CACV 270/2017

[2020] HKCA 186

IN THE HIGH COURT OF THE

HONG KONG SPECIAL ADMINISTRATIVE REGION

COURT OF APPEAL

CIVIL APPEAL NO 270 OF 2017

(ON APPEAL FROM HCAL 122/2014)

BETWEEN

SHAM WING KAN (岑永根)	Applicant
and	
COMMISSIONER OF POLICE	Respondent
and	
YEUNG CHING YIN (楊政賢)	1st Interested Party
CHAN SIN YING (陳倩瑩)	2nd Interested Party
HUNG HIU HAN (洪曉嫻)	3rd Interested Party
CHAN SIU PING (陳小萍)	4th Interested Party

Before: Hon Poon CJHC, Hon Lam and Macrae VPP in Court

Dates of Hearing: 25, 26 and 27 June 2019

Date of Judgment: 2 April 2020

J U D G M E N T

The Court:

1. This is an appeal from the judgment of Au J[1] ("the Judge") dated 27 October 2017 whereby he held that section 50(6) of the Police Force Ordinance[2] ("Section 50(6)") authorizes police officers to search the digital contents of a mobile phone or a similar device seized from an arrestee without warrant in exigent circumstances only; and that in so authorizing the warrantless search, Section 50(6) is constitutional and compliant with article 14 of the Hong Kong Bill of Rights[3] ("BOR 14") and article 30 of the Basic Law ("BL 30").

A. Background facts

2. The Civil Human Rights Front has been organizing an annual march on 1 July on Hong Kong Island for many years. The applicant and the 4 interested parties took part in the one held on 1 July 2014 ("the March"). On 4 July 2014, they were all arrested for alleged offences committed in connection with the March. Their mobile phones were seized upon arrest, which led to the proceedings below.

3. The Judge only briefly summarized the facts in connection with the applicant and regarded the facts concerning the interested parties irrelevant for the purpose of the proceedings before him. Apparently, that was because by the time when the Judge heard the application substantively, all the seized mobile phones had already been returned to the applicant and the interested parties without inspection. However, for the purpose of this

---

[1] As Au JA then was.

[2] Cap 232.

[3] Section 8, Hong Kong Bill of Rights Ordinance, Cap 383.

appeal, we consider it necessary to set out the facts giving rise to the proceedings below in greater detail[4]. The reasons will become apparent shortly.

A1. Circumstances leading to the arrest

4. On 13 June 2014, the police issued a letter of no objection to the responsible person of the Civil Human Rights Front under sections 11(2) and 15(2) of the Public Order Ordinance[5] for holding the March ("the Letter of No Objection"). Various conditions were imposed, including the time to start (3 pm) and the time to finish (8 pm); and the route designated for the March. In particular, condition (c) stipulated that in light of safety concerns, the police would only allow the March to take place along the westbound carriageways of the route, eastbound and westbound of Des Voeux Road Central and also eastbound and westbound of the tramways as defined. The eastbound carriageways of Causeway Road, Yee Wo Street, Hennessy Road and Queensway were explicitly reserved for emergency vehicles and other road users.

5. On 1 July 2014, the applicant was responsible for driving the head vehicle LM8399 ("the Vehicle") leading the March. The 2nd interested party was one of the three chief marshals responsible for monitoring the whole line of the procession. She was also responsible for

---

[4] The facts are gathered from the Form 86, the affidavits filed by the applicant, the 2nd interested party and the respondent below. The 1st, 3rd and 4th interested parties did not file any affidavit below.

[5] Cap 245.

leading the head of the procession and had remained at that position throughout the March.

6. At about 2:33 pm, the applicant drove the Vehicle arriving at Moreton Terrace for police inspection. At about 3:26 pm, the March commenced when the participants started leaving Victoria Park. It was already 26 minutes behind the commencement time stipulated in the Letter of No Objection. A large banner was held by the marshals at the head of the procession. In front of the banner the marshals held a black belt stretching across the carriageway.

