

HCAL 122/2014

**IN THE HIGH COURT OF THE
HONG KONG SPECIAL ADMINISTRATIVE REGION
COURT OF FIRST INSTANCE
CONSTITUTIONAL AND ADMINISTRATIVE LAW LIST
NO 122 OF 2014**

BETWEEN

SHAM WING KAN

Applicant

and

COMMISSIONER OF POLICE

Respondent

and

YEUNG CHING YIN

1st Interested Party

CHAN SIN YING

2nd Interested Party

HUNG HIU HAN

3rd Interested Party

CHAN SIU PING

4th Interested Party

Before: Hon Au J in Court

Dates of Hearing: 4 November and 21 December 2015

Dates of Supplemental Written Submissions: 24, 29 December 2015, and
20 May 2016

Date of Judgment: 27 October 2017

J U D G M E N T

A. INTRODUCTION

1. This judicial review raises the important questions of (a) whether under section 50(6) of the Police Force Ordinance (Cap 232) (“PFO”), the police has power to search and examine *without warrant* the digital content of a mobile phone found on the person the police has arrested, and if so, (b) whether that section is so authorizing such a warrantless search is unconstitutional being contrary to the protection of a person’s privacy under Article 14 of the Hong Kong Bill of Rights Ordinance (Cap 383) (“BOR14”) and Article 30 of the Basic Law (“BL30”).

2. The facts giving rise to this judicial review, as the matters developed, are indeed no longer material, but it provides a factual context to highlight the arguments raised under these questions. I will therefore give a brief summary of the background facts as an introduction.

3. The applicant participated in the 1 July 2014 procession. He drove the leading motor vehicle of the procession. He was arrested by police on 4 July 2014 for suspected offence of obstructing a police officer in the execution of his duty by idling the vehicle during the procession. It was alleged that he did not follow the directions and verbal warnings given by the police officers at that time to continue to lead the public procession and hence causing the procession to block the road, and thereby affecting public order. This was said to be contrary to the notice of no objection to organising the public possession issued by the police.

4. On arrest, the applicant was searched by the police, and five mobile phones were seized. The arresting officer briefly inspected each of these mobile phones and took possession of them, saying that he suspected that they were related to the offences for which the applicant was arrested. Later, the police returned two of the five mobile phones to the applicant, and allowed the applicant to choose which two.

5. The police continued to retain the other three mobile phones (“the Subject Mobile Phones”), one of which was a smartphone, and sealed them separately into tamper-proof bags in front of the applicant and his legal advisers. The applicant’s legal advisers later claimed for the applicant legal professional privilege (“LPP”) in respect of the Subject Mobile Phones. After further interviews, the applicant was released on police bail in the evening of 4 July 2014.

6. On 30 September 2014, the applicant applied for leave to apply for judicial review, seeking (a) a declaration that section 50(6) of the PFO (“section 50(6)”) does not authorise police officers to search *without warrant* the contents of mobile phones seized on arrest, or (b) alternatively if such search power is so authorised, a declaration that section 50(6) is unconstitutional (“the unconstitutionality declaration”). The applicant also sought the relief that the Commissioner’s decision (“the Decision”) made on 4 July 2014 to seize the Subject Mobile Phones for the purpose of searching their contents be quashed. The court granted leave on papers on 8 January 2015.

7. However, when it came to the substantive hearing of the judicial review on 4 November 2015, the Commissioner submitted that

the judicial review had become academic and should be dismissed, because the police had already returned the Subject Mobile Phones to the applicant without searching its contents (given the claim of LPP). Moreover, the police had decided not to lay any charges against the applicant.

8. After hearing submissions, the court decided to continue to hear the judicial review. The court agreed that the application concerned with the scope and constitutionality of section 50(6) in relation to the search of the digital contents of seized mobile phones, and similar challenges were likely to arise again in the future. The substantive hearing was then adjourned to 21 December 2015, to enable the Commissioner to file further evidence.

B. THIS JUDICIAL REVIEW

B1. The warrantless search power incident to arrest under section 50(6)

9. Under section 50(1) of the PFO, it shall be lawful for any police officer to apprehend any person who he “reasonably believes” will be charged with or whom he reasonably suspects of being guilty of an offence as defined therein.

10. Section 50(6) further provides that:

“Where any person is apprehended by a police officer it shall be lawful for such officer to search for and take possession of any newspaper, book or other document or any portion or extract therefrom and any other article or chattel which may be found on his person or in or about the place at which he has been apprehended and which the said officer may reasonably

suspect to be of value (whether by itself or together with anything else) to the investigation of any offence that the person has committed or is reasonably suspected of having committed:

Provided that nothing in this subsection shall be construed in diminution of the powers of search conferred by any particular warrant.” (*emphasis added*)

11. Thus, under this provision, it is lawful for a police officer to search *without warrant* “any other article or chattel” found on an arrested person or at or about the place of the arrest and which the officer may “reasonably suspect” to be of value to the investigation of any offence that the person has been committed or is “reasonably suspected” of having committed. Parties are not in dispute that it must be implied in this search power that the police could generally also examine the object so seized of.

B2. The grounds of judicial review

12. In this judicial review, the applicant raises two grounds of challenge:¹

(1) The Constitutional Ground: insofar as if section 50(6) authorizes the police to search *without warrant* the digital content of a mobile phone seized on arrest, it is unconstitutional as it disproportionately infringes the right to privacy protected under BOR14 and BL30.

(2) The Construction Ground: alternatively, on a proper construction, the digital content of a seized mobile phone is

¹ At the hearing, given the change of circumstances, the applicant has rightly decided not to pursue the third judicial review ground set out in the Form 86 that the Decision was in any event illegal as there was no reasonable basis to suspect that the Subject Mobile Phones were of value to the investigation of any offences in connection with the applicant.

not found “on” the apprehended person or “in or about the place at which he has been apprehended”. It therefore does not fall within the scope of section 50(6).

13. I will consider these grounds in turn. First, the Constitutional Ground.

B3. The Constitutional Ground

14. The applicant’s principal arguments made in support of the Constitutional Ground run as follows:

(1) A mobile phone nowadays contains massive and extensive personal information of its owner, which includes information and data of private nature. Such private information is subject to constitutional protection under BOR14 and BL30 against any unlawful or unauthorised interference or invasion.

(2) When considered in the above context of constitutional protection of privacy, on a proper construction, section 50(6) of the PFO cannot be intended objectively to permit police officer a search *of the digital content* of the mobile phone seized under arrest without first having obtained specific and prior authorization by a neutral and impartial person acting judicially (ie, a warrant) when it is feasible or practicable to obtain such authorization.

