes

Council Business Division 2
Legislative Council Secretariat
31 December 2020