7. The head of the procession later joined the Vehicle at Moreton Terrace near Hong Kong Central Library. According to the police, the Vehicle was then driven at a speed of about 5 km per hour. The applicant and the 4 interested parties were closely coordinating with the marshals who were holding the black belt. When the applicant and the 4 interested parties stopped, the black belt carriers also stopped.

8. As it happened, the March progressed quite slowly. At about 4:43 pm, at the junction of Hennessy Road and Tin Lok Lane, the police gave a verbal advice to the 2nd interested party for being slow in leading the procession forward. She replied that there was a big crowd and the procession was moving on.

9. When the head of the procession reached Fenwick Street, it was about 5:10 pm[6]. The 4 interested parties kept discussing with the marshals

[6] By comparison, according to the police's records, for the march on 1 July 2013, which was also led by the vehicle driven by the applicant, it started at Victoria Park at about 2:40 pm and took 64 minutes to reach Justice Drive.

in the vicinity. The Vehicle stopped at the third lane of Hennessy Road westbound just past the junction with Fenwick Street outside Chinese Methodist Church. The applicant left the driver's seat of the Vehicle while the engine was still running. The marshals carrying the black belt stopped. The large banner was laid on the ground. The procession came to a standstill.

10. At about 5:12 pm, the applicant returned to the driver's seat of the Vehicle. The 4 interested parties were broadcasting slogans and messages through microphones and a public announcement system on the Vehicle to demand the police to open up all six carriageways of Hennessy Road for the March. The 2nd interested party said that they made the request because her fellow marshals further down the line of the procession informed her that the crowd had become very congested. The police advised the 2nd interested party that it was not a time to consider opening up the carriageways. She replied that if the police did not open up the carriageways, the procession could not finish before 10 pm. She so estimated because at the time there were still people covering 6 football courts waiting to leave Victoria Park, which meant that it would take an even longer time for the March to finish.

11. At about 5:17 pm, the 2nd to 4th interested parties told the head of the procession that they would wait at Fenwick Street for others from Causeway Bay to arrive.

12. While the head of the procession came to a standstill at Fenwick Street, participants who had been building up in the Causeway Bay area also chanted at the police demanding to open up all the carriageways. Some individuals even charged at the police cordon line and mills barriers. At

about 5:20 pm, the participants rushed through the police cordon line and spilled out into Sugar Street, Yee Wo Street eastbound and the crossing outside SOGO Department Store. The police set up a check-line at the crossing to direct the participants back to the westbound carriageways. The traffic flow along the eastbound carriageways was seriously obstructed and much inconvenience was caused to other road users.

13. At about 5:21 pm, the police gave a formal verbal warning to the 1st interested party to move forward and proceed with the procession according to the conditions in the Letter of No Objection. The 1st interested party then raised his voice and told the participants through a microphone that he had just received a warning from the police and the police would not open up all the six carriageways. The crowd continued to chant and the 1st interested party did not follow the police's instructions to move forward with the procession.

14. At about 5:30 pm, the applicant walked around the Vehicle and returned to the driver's seat. About 5 minutes later, the 2nd interested party urged the participants through the public announcement system to walk slowly because of the heavy rain and to wait for other participants approaching from Causeway Bay. The Vehicle and the marshals then continued to move towards the direction of Admiralty. By then, the Vehicle had remained in a standstill position near Fenwick Street for 25 minutes.

A2. Arrest and seizure of mobile phones

15. After the March, the police gathered evidence including downloading a number of video footages from open sources on the internet.

After reviewing the evidence, the police on 4 July 2014 arrested the applicant and the 4 interested parties.

16. The applicant, the 1st and 3rd interested parties surrendered to the police and were arrested at the police station at around noontime on 4 July 2014. They were all arrested for (a) breach of the requirements and conditions applying to public processions under section 15(4) of the Public Order Ordinance, and (b) obstructing a police officer in the due execution of his duty under section 36 of the Offences Against the Person Ordinance[7]. The applicant was also arrested for leaving the Vehicle unattended whilst the ignition was on at Hennessy Road just past the junction with Fenwick Street under regulation 61 of the Road Traffic (Traffic Control) Regulations[8].