(3) Thus, the police did not have any power to search *without warrant* the digital contents of the Subject Mobile Phones and the Decision was therefore unlawful. The court should make a declaration to that effect.

(4) However, if section 50(6) does authorize a warrantless search of the digital content of a seized mobile phone other than in circumstances when it is not feasible or practicable to obtain such authorization, it is unconstitutional as it infringes an individual's privacy disproportionately and unlawfully and is thus inconsistent with BOR14 and BL30. The Decision is therefore also unlawful.

15. In support of these contentions, Mr Pun SC (together with Mr Newman Lam) for the applicant rely principally on the minority judgment of the Supreme Court of Canada in *R v Fearon* [2014] 3 SCR 621 and the judgment of the Supreme Court of the United States in *Riley v California* 573 US__ (2014). These two cases concern the constitutionality of the common law right for police to search the content of cell phones seized upon arrest respectively in Canada and the United States.

16. Mr McCoy SC (for the 2nd interested party) and Mr Albert Wong (for the 1st, 3rd and 4th interested parties) in substance support the applicant's submissions.²

17. Mr Mok SC (with Mr Jonathan Chang and Mr Antony Leung) for the Commissioner however submit otherwise. In principle, Mr Mok submits that on a proper construction, section 50(6) plainly authorizes a search, including a search of the content, of a mobile

² It is the applicant's case that mobile phones of the four interested parties (who also participated in the procession on 1 July 2014) had also been seized and retained by the police upon their arrests. However, the circumstances relating to the interested parties and retention of mobile phones are irrelevant for the present purposes. Suffice to say that the Commissioner has not objected to them being so joined in these proceedings. I therefore would not set out their circumstances in this judgment.

phone seized on arrest, and there are sufficient procedural safeguards provided under the Personal Data (Privacy) Ordinance (Cap 486) (“PDPO”) and the relevant internal guidelines of the police governing such a search which make the search so authorised under section 50(6) constitutionally compliant with BL30. These procedural safeguards are (says Mr Mok) consistent with the conditions of the common law right for the police to search the contents of mobile phones seized upon a lawful arrest as laid down by the majority judgment in *Fearon*. The majority decided that the common law warrantless search power with those conditions was constitutionally compliant with section 8 of the Canadian Charter of Rights and Freedoms (“the Canadian Charter”). For the same reasons, the power under section 50(6) insofar as a search of the content of a seized mobile phone on arrest is concerned is therefore also a proportionate one and hence compliant with BOR14.

18. For a proper consideration of these competing arguments, it will be helpful to first examine the principles governing the relevant constitutional provisions relating to the protection of privacy in Hong Kong.

B3.1 The principles relating to the protected right of privacy under BL30 and BOR14

19. BL30 provides as follows:

“The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.” (emphasis added)

20. BOR14 also provides:

“Protection of privacy, family, home, correspondence, honour and reputation

(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.”

21. The protection against unlawful and arbitrary interference of one’s privacy under BOR14, read together with BL30, includes a right to be secure against intrusion of an individual’s rights over his properties such as search and seizure. The right balance between the demands of interests of the society in effective law enforcement and the requirements of the protection of an individual’s fundamental right to privacy is achieved in law through having a balance that meets the proportionality test. See: *R v Yu Yem-kin* (1994) 4 HKPLR 75 at 92, lines 38 - 43, *per* Jerome Chan J; *Democratic Party v Secretary for Justice* [2007] 2 HKLRD 804 at paragraphs 64 and 65, *per* Hartmann J (as he then was); *Leung Kwok Hung v Chief Executive of Hong Kong Special Administrative Region* (unreported, CACV 73 & 87/2006, 10 May 2006, Stuart-Moore VP, Yeung and Tang JJA) at paragraphs 1 and 34, *per* Tang JA (as the learned PJ then was).

22. The protection of privacy against unlawful or arbitrary interference under BOR14 has also recently been examined by our Court of Appeal in *Keen Lloyd v Commissioner of Customs and Excise* [2016] 2 HKLRD 1372 in the context of a search made pursuant to a warrant issued under section 21 of the Import and Export Ordinance (Cap 60).

In this respect, the Court of Appeal after considering a line of authorities (both local and overseas) has emphasized and reiterated that:

(1) A permitted lawful and non-arbitrary interference with one's privacy right must be a justified one which satisfies the proportionality test (paragraphs 51 - 58).

(2) In the context of a search which would interfere with privacy, *prima facie*, prior authorization (such as obtaining a judicial warrant) is a pre-condition for a valid search subject to exception such as infeasibility of obtaining prior authorization under urgent situations, and other justifications which can meet the proportionality test. It must be reminded that the vetting of an application for a warrant by judicial officer provides important safeguards against arbitrary interference with the right of privacy guaranteed under BOR14 (paragraphs 71 - 75).

(3) The proportionality test requires the court to consider if the means used to impair the right is no more than necessary to accomplish the legitimate purpose in question. When assessing proportionality in this context, one of the examinations the court has to see is whether there are adequate and effective safeguards against abuse. The court must examine whether the justification is cogent enough and whether other safeguards are in place to protect a citizen from abuse or excess of executive action in the name of investigation (paragraphs 60 - 70 and 90 - 91).

(4) The test must be applied cautiously so that only a statutory provision authorizing a search which is manifestly disproportionate would be struck down as arbitrary. The

law must also be certain and ascertainable to satisfy the requirements under BOR14 (paragraphs 59 - 62).

B3.2 The search of mobile phones and the decisions in Fearon and Riley

23. The court notes the common ground among the parties that nowadays mobile phone is akin to a personal computer where massive and extensive personal data and information can be stored in and accessed through it. Hence, such contents shall be subject to significant and high privacy constitutional protection. In the premises, any search power for law enforcement purposes which interferes with a person's privacy, in order to be lawful, must satisfy the proportionality test (under BOR14) and be guided by "legal procedures" (under BL30). See the principles laid down in *Keen Lloyd* as summarized at paragraph 22 above.

24. The issue of proportionality concerns where the line should be drawn between individuals' high expectation of privacy in their cell phones and the police's ability of effective law enforcement to combat crime. *Fearon* and *Riley* are two leading authorities respectively in Canada and the United States dealing with this question.³

25. In *Fearon*, the applicant was tried for the offence of robbery with a firearm and related offences. At the trial, the police relied on certain evidence (photos and text messages) obtained by the police through the search of the applicant's mobile phone when he was first

³ Notwithstanding counsel's industry, apparently there are no English authorities on this matter. At the same time, as helpfully pointed out by Mr McCoy in his skeleton submissions, in the UK, powers of arrest, search and seizure were comprehensively codified in the Police and Criminal Evidence Act 1984. At section 20 thereof, it has also provided for "extension of powers of seizures to computerized information".

arrested suspected of committing the robbery. The search was made without a warrant. The applicant argued that the warrantless search was in breach of his constitutionally protected right to privacy under section 8 of the Canadian Charter, and thus the evidence obtained was unlawful and not admissible. The trial judge rejected the challenge and admitted the evidence. He was convicted of the offences. The Court of Appeal dismissed his appeal, which was based on the constitutional challenge of the search and the admission of the evidence. He further appealed to the Supreme Court of Canada.

26. The Supreme Court unanimously recognised that nowadays mobile phones raise significant and important privacy protection concerns as they are akin to personal computer containing extensive personal information and data. See paragraphs 51 - 52, *per* Cromwell J, and 100 - 102, *per* Karakatsanis J.

27. However, by majority (McLachlin CJ, Cromwell, Moldaver and Wagner JJ, judgment delivered by Cromwell J), the appeal was dismissed. The majority were of the view that the common law right for the police to search the content of the mobile phone seized on arrest, which was subject to a number of conditions as revised by the majority in the judgment, was constitutionally compliant.

28. The majority's reasons for finding that the common law right to search was constitutional in gist are as follows.

29. Section 8 of the Canadian Charter provides that "Everyone has the right to be secure against unreasonable search or seizure".

30. Given a mobile phone contains extensive and massive personal and private information and data, the majority recognised that a warrantless search of the contents is *prima facie* “unreasonable” for the purpose of the Canadian Charter unless justified. See paragraphs 51 - 58.

31. At the same time, it has been well established that there is a common law power to search incident to a lawful arrest. See: paragraphs 16 - 26. The protection of privacy through the right to be free of unreasonable searches must therefore be balanced against the demands of effective law enforcement. See: paragraphs 2 - 4.

32. Seeking to strike the balance, the majority have concluded that police officers will not be justified in searching a cell phone or similar device incidental to *every* arrest. Rather, such a search will comply with section 8 of the Canadian Charter (and thus reasonable and lawful) if it satisfies the following four conditions as revised by the majority (“the Conditions”):

- (1) The arrest was lawful.
- (2) The search is truly incidental to the arrest in that the police have a reason based on a valid law enforcement purpose to conduct the search, and that reason is objectively reasonable. The valid law enforcement purposes in this context are:
 - (a) protecting the police, the accused, or the public;
 - (b) preserving evidence; or
 - (c) discovering evidence, including locating additional suspects, in situations in which the investigation will

be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest.

(3) The nature and extent of the search are tailored to the purpose of the search.

(4) The police take detailed notes of what they have examined on the device and how it was searched.

See: paragraphs 58 - 64.

33. Although the police in that case failed to comply with the fourth condition in relation to the search, the majority have found that the prejudice caused to the applicant because of that non-compliance was minimal (given the particular circumstance of that case) and hence the evidence should still be admissible. The appeal was therefore dismissed.

34. The minority (LeBel, Abella and Karakatsanis JJ, with judgment delivered by Karakatsanis J) on the other hand have concluded that the common law right to search without warrant should only be carried out in exigent circumstances to be compliant with section 8. There were no exigent circumstances in that case, and therefore the search was unconstitutional. The evidence therefore should not be admitted.

35. While agreeing that there is a common law power of search incident to an arrest, the minority have emphasized that an individual's right to a private sphere is a "hallmark of" a free and democratic society,

and privacy is essential “to human dignity, to democracy, and to self-determination”. The law, in balancing legitimate state interests (including safety and securing evidence in law enforcement) with privacy interests of individuals, requires generally judicial pre-authorization for a search, and a warrantless search is *prima facie* unreasonable. See: paragraph 103.

36. Given the high importance of the constitutional protection of privacy right, they are of the view that warrantless search incidental to arrest is and should only be limited to “exigent circumstances” (as has been the position under common law), which include circumstances where there is a reasonable basis to suspect a search may prevent (a) the imminent loss or destruction of evidence, or (b) an imminent threat to police or public safety. See: paragraphs 175 - 179.

37. The minority are of the view that the majority’s conclusion in modifying and expanding the common law right to be subjected to the Conditions (instead of only in exigent circumstances) does not provide a sufficient protection of the privacy right (given that mobile phones contain such extensive and important personal data and information), is too uncertain in practice, and places the balancing decision into the hands of the police as to whether the Conditions are satisfied in a given circumstance (which was inappropriate and undesirable). See: paragraphs 170 - 172.

38. I now turn to look at briefly the case of *Riley*.

39. In *Riley*, the Supreme Court of the United States was concerned with the question of whether a warrantless search of the content of a mobile phone seized upon arrest was constitutional under the Fourth Amendment of the US Constitution. Relevantly, the Fourth Amendment provides:

“... the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oaths or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

40. As with section 8 of the Canadian Charter, the touchstone of the Fourth Amendment is about “reasonableness” of a search, and thereunder *prima facie*, a warrantless search is unreasonable.

41. The US Supreme Court comes to the same conclusion as the minority in *Fearon* that a warrantless common law search of the contents of a mobile phone seized on a lawful arrest is only reasonable (and hence constitutional) if it is made for exigent circumstances. See pp 15 - 16.

42. In coming to this conclusion, again, the US Supreme Court emphasizes the great importance in the protection of privacy rights, and the fact that nowadays cell phone contains massive and very private personal information and data, which must be subjected to protection in law in the balancing exercise. The court’s view is that the common law exception of exigent circumstances provides the appropriate balance between the interests of effective law enforcement and the importance of privacy protection. In particular, one must still remember that it is always open to the police to obtain a warrant (if so justified) to search the

content of a seized mobile phone. The US Supreme Court thus says these in conclusion (at pp 25 - 27):

“We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is ‘an important working part of our machinery of government,’ not merely ‘an inconvenience to be somehow “weighed” against the claims of police efficiency.’ *Coolidge v. New Hampshire*, 403 U. S. 443, 481 (1971). Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient. See *McNeely*, 569 U. S., at ____ (slip op., at 11–12); *id.*, at ____ (ROBERTS, C. J., concurring in part and dissenting in part) (slip op., at 8) (describing jurisdiction where ‘police officers can e-mail warrant requests to judges’ iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes’).

Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone. ‘One well-recognized exception applies when “the exigencies of the situation’ make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.”’ *Kentucky v. King*, 563 U. S., at ____ (slip op., at 6) (quoting *Mincey v. Arizona*, 437 U. S. 385, 394 (1978)). Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury. 563 U. S., at _____. In *Chadwick*, for example, the Court held that the exception for searches incident to arrest did not justify a search of the trunk at issue, but noted that ‘if officers have reason to believe that luggage contains some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house without opening the luggage.’ 433 U. S., at 15, n. 9.