17. Upon arrest, the police searched the applicant and seized from him five mobile phones. After briefly inspecting each of the mobile phones, the arresting officer took possession of them on the ground that they were suspected to be related to the offence for which the applicant was arrested. Later, the police allowed the applicant to choose which two of the five mobile phones were to be returned to him. The police retained the remaining three ("the Subject Mobile Phones"), one of which was an iPhone, and in the presence of the applicant and his lawyers, put them in separate sealed tamper-proof bags. The applicant's lawyers claimed legal professional privilege in respect of the Subject Mobile Phones.

18. Likewise, upon arrest of the 1st and 3rd interested parties, their respective mobile phones were seized by the police and placed in a sealed

---

[7] Cap 212.

[8] Cap 374G.

tamper-proof envelope. They also claimed that their phones contained legal professional privileged materials.

19. The 2nd interested party was arrested in the early morning of 4 July 2014. At about 7 am, four police officers came to her flat and asked her to go with them to the police station. The 2nd interested party was then arrested outside her flat. The police officers waited for her outside her flat while she returned to retrieve her personal belongings. At about 7:40 am, the police officers and the 2nd interested party left her flat and brought her to the police station. The 2nd interested party was not searched at the time of her arrest. Nor was any house search conducted on her flat. For it was the police's assessment that no apparent danger was present against the officers at that time.

20. However, as a matter of fact, the police had on 3 July 2014 obtained a warrant from a magistrate to search the 2nd interested party's flat in connection with the suspected offence of obstructing a police officer and to seize "(i) the microphones, (ii) the speakers, (iii) the banners which were used in [the March] and (iv) all relevant articles related to the case which are likely to be of value of the investigation of the offence". That warrant was not executed and the reason was not apparent from the evidence.

21. Upon return to the police station, the 2nd interested party's mobile phone was seized. Later in the afternoon, upon her claim of legal professional privilege, her mobile phone was put in a sealed tamper-proof envelope in her and her lawyer's presence.

22. The 4th interested party was arrested at about 8:48 am on 4 July 2014, whereupon her mobile phone was seized. Likewise, upon her

claim of legal professional privilege, her mobile phone was put in a sealed tamper-proof envelope in her and her lawyer's presence in the police station. The 4th interested party was also arrested for misleading a police officer under section 63 of the Police Force Ordinance for failing to provide a correct home address to the police following her earlier arrest.

A3. Reasons for the seizure

23. It is the Commissioner of Police's case that the Subject Mobile Phones and the mobile phones of the interested parties were seized in order to preserve the potential evidence contained in them. Based on the facts narrated above, the Commissioner asserted that there was a reasonable basis to suspect that the mobile phones might be of value to the investigation of the alleged offences as they might have evidential value to prove any suspected joint enterprise between the applicant and the 4 interested parties and/or with others prior to or even in the course of the March to cause a stoppage of the procession deliberately and further cause an outbreak of the procession onto the eastbound carriageways in the Causeway Bay area. In particular, the Commissioner went on to contend, their social networking and instant messages applications might show there was a plan between the applicant and the 4 interested parties to slow down or block the procession among themselves and/or with others, thereby showing that they also had intent to obstruct the police.

A4. No inspection

24. Whatever might have been the reasons for seizure, the police in the end returned the Subject Mobile Phones and the mobile phones seized to their owners without inspection because of the claims for legal professional privilege.

B. Proceedings below

25. The seizure of the Subject Mobile Phones prompted the applicant to commence the proceedings below on 3 October 2014.

26. The applicant sought, by way of judicial review, a declaration that (1) Section 50(6) does not authorize police officers to search without warrant the contents of mobile phones seized on arrest, or (2) alternatively, that if such search power is so authorized, Section 50(6) is unconstitutional under BOR 14 and BL 30. He also sought to quash the decision of the Commissioner of Police on 4 July 2014 to seize the Subject Mobile Phones for the purpose of searching their contents ("the Decision"). The court granted leave on 8 January 2015.