In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize—indeed, they stress—that such fact-specific threats may justify a warrantless search of cell phone data. See Reply Brief in No. 13–132, at 8–9; Brief for Respondent in No. 13–212, at 30, 41. The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case. See *McNeely, supra*, at ____ (slip op., at 6).”

B3.3 The search power under section 50(6) in relation to content of a seized mobile phone

43. For the present purposes, the relevant words of section 50(6) are: “Where any person is apprehended by a police officer it shall be lawful for such officer to search for ... any article or chattel which ... the said officer reasonably suspect to be of value ... to the investigation ...”.

44. It is common ground among the parties that the words “article or chattel” on their plain meaning must include a mobile phone.

45. The only question is whether the words “lawful ... to search for ... any [mobile phone]” on a proper construction also empower the police officer to search *without a warrant* the digital content of the mobile phone so seized of, and if so, whether such authorization is constitutional in complying with BOR14 and BL30.

46. In considering these questions, the court will bear in mind the principles and approach laid down in *Keen Lloyd* as summarized above.

47. In my view, on a proper construction, section 50(6) only empowers the police officer to search without warrant the digital content of mobile phone in exigent circumstances, and that is constitutional. I will explain why.

48. It is trite that the court adopts a purposive construction of a statutory provision, which should be construed in its proper context, and insofar as possible, the court should adopt a construction which is constitutionally compliant.⁴

49. The present form of section 50(6) was amended (together with sections 50(1), (2), (3), (7), 51, 54 and 56) in 1992 under the Police Force (Amendment) Bill. As explained in the Legislative Council Brief of the Police Force (Amendment) Bill (SBCR 7/2801/77) dated May 1992 prepared by the Security Branch (“the LegCo Brief”), the purpose of the amendments was to ensure that these provisions would be consistent with Articles 5 and 14 of the BOR which was to come into effect in June 1992. Articles 5 and 14 of the BOR provide respectively that no one shall be subjected to arbitrary arrest or detention and no one shall be subjected to arbitrary or unlawful interference with his privacy. The amendments proposed were said to remove the potential “arbitrariness” that might be argued against the original provisions.

⁴ See: *T v Commissioner of Police* (2014) 17 HKCFAR 593 paragraphs 194 - 196, *per* Fok PJ; *HKSAR v Lam Kwong Wai* (2006) 9 HKCFAR 574 at paragraphs 78 - 79, *per* Mason NPJ. Mr McCoy’s skeleton at paragraph 52.

50. Relevant for the present purposes, the original form of section 50(6) provided that a police officer might search an apprehended person for any article which might reasonably be suspected of “throwing light on the character or the activities of the person or his associate”. It was therefore believed that under the original provision, an arrested person might be searched for reasons that might not be relevant to the circumstances of the arrest, or where there was no basis for suspecting an associate of having committed an offence. The authority was concerned that there was a serious risk that the exercise of this search power would be regarded as an arbitrary interference with privacy and thus in breach of BOR14, in the sense that it went beyond, and was thus disproportionate to, what was necessary to achieve the relevant objective. See paragraph 8 of the LegCo Brief.

51. The amendment of section 50(6) to its present form⁵ was intended to address the above concern and risk about arbitrariness. It is pertinent to note that the authority was of the view the amendment would satisfy the proportionality requirement in conducting a warrantless search by bringing it in line with *the common law principles*. This was made clear at paragraph 13 of the LegCo Brief as follows:

“s.50(6) – power to search arrested person

13 We propose that the power of search and seizure in this subsection (*where no warrant is required*) in respect of arrested persons should be restricted to things that the police officer reasonably suspects to be of value in the investigation of any offence which the arrested person has committed or is suspected of having committed. *This formulation is derived from common law principles.” (emphasis added)*

⁵ Which provides that the search should be related to what the police officer “may reasonably suspect to be of value (whether by itself or together with anything else) to the investigation of any offence that the person has committed or is reasonably suspected of having committed.”

52. The court notes that the amendment was made to address the question of “arbitrariness” related to conducting a warrantless search without linking it to the crime the arrested person is suspected of having committed. However, from the above, it is also clear that it was objectively intended by both the authority and the legislature that section 50(6) in its present form is to be BOR14 compliant by bringing it in line with the corresponding common law principles governing warrantless search.

53. In the premises, on a proper construction with the above objective legislative intention, the warrantless search power provided under section 50(6) is intended to be one which would correspond with the relevant common law principles and meet the proportionality requirement in its interference with a person’s privacy right.

54. In relation to this, I agree with Mr Pun that the minority’s view on the common law power of search in *Fearon* is to be preferred in providing the right balance between the protection of privacy right and the interests of effective law enforcement in meeting the proportionality test in Hong Kong context.

55. In my view, given the high importance in protecting the massive and extensive personal information and data, and to give meaningful effect to the constitutionally protected right to privacy and freedom of private communication against unlawful intrusion, it is only proportionate to achieve the objective of effective law enforcement by permitting *warrantless* search for the digital content of mobile phones seized on arrest only in exigent circumstances. The said approach and

analysis of the minority judgment in *Fearon* is more in line and consistent with the approach to proportionality in the context of a search power as laid down in *Keen Lloyd*.⁶

56. As explained in the minority judgment in *Fearon* at paragraphs 140 - 150, only the three purposes underlying exigent circumstances (that is, the protection of the safety of the public and the police officers which is subject imminent threat, the preservation of evidence which could be destroyed imminently, and the discovery of evidence in extremely urgent and vulnerable situation) fairly and rightly justify the intrusion of privacy without prior authorization. This is so because other than in exigent circumstances, there are effective and efficient alternative avenues to address these concerns without any urgent need to carry out an immediate warrantless search of the phone for its digital content, thereby infringing the arrested person's protected privacy. As observed by Karakatsanis J, in relation to:

- (1) Safety: "Clearly a cell phone (or any other digital communication device) is not a physically dangerous weapon and, unlike a physical receptacle like a briefcase, cannot conceal such a weapon" (paragraph 140). "The mere possibility that a phone could have been used to summon backup does not justify a search incident to arrest any more than the theoretical possibility that the suspect's home could contain accomplices justifies a search of the

⁶ The Court of Appeal in *Keen Lloyd* at paragraphs 63 - 68 notes that the wordings of section 8 of the Canadian Charter concerns with the reasonableness of a search or seizure, which are different from BOR14, and cautions against a direct transplant of the reasoning in those cases to the Hong Kong context. However, it has still found the approach in those cases to be "enlightening in the application of [HK's] proportionality test". See also paragraphs 69 - 70 where the Court of Appeal similarly adopts the approach in authorities of the European Court of Human Rights concerning article 8 of the European Convention for considering whether a statutory power of search is consistent with BOR14's protection of privacy right.