27. The substantive hearing took place before the Judge on 4 November 2015. By then, the police had already returned the Subject Mobile Phones to the applicant without searching their contents because of the claim for legal professional privilege. The Commissioner invited the Judge to dismiss the judicial review as it had become academic. The Judge, however, refused to do so because he agreed with the applicant that challenges similar to the present, which concerned the scope and constitutionality of Section 50(6) in connection with the search of digital contents of seized mobile phones, were likely to arise in the future. He then adjourned the substantive hearing to 21 December 2015.

28. The Judge handed down his judgment on 27 October 2017. He identified the two main issues for his determination[9]:

[9] Judgment, at [1].

(1) whether Section 50(6) permits a warrantless search of the digital contents of a mobile phone or a similar device found on the arrested person?

(2) If yes, whether Section 50(6) is unconstitutional as it disproportionately infringes the right to privacy protected by BOR 14 and BL 30?

29. The Judge first reminded himself of the proportionality principles enunciated by the Court of Appeal in *Keen Lloyd*[10] on protection of privacy against unlawful and arbitrary interference under BOR 14 in the context of a search made pursuant to a warrant issued under section 20 of the Import and Export Ordinance (Cap 60[11]). He then referred to the Legislative Council Brief concerning the amendment leading to the present form of Section 50(6) prepared by the Security Branch dated May 1992 ("the Legco Brief"). He noted the Government's position as stated in the Legco Brief that the proposed amendment to Section 50(6) would satisfy the proportionality requirement in conducting a warrantless search by bringing it into line with common law principles[12]. He distilled from the Legco Brief the proposition that[13]:

> "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".

---

[10] *Keen Lloyd v Commissioner of Customs and Excise* [2016] 2 HKLRD 1372.

[11] Judgment, at [22].

[12] Judgment, at [49] to [52].

[13] Judgment, at [53].

30. Proceeding from that proposition, the Judge went on to hold that the view of the minority of the Canadian Supreme Court on the common law power of search incidental to arrest in *Fearon*[14] is to be preferred in providing the right balance between the protection of privacy rights and the interests of effective law enforcement in meeting the proportionality test in the Hong Kong context[15]. He reasoned[16]:

> "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*."

31. Adopting the minority's view and reasoning in rejecting the majority's in *Fearon*, the Judge held[17]:

> "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. The exigent circumstances are where, when a person has been lawfully arrested under section 50[18], 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

---

[14] *R v Fearon* [2014] 3 SCR 621.

[15] Judgment, at [55].

[16] Judgment, at [56].

[17] Judgment, at [64].

[18] That is section 50 of the Police Force Ordinance.

> of evidence, or (c) lead to the discovery of evidence in extremely urgent and vulnerable situation."

32. For the reasons that he gave, the Judge rejected the submissions of the 2nd interested party on the requirement of "legal procedures" under BL 30[19], and the submissions of the Commissioner as to why the majority view in *Fearon* should be preferred and found his reliance on the Personal Data (Privacy) Ordinance[20]("PDPO"), the Police General Orders and Force Procedures Manual misplaced[21].

33. In the result, the Judge made a declaration that Section 50(6) on a proper construction authorizes police officers to search the digital contents of a mobile phone (or a similar device) seized on arrest without warrant only in exigent circumstances; and that in so authorizing the warrantless search, Section 50(6) is constitutional and compliant with BOR 14 and BL 30. He made no order in respect to the applicant's relief to quash the Decision as the Subject Mobile Phones had already been returned to the applicant without any search of their contents.

C. Parties' stance on appeal

34. Though the wording of section 50(7) of the Police Force Ordinance ("Section 50(7)") is not that clear, it is common ground among the parties that a magistrate has the power to issue a warrant for the search of a mobile phone and other electronic devices. We accept this common

---

[19] Judgment, at [65] and [66].

[20] Cap 486.

[21] Judgment, at [67] to [80].

ground as correct in law and later on in this judgment we will explain our reasons for such acceptance for the sake of clarifying the law[22].

35. At the same time, it was common ground before us that a magistrate does not have the power to compel a person to give the police the password to unlock his mobile phone or other electronic devices. Mr Mok SC, appearing with Mr Chang and Mr Lau on behalf of the Commissioner, also accepted that refusal to give such a password to the police would not constitute an offence of obstruction of a police officer in the due execution of his duty.

36. Mr Mok further acknowledged that with developments in modern technology in many cases there will only be a very short window upon the arrest of a person for the police to gain access to the contents of that person's mobile phone before the locking of the phone is automatically activated. However, counsel submitted that there are still some cases where the determination of the issues before us would have practical significance.

C1. Submissions of the Commissioner

37. Mr Mok submitted that the power in question is a power of search incidental to arrest. Citing the discussion on such power in the common law context in *Rottman*[23], counsel submitted there was an inextricable link between a lawful arrest and the state's interest in investigating offences arising from the arrest. An arrest placed the arrested person and the materials found in his possession under the custody of the

[22] We were told by Mr Mok SC that there were doubts amongst some magistrates if they have the power to issue such warrants.

[23] *R (Rottman) v Commissioner of Police of the Metropolis* [2002] 2 AC 692.

police. There is a duty on the part of the arresting officer(s) to ensure the safety of that person as well as those in the vicinity (including the police officers themselves) and to preserve evidence found on his person. There is also a duty on the part of the police to follow up on leads that could be retrieved from information derived from the search. Delays in search may compromise the effective performance of such duties.

38. The immediate exercise of such power of search and seizure is necessary to ensure that material evidence would not disappear after the arrest and before the police have time to obtain a search warrant[24]. As an arrest would be made on reasonable suspicion of guilt, that would be a sufficient justification for the search[25]. Relying on the judgment of La Forest J in the context of fingerprinting in *R v Beare*[26] at p.413, counsel submitted that an arrested person has a lower expectation of privacy.

39. Mr Mok submitted that the common law power was not extinguished by Section 50(6)[27]. He accepted that the power is not open-ended. There is a common law requirement that the search must be truly incidental to the arrest[28] and the police must be able to explain the purposes of the search by reference to a ground incidental to the arrest: protection of persons and property, the preservation and discovery of evidence, the apprehension and detection of accomplices and safeguarding the custody of the arrested person. However, the power of warrantless search should not

---

[24] *Rottman* at [59] and [63].

[25] *Chic Fashions (West Wales) Ltd v Jones* [1968] 2 QB 299 at p.317.

[26] *R v Beare* [1988] 2 RCS 387.

[27] *Rottman* at [75], [106] and [113].

[28] *R v Caslake* [1998] 1 RCS 51 at [25]; *Fearon* at [76].

be confined to situations of emergency. There are non-emergency situations where the day-to-day operational needs of the police require the search be conducted immediately.

40. Thus, the power of search incidental to arrest is not the same as the power of search in exigent circumstances. The latter is a doctrine developed in the United States and Canada where there are constitutional safeguards against unreasonable searches[29]. There is no such doctrine in the common law of Hong Kong. It is not apposite to apply directly the jurisprudence developed from that doctrine[30] in the assessment of the impact of our BOR 14 and BL 30 on the power of search incidental to arrest.

41. Section 50(6) cannot be construed in a way to incorporate the exigency exception. Mr Mok complained that in following the approach of Karakatsanis J in *Fearon*, Au J effectively created a new common law doctrine of exigent circumstances in Hong Kong to replace the existing regime under Section 50(6) or the common law in Hong Kong.

42. In practical terms, the approach espoused by the judge is problematic. The basic problem, according to counsel, was that before

---

[29] The Fourth Amendment to the Constitution of the United States 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 Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Canadian Charter of Rights and Freedoms section 8 provides, "Everyone has the right to be secure against unreasonable search and seizure."

[30] See *Riley v California* (2014) 134 S Ct 2473; and the minority view in *Fearon*. The doctrine was developed as an exception to the presumption that warrantless search is unreasonable, see *Katz v United States* (1967) 389 US 347, *Mincey v Arizona* (1978) 437 US 385 and *Hunter v Southam* [1984] 2 SCR 145.

inspection of the contents of a phone it will often be impossible for a police officer to reasonably foretell whether (i) the safety of some persons will be put at risk; or (ii) the evidence in the phone or stored in a cloud platform will be remotely deleted; or (iii) a phone number in the mobile phone's contact or call lists will lose its relevance because it will shortly be changed; or (iv) an accomplice who had sent a message to the phone will go into hiding before a search warrant can be obtained; or (v) the phone contains information about another location where the offence would continue or further related offence would be committed.