home. This does not rise to the level of imminent risk to safety.” (paragraph 141, footnote omitted)

(2) Preservation of Evidence: “Usually the information on the cell phone will remain available pending the acquisition of a search warrant. ... The mere possibility that evidence on the cell phone could be remotely deleted should not justify a search. Furthermore, even if the suspect has an accomplice with the technological skills to wipe the cell phone remotely, this threat is easily addressed by removing the cell phone’s battery or placing it in a ‘Faraday bag’, an inexpensive receptacle which blocks wireless communications.” (paragraph 144)

(3) Discovery of evidence: “There is a cost to requiring police officers to obtain a warrant before searching an arrestee’s phone. Searches for the purposes of imminent risks to safety or the preservation of evidence are permitted under exigent circumstances, answering the most serious of these concerns. However, the requirement to obtain a warrant will sometimes mean that the police are unable to discover potentially valuable evidence or that their investigation will be delayed. This cost must be weighed against the privacy interest in a phone.” (paragraph 150) See also the quotes from *Riley* at paragraph 42 above.

57. On the other hand, the more relaxed restrictions embodied in the Conditions as laid down in the majority judgment do not in my view strike the right and proportionate balance, as it cannot demonstrate why (save in exigent circumstances) it is necessary to urgently carry out the search even for law enforcement purposes *without waiting for a warrant*.

This is particularly so as the police have efficient and effective access to obtain a search warrant from a magistrate, and there are efficient ways to protect evidence in the seized mobile phone pending a warrant, such as putting them in an evidence bag (such as what was done to the Subject Mobile Phones in the present case) and, for example (as mentioned in *Fearon and Riley*), in a simple Faraday bag which would effectively prevent the means to delete the mobile phone contents remotely.⁷

58. I am therefore *not* satisfied that it is proportionate for the purposes of law enforcement to conduct a warrantless search of the digital content of a seized mobile phone in *non-exigent* circumstances.

59. Moreover, I also agree with Karakatsanis J's analysis as to why the Conditions laid down by Cromwell J would result in greater impracticability, police uncertainty and increased after-the-fact litigation. The learned judge explained these at paragraphs 169, 171 - 172:

"[169] ... If a police officer searches a cell phone, mistakenly believing that she has reasonable grounds, the exclusion of the evidence obtained at a subsequent trial does not render the search harmless. The arrested person's privacy will have been unjustifiably infringed, and their general sense of freedom and security affected, even if any information thereby obtained cannot be used against her. Only a requirement of pre-authorization can give people confidence that their privacy will be respected. As La Forest J. wrote in *Dyment*, at p. 430:

... if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. ... Dickson J. made this clear in *Hunter v. Southam Inc.* After repeating that the purpose of s.8 of the *Charter* was to protect individuals against unjustified state intrusion, he continued at p. 160:

⁷ See also Force Procedures Manual ("FPM") 21 - 51 at paragraphs 61 - 63, which provide detailed guidelines to police officers as to how to effectively isolate mobile phone from network to avoid its data being tampered with or deleted remotely.

That purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be accomplished by a system of prior authorization, not one of subsequent validation. [Emphasis in original.]

...

[171] In my view, Cromwell J.'s proposed tailoring of the search's scope encounters the same problems of **impracticality, police uncertainty, and increased after-the-fact litigation** as the cursory search discussed above⁸. My colleague draws a parallel between his approach and the approach set out by this Court in *Vu*, but *Vu* provides that a *judge* may determine the scope of a search of a computer when issuing the warrant (para. 62). And while detailed note-taking of what the police have searched and why may be desirable (*Vu*, para. 70, in the context of a search under warrant), it may prove to be an impractical requirement in the context of a time-sensitive investigation. It is not, in my view, an adequate remedy to what would be 'an extraordinary search power' (para. 82).

[172] Fundamentally, my colleague's approach **puts the balancing decision in the hands of the police**. I doubt not that police officers faced with this decision would act in good faith, **but I do not think that they are in the best position to determine 'with great circumspection' whether the law enforcement objectives clearly outweigh the potentially significant intrusion on privacy in the search of a personal cell phone or computer** (para. 80). **If they are wrong, the subsequent exclusion of the evidence will not remedy the initial privacy violation.**" (emphasis added; emphasis original)

⁸ See also paragraphs 162 - 165 in *Fearon* at pp 689 - 690, which are in essence that: (i) 'Given that the information that can be accessed through a cell phone is highly private, it would be unprincipled to countenance a cursory infringement of the owner's privacy — much as it is not permissible to take a cursory walk inside a suspect's home' (paragraph 163); (ii) 'it is very difficult — if not impossible — to perform a meaningfully constrained targeted or cursory inspection of a cell phone or other personal digital device. ... In short, a cursory inspection for recent communications will need to search a host of applications — the privacy infringement may be far from minimal and the inspection far from quick. Similarly, a cursory inspection of photos may involve any number of private and personal photographs of the individual — and of third parties.' (paragraph 164); and (iii) 'the difficulty inherent in setting a standard for a cursory search would generate uncertainty for the police and result in increased after-the-fact litigation of searches. That same uncertainty would also result in increased numbers of searches that were later determined to be unconstitutional.' (paragraph 165)

60. The problems of “impracticality, police uncertainty, and increased after-the-fact litigation” are indeed illustrated in Cromwell J’s own reasons in *Fearon* as pointed out by Mr Pun. For example:

(1) On the first requirement that “the scope of the search must be tailored to the purpose for which it may lawfully be conducted”, in practice, “this will mean that, generally, even when a cell phone search is permitted because it is truly incidental to the arrest, only recently sent or drafted emails, texts, photos and the call log may be examined as in most cases only those sorts of items will have the necessary link to the purposes for which prompt examination of the device is permitted. *But these are not rules, and other searches may in some circumstances be justified.* The test is whether the nature and extent of the search are tailored to the purpose for which the search may lawfully be conducted. To paraphrase *Caslake*, the police must be able to explain, within the permitted purposes, what they searched and why ...”. (paragraph 76, *emphasis added*)

(2) Another requirement is that the “discovery of evidence, in the context of a cell phone search incident to arrest, will only be a valid law enforcement objective when the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest.” “This will mean, in practice, that cell phone searches are not routinely permitted simply for the purpose of discovering additional evidence. The search power must be used with great circumspection. It also means, in practice, that the police will have to be prepared to explain why it was not practical (and I emphasize that this does *not* mean impossible), in all the circumstances of the investigation, to

postpone the search until they could obtain a warrant.”
(paragraph 80)

(3) Moreover, whether a cell phone search is justified further depends on the types of crimes in a wide variety of circumstances. (paragraph 79⁹)

(4) Even assuming that the police will act in good faith in conducting the search of cell phones seized upon arrest, such approach will inevitable create much uncertainty for the police and increase the possibility of after-the-fact litigation as to whether the search was properly done.