43. Further, as highlighted by Cromwell J in *Fearon*, the exigency standard requires too much knowledge on the part of the police and gives almost no weight to the law enforcement objectives served by a prompt search incidental to arrest. It is not consistent with the underlying rationale for search incidental to arrest[31]. See [69] to [71] of *Fearon*.

44. Based on new evidence admitted on appeal[32], counsel said the time frame for obtaining a warrant is not as speedy as Au J envisaged. Because of advances in technology, the security provided by a Faraday bag could not prevent remote wiping of evidence stored in cloud. Also, once a phone is placed in such bag, internet connection would be broken and the link of the phone with information in cloud will be lost. Further, with an

---

[31] References were made to the facts of *Riley*, supra, as well as *The State v Lacey* (2015) 862 NM 2d 414 to illustrate the defeat of the object of the power of search incidental to arrest if one were to adopt the approach in *Riley* and Karakatsanis J in *Fearon*, as Au J did. Mr Mok also highlighted the observations of Alito J in *Riley* on the anomalies in the result, citing an article by Professor Leslie Shoebotham, "The Strike of Riley: The Search-Incident Consequences of Making an Easy Case Simple", (2014) 75 La L Rev 29.

[32] The affirmation of Chan Chung Yan of 3 July 2018 and the affirmation of Cao Wai Ki Raymond of 3 July 2018.

auto-lock function in place, there is only a narrow window to access information stored in a mobile phone.

45. In Hong Kong, examining the legality of the power of search against the proportionality analysis as applied here, Mr Mok submitted that the approach of the majority in *Fearon* is appropriate.

46. The legitimate interests are those set out at [39] above. They are rationally connected with the majority approach in *Fearon* which provides a prompt access to information in the mobile phone to serve these legitimate interests. Mr Mok submitted that the approach is no more than necessary to achieve these objectives and under such approach there are effective and sufficient safeguards against abuse.

47. There are also safeguards in terms of the requirement of notetaking of every form of search in the Police General Orders[33] and the requirements under PDPO.

48. Insofar as necessary, he invited the Court to apply the power of remedial interpretation to arrive at a construction of Section 50(6) which is consistent with that approach.

C2. Submissions of the Applicant

49. Mr Pun SC, appearing with Mr Wong for the applicant, submitted that there is no more residual common law power of search incidental to arrest in Hong Kong as such power is now provided for in

[33] Published and promulgated under section 46 of the Police Force Ordinance.

Section 50(6). In this connection, he relied on the cannon of construction at [25.11] of *Bennion on Statutory Interpretation* 7th Edn: the implied displacement by a comprehensive statutory scheme. He distinguished *Rottman* on the basis that the House of Lords in that case was concerned with the power of search in relation to an extradition offence that was not covered by the Police and Criminal Evidence Act 1984.

50. Whilst recognizing that there is no common law doctrine of exigent circumstances in Hong Kong, he urged this Court to adopt the same. He referred to the concept of "reasonable impracticality" discussed by Jerome Chan J in *R v Yu Yem-kin*[34] at p.98 which he read as being developed from the Canadian jurisprudence in *Hunter v Southam*[35]. Counsel also referred to another Canadian case of *R v Grant*[36] at p.243, in which the Supreme Court of Canada identified exigent circumstances which render it impracticable to obtain a warrant[37].

51. Mr Pun relied on *Wong Ho Ming*[38] at [56] to invite this Court to embrace the doctrine of exigent circumstances as part of the common law of Hong Kong.

---

[34] *R v Yu Yem-kin* (1994) 4 HKPLR 75.

[35] See citation in footnote 30.

[36] *R v Grant* [1993] 3 SCR 223.

[37] The judgment was cited by counsel at [144(2)] of the Form 86 in the present case.