61. Cromwell J’s approach therefore leaves much uncertainty as to how to determine in the future whether a search of cell phones may or may not be lawful.

62. I can do no better than to adopt Karakatsanis J’s observation at paragraph 105 of *Fearon* as to why the majority’s approach by adopting the Conditions does not provide adequate protection of privacy against a warrantless search:

“[105] The intensely personal and uniquely pervasive sphere of privacy in our personal computers requires protection that is clear, practical and effective. An overly complicated template, such as the one proposed by the majority [ie, the Conditions], does not ensure sufficient protection. Only judicial pre-authorization can provide the effective and impartial balancing of the state’s law enforcement objectives with

⁹ Where it was held that: ‘The law enforcement objectives served by searches incident to arrest will generally be most compelling in the course of the investigation of crimes that involve, for example, violence or threats of violence, or that in some other way put public safety at risk, such as the robbery in this case, or serious property offences that involve readily disposable property, or drug trafficking. Generally speaking, these types of crimes are most likely to justify some limited search of a cell phone incident to arrest, given the law enforcement objectives. Conversely, a search of a cell phone incident to arrest will generally not be justified in relation to minor offences.’

privacy interests in our personal computers. Thus, I conclude that the police must obtain a warrant before they can search an arrested person's phone or other personal digital communications device. Our common law already provides flexibility where there are exigent circumstances – when the safety of officer or the public is at stake, or when a search is necessary to prevent the destruction of evidence.”

63. In other words, adopting the exception of exigent circumstances for warrantless search in law provides a clearer, more certain and practicable guidance on the circumstances as to when the police are empowered and entitled to search the digital content of a seized mobile phone upon arrest under section 50(6). This greater clarity, certainty and practicality further defines and thus justifies a proportionate, and hence permitted, intrusion into privacy without prior authorization under BOR14. This is also consistent with the observations in *Keen Lloyd* where our Court of Appeal emphasizes that a statutory power of search must also be certain and ascertainable to make it BOR14 compliant. See paragraph 22(4) above.

64. In the premises, on a proper purposive construction of section 50(6), insofar as to the digital content of a mobile phone seized upon arrest is concerned, a police officer is authorized to search it *without warrant only* in exigent circumstances.¹⁰ The exigent circumstances are

¹⁰ In this respect, Mr Pun has submitted that the legislature could not have in mind at the time of amending section 50(6) in 1992 the privacy concerns relating to mobile phone contents (in particular the massive scale and extent of private information and data that could nowadays be stored in or accessed through the phone). In the premises, he therefore contends that section 50(6) cannot be construed to apply to mobile phone contents. I do not agree. It is usual for the court in construing statutes, in particular those which concern with matters of the ever evolving areas of technology, to apply the statute is always speaking principle to cater for new circumstances which were not within the minds of the legislature at the time of enactment, so long as that would not be contrary to the statute's express words or clear objectives. See: this court's judgment in *Hong Kong Mobile Television Network Ltd v Office of the Communication Authority* [2016] 2 HKC 44 at paragraphs 57 - 60 and the authorities cited therein. See also: *Halsbury's Law of England*, Vol 96 (2012), 5th ed, paragraph 1175. For the reasons I have explained at paragraphs 49 - 53 above, I do not find this interpretation

where, when a person has been lawfully arrested under section 50, the police officer “may reasonably suspect” (as the standard now laid down by the provision) such an urgent search may (a) prevent an imminent threat to safety of the public or police officers, (b) prevent imminent loss or destruction of evidence, and (c) lead to the discovery of evidence in extremely urgent and vulnerable situation.

65. The court notes Mr McCoy’s submissions that, other than meeting the proportionality test, the warrantless search power provided under section 50(6) must also comply with the protection under BL30, which emphasizes the requirement of compliance of “legal procedures” for any invasion or interference of private communication even for law enforcement purposes.¹¹ Leading counsel contends that section 50(6) does *not* expressly provide *any procedures* to regulate a warrantless search for mobile phone private information and data. Any power so given must still be unconstitutional. Mr McCoy hence submits that any search for the digital information in or through a seized mobile phone can *only* be lawfully performed under a specific warrant.¹²

66. With respect, I am unable to agree. The exigent circumstances requirement for the exercise of the power of a warrantless search in relation to mobile phone digital content is part of the common law prerequisite, this would therefore satisfy BL30’s requirement that the infringement on privacy of communication is done in accordance with

in relation to mobile phone contents is contrary to the express words or the clear intention of section 50(6) as identified above.

¹¹ See: *Koo Sze Yiu v Chief Executive of HKSAR* (2006) 9 HKCFAR 441 at paragraph 3, *per* Bokhary PJ (as the learned NPJ then was); *Leung Kwok Hung v Chief Executive of HKSAR* (HCAL 107/2005, 9 February 2006) at paragraphs 120 - 127 and 182 - 184, *per* Hartmann J.

¹² These submissions are shared and relied on by Mr Albert Wong and Mr Pun.

“legal procedures” and to “meet the needs of public security or of investigation into criminal offences”. The relevant “legal procedure” is the guidance laid down in common law on what constitute exigent circumstances and that the police officer must “reasonably suspect” (as provided in section 50(6)) that such exigent situations do arise in the circumstances of the case as explained above.

67. Mr Mok on the other hand seeks to contend that the court should adopt the majority judgment in *Fearon* for the purpose of construing the *warrantless* search power under section 50(6). He submits that such statutory power of search in relation to mobile phone digital content is also constitutionally compliant as the Conditions provide a fair balance between effective law enforcement and protection of privacy as explained by the majority, and meet the “in accordance with legal procedure” requirement under BL30. He also says the 4th condition as a matter of procedure, albeit not expressed in the statutory provision, is in practice governed by Data Protection Principles of the PDPO, the Police General Orders (“PGO”) 44-05(6)¹³ and the FPM 21 - 51, paragraphs 33, 36 and 64.

68. With respect, I am also not convinced by Mr Mok’s submissions.

69. First, for the reasons I have explained above, the Conditions do not meet the proportionality test in providing a proportionate balance

¹³ Which states “Having conducted any form of search, an officer will make a notebook entry as required by PGO53-01. The notebook entry will contain the particulars of the subject, the time, date and location of the search, the scope of the search, the reason for conducting the search, details of the witnessing/guarding officer and, where appropriate, details of the authorizing officer.”

between effective law enforcement and protection of privacy right. On this basis alone, the court should not adopt the majority judgment's approach.

70. Second, I agree with Mr Pun that the PDPO, PGO and FPM do not assist Mr Mok.

71. The reliance on PDPO is misplaced because:

- (1) First of all, search of private information stored in a mobile phone by a police officer *without collecting* the information infringes the owner's privacy but is not governed by the PDPO, so that the PDPO has no application to whether the police may exercise its purported power under section 50(6) to "search" the personal data in the mobile phone without a warrant.
- (2) Further and in any event, plenty of the private information stored in a mobile phone may *not* be regarded as "personal data" within the meaning of section 2 of the PDPO because it does not satisfy the three *conjunctive* requirements of attribution, identification and retrievability under section 2 of the PDPO: see Mark Berthold and Professor Raymond Wacks, *Hong Kong Data Privacy Law* (2nd ed) at paragraphs 7.1 - 7.46.
- (3) Therefore, private information stored in a mobile phone such as photos, video recordings, films and emails (which can be of a highly private nature) may not be "personal data" within the meaning of the PDPO and hence not protected by Data Protection Principles.

72. The reliance on PGO 44-05(6) is similarly misplaced as that is concerned with the search of “persons”¹⁴ but not searches of mobile phones.

73. Finally, the FPM are internal guidelines not accessible or known to the public, which therefore do not satisfy the “prescribed by law” requirement.

74. In response, Mr Mok submits that the Commissioner would undertake to publish the FPM if the court regards that as necessary. However, this *readiness* to publish the guidelines *later* if so required cannot assist the submissions as to whether, *as a matter of proper construction*, the warrantless search power provided under section 50(6) in relation to the digital content of mobile phones satisfy the requirements of BL30.

75. In any event FPM 21 - 51 properly read as a whole is in substance concerned with how to properly *preserve* the digital evidence stored in a seized mobile phone as evidence, but not prescribing procedures that would take into account and safeguard the privacy right of the person that the phone belongs to against abuse. It therefore would not render the warrantless search power (if for circumstances other than exigent ones) proportionate. See: *Keen Lloyd*, paragraphs 62 and 69 (as summarized at paragraph 22(3) above).

76. In the premises, I reject Mr Mok’s submissions that section 50(6) provides a power for the police officer to conduct

¹⁴ PGO 44-05 is entitled “Search of Persons”.

warrantless search of the digital content of a seized mobile phone which is in line with the Conditions, and which is complaint with BOR14 and BL30.

B3.4 Conclusion on the Constitutional Ground

77. For all the above reasons, on a proper construction, I conclude that section 50(6) only authorises a police officer to search *without warrant* the digital contents of mobile phones seized on arrest only in exigent circumstances. Section 50(6) insofar as it so authorizes a warrantless search of the *digital contents* of mobile phones seized on arrest only in exigent circumstances is BOR14 and BL30 compliant and thus constitutional.

78. In relation to this, I would like to add two further observations.

79. First, I have referred to above that the protection against warrantless search save in exigent circumstances is in relation to the “digital” contents of mobile phones seized on arrest, as it is that information that attracts a heightened expectation of privacy. This however does not extend to cover the physical devices themselves. Hence, warrantless searches that treat a mobile phone merely as a physical object continue to be permissible incident to arrest under section 50(6) (as in common law). As said by Karakatsanis J in *Fearon* at paragraph 155, for example, seizing a cell phone, searching for hidden compartments, testing that cell phone for fingerprints, or reading the

identification number physically inscribed on it, do not interfere with the heightened expectation of privacy in the accessible information.

80. Second, for the same reason that it is the digital information that is subject to the heightened privacy protection, and it is the nature of the information accessible through that device that is relevant, the form of the digital devices is immaterial. The protection against warrantless search save in exigent circumstances incident to an arrest under section 50(6) covers also other similar devices such as tablets, smart watches, and laptop computers. See also *Fearon*, paragraphs 156 and 161.

B4. The Construction Ground

81. Mr Pun reiterates at the hearing that the Construction Ground is only an alternative argument raised by him.

82. The arguments run as follows:

- (1) Section 50(6) only authorizes a search of “article or chattel” found “on the [arrested] person” or “at or about the place” of the arrest.
- (2) However, the “place” where the digital information may be accessed in or through the mobile phone is neither a place “on the person” of an apprehended person nor “the place at which he has been apprehended”. The digital information should be regarded as having stored in a “separate place”, which is wholly separate from the arrestee’s person or the place of arrest, *once the mobile phones are taken away from the person or the place of arrest*. Hence, on a proper

construction, the digital content of a mobile phone is not found “on the person” or “at or about the place” of the arrest and is therefore not covered by section 50(6).

83. I am unable to accept these submissions.¹⁵

84. On the plain words of section 50(6), it is clear that the words “may be found on his person or in or about the place at which he has been apprehended” refer to where the seized object (may it be newspaper, book or other document, or any other article or chattel) is located, but not to qualify where the actual inspection of the object that must be conducted.

85. As submitted by Mr Mok, it would be absurd to suggest that section 50(6) also requires that the inspection of the seized object must be carried out “on the person”. Further, it is equally absurd to suggest that the provision requires the inspection of the contents of the seized object also takes place in or about the place where the person has been apprehended. For example, if the police have seized a wallet found on a person arrested in the street and inspect the contents therein at the police station subsequently, such contents would no longer be on the arrested person, or in or about the place at which he has been apprehended. This would not invalidate the seizure of the wallet in the first place. Once the object is validly and lawfully found and seized on the person or at or about the place where the person has been apprehended as required under section 50(6), the court can see no good objective legislative intent to further require the contents and information contained therein to be only inspected also on the person or at or about the place.

¹⁵ The “place” arguments are also shared by Mr McCoy and Mr Albert Wong.

86. Mr Pun relies on the observation of Cromwell J in *R v Vu* [2013] RCS 657 at paragraph 51 to support his argument that the information accessed through a mobile phone should be treated as a separate place. Cromwell J said this at paragraph 51:

“[51] As I explained above, if computers give rise to particular privacy interests that distinguish them from other receptacles typically found in a place, then s. 8 requires those interests to be taken into account *before* the search takes place, not just after-the-fact, in order to ensure that the state’s interest in conducting the search justifies the intrusion into individual privacy. ***In effect, the privacy interests at stake when computers are searched require that those devices be treated, to a certain extent, as a separate place.***” (*emphasis added*)

87. With respect, this does not assist Mr Pun.

88. In *Vu*, the court was concerned with the issue of whether a search warrant, without specifying the search of computer found at the place identified in the warrant, could be impliedly inferred to include the searching of the computer found there. It was in this particular context where search warrant had been issued that Cromwell J made the observation that, for privacy concern and interests, the computer as a device containing massive personal data and information could “to a certain extent” be treated as a separate place and thus not covered by the specific search warrant. The court concluded that no such necessary inference could be drawn.

89. The issue therefore concerns with the construction of the scope of the specific warrant in question, and it is in that context that Cromwell J made the above observation, by emphasizing that “to a

certain extent” the information stored in the computer can be treated as a separate place.

90. This cannot be regarded as an authority to support a general proposition that all the information contained in a mobile phone (comparable to a computer) should be treated as contained at a separate place from the mobile phone itself. Without more, it provides no support to the contentions that, for the purposes of section 50(6), the digital information of a mobile phone seized at the place of arrest should be treated as at a separate place.

91. Further, it also cannot be said it must be the case that all the digital information one can access through a mobile phone is not stored in it. Of course, one can understand that there could be information say saved in a remote server that could be accessed through the phone. But there could also be some information that can be regarded as having been saved and stored in the phone’s memory chip itself. In other words, as observed by Karakatsanis J in *Fearon* at paragraphs 127 - 131, the phone itself could store and keep the private information, *and* also act as a “portal” to information and data saved and stored in a remote server:

“[127] However, a cell phone cannot be treated like any other piece of physical evidence that may be found on an arrestee and searched incident to arrest. The analogy to a ‘briefcase’ is not apt. in *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at paras. 38 and 47, this Court recognized that a computer or cell phone is fundamentally unlike a conventional ‘receptacl[e]’. the four reasons Cromwell J. identified in that case are equally applicable here.

[128] First, computers and cell phones store immense amounts of information, some of which will be highly private in nature (*Vu*, at para. 41). In the case of a cell phone, this will include private communications in the form of texts and

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V

emails, potentially dating back years. ***The data storage capacity of a phone*** can vastly exceed what an individual could carry on their person or in a briefcase: thousands of pictures, messages, or videos. When combined in sufficient quantities, even individually mundane pieces of information have the potential to reveal aspects of our most private lives.

[129] Second, computers and cell phones are ‘fastidious record keeper[s]’ (Vu, at para. 42). These digital devices can generate records of websites visited, documents read and created, and the details of the uses of almost all programs on the device. Cell phones in particular ***retain records of messages, both drafted and sent, calls made, and files transmitted and received***. The ability of a cell phone to generate an exhaustive record of seemingly trivial aspects of a person’s day-to-day life means that it contains a far more thorough picture of what that person thought, said and did than any conventional form of data storage ever could. Because cell phones record details about so many aspects of our lives that would otherwise disappear, any intrusion into the device compromises our privacy interest in an unprecedented way. Our cell phones, on a daily basis, perform a level of surveillance which can generate and allow access to information ranging from social media communications to personal habits, and from tracked news feeds to medication schedules.

[130] As well, digital devices can retain files and data even after users think they have been destroyed (Vu, at para. 43). This problem may be even more pronounced with respect to cell phones, on which detailed manipulation of background files can be even more challenging for the average user.

[131] Finally, the limitation inherent in searches incident to arrest – limiting a search to a particular place or item – is not a meaningful restriction, since modern digital devices ***are portals to vast stores of information that is not ‘in’ the device, but is instead stored on servers, or on third party devices*** (Vu, at para. 44). For example, if a user logs in to an Internet browser on both her home computer and on her cell phone, the browser on the cell phone may contain not just a fastidious record of Internet usage on the cell phone, but also on the home computer. Similarly, social media applications may allow the holder of the cell phone to review messages and information generated by the user on other devices. Emails which have never been sent or read from the cell phone may be accessible through email applications (potentially including those sent many years ago). Files which have never been opened or created on the cell phone may be accessible through

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V

applications that allow the user to store files remotely. Moreover, someone examining the device may not be able to identify what is stored remotely.” (*emphasis added*)

92. Thus, without any cogent evidence to support it, it is not correct for Mr Pun to say *as a general proposition* that all data and information which can be viewed via the cell phones is stored in a place other than the phone itself.¹⁶

93. In the premises, I also reject the Construction Ground.

C. CONCLUSION

94. For the above reasons:

- (1) On a proper construction, in relation to the *digital content* of a mobile phone (or a similar device) seized on arrest, section 50(6) authorizes police officers to search it *without warrant only* in exigent circumstances. I will make a declaration to that effect.
- (2) In authorizing a warrantless search of the digital content of mobile phones seized on arrest only in exigent circumstances, section 50(6) is constitutional and compliant with BOR14 and BL30. I therefore will refuse to grant the unconstitutionality declaration sought.

¹⁶ Mr McCoy separately submits that the digital information cannot be regarded as “documents” for the purpose of section 50(6) at the time of arrest as “the digital information inside the mobile phone is not yet in the form of a document”. Hence, leading counsel continues, while a police officer can “search for” that record, it is impossible, in the circumstances of exercising the power under section 50(6), to “take possession” of that record. With respect, given that the court is satisfied that the police could take possession of an “article or chattel” (which includes a cell phone) under section 50(6) and search the digital information of the phone as an article or chattel (albeit only in exigent circumstances), this contention is neither here nor there.

95. Given that the Subject Mobile Phones have already been returned to the applicant without any search of their contents, it does not serve any useful purpose to quash the Decision. I therefore would not make any order to that extent.

96. The applicant is partially successful in the application. Considering the substance of all the arguments raised, I think it is fair and just to award two-thirds of the costs to the applicant, to be taxed if not agreed with certificate for two counsel. Given that the interested parties' submissions generally and materially overlap with the applicant's submissions, I do not think it is justified and fair in the present circumstances to order two sets of costs against the Commissioner. I would therefore make no order as to costs as between the interested parties and the Commissioner. The applicant and the 2nd interested party's own costs shall also be taxed in accordance with legal aid regulations. These costs orders are on a *nisi* basis, and shall become absolute 14 days from today unless any of the parties applies by summons to vary it.

97. I thank counsel's helpful assistance in the matter.

(Thomas Au)
Judge of the Court of First Instance
High Court

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V

Mr Hectar Pun SC and Mr Newman Lam, instructed by JCC Cheung & Co,
assigned by Director of Legal Aid, for the applicant

Mr Johnny Mok SC, Mr Jonathan Chang and Mr Antony Leung (public
prosecutor, only appearing on 21 December 2015), instructed by
Department of Justice, for the respondent

Mr Gerard McCoy SC, instructed by Ho Tse Wai, Philip Li & Partners,
assigned by Director of Legal Aid, for the 2nd interested party

Mr Albert NB Wong, instructed by Ho Tse Wai, Philip Li & Partners, for
the 1st, 3rd and 4th interested parties

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V