[38] *Secretary for Justice v Wong Ho Ming* [2018] HKCA 173.

52. He cited some Australian and New Zealand cases[39] to show that the doctrine of exigent circumstances had been adopted in those jurisdictions in the context of the entry of private premises without prior announcement and search without warrant. In New Zealand, section 21 of the New Zealand Bill of Rights Act 1990 provides against unreasonable search.

53. Counsel acknowledged that English jurisprudence does not have a doctrine of exigent circumstances. The closest he found is the discussion in *Swales v Cox*[40] where Donaldson LJ considered at p.175 the circumstances of the power of entry into premises without warrant at common law.

54. Coming back to the context of mobile phone search, counsel highlighted the fact that mobile phones are like personal computers containing massive and extensive personal data and information. For this reason, searches of mobile phones raise special privacy concerns as the potential for invasion of privacy is high. He submitted that Au J was correct in following the approach of Karakatsanis J in *Fearon*. Though the judge reached that result by way of purposive construction, Mr Pun submitted that it would be more appropriate to reach the same result by way of an unconstitutionality declaration or remedial interpretation[41].

55. He said that Au J's formulation of exigent circumstances was too wide and discovery of evidence should not fall within the scope of the

---

[39] *Lippl v Haines* (1989) 18 NSWLR 620 at p.622 and 633; *R v Gary Shane Austin (No 2)* [2010] ACTSC 136 at [50] to [62]; *R v Jefferies* [1994] 1 NZLR 290.

[40] *Swales v Cox* (1981) 72 Cr App R 171.

[41] See the applicant's Respondent's Notice of 18 April 2018.

same. It should be confined to the circumstances set out at [137] of *Fearon*: namely, (1) when there is a reasonable basis to suspect that a search may prevent an imminent threat to safety; or (2) there are reasonable grounds to believe that the imminent loss or destruction of evidence may be prevented by a warrantless search.

56. Citing *Keen Lloyd* at [64] to [67], *R v Vu*[42] at [40] and *Fearon* at [172], counsel stressed the significance of prior scrutiny of justification by an impartial authority and the importance of judicial gatekeeping in the balance of the privacy interest of the individual against the interest of the state in investigating criminal activity[43]. The majority approach in *Fearon* did not give adequate protection as it places any decision as to the extent of access to mobile phones in the hands of police officers. After the event review (by way of judicial review) would not be an adequate safeguard. The reliance placed by the Commissioner on the Police General Orders and PDPO was, counsel said, rightly rejected by Au J[44].

57. Further, the majority approach would not be an adequate remedy because it did not provide adequate guidance to police to avoid unreasonable searches and exclusion of evidence (which is more difficult to achieve in Hong Kong due to our law on evidence[45]).

---

[42] *R v Vu* [2013] 3 SCR 657.

[43] He also referred to an article by Professor Steven Penney, *"Searches of Digital Devices Incident to Arrest*: *R v Fearon"* (2014) 23(2) Constitutional Forum constitutionnel 1.

[44] Judgment, at [72] to [75].

[45] See *HKSAR v Indra Agus Setiawati* [2018] 3 HKC 394.

58. In any event, the majority approach cannot be read into Section 50(6). It is not possible to resort to remedial interpretation to achieve that result since it involves choosing between various options which requires legislative deliberation.

59. The applicant filed evidence in reply[46] to the new evidence of the Commissioner. It was submitted on behalf of the applicant that it is the Government's duty to devise a more efficient search warrant application mechanism to redress the difficulty arising from delay occasioned by that process. In light of the prevalence of mobile phones with an automatic lock, the utility of the power to conduct warrantless search of mobile phone is very limited as it is unlikely that an arrested person will provide his / her password voluntarily. There is little reason for believing that the problem of remote wiping is prevalent. The new evidence of the Commissioner could only refer to anecdotal examples. Quoting the remarks of Roberts CJ in *Riley*, Mr Pun submitted that it is very unlikely that a police officer can come upon a phone in an unlocked state.

60. Adopting the reasoning of the majority of the Supreme Court of Canada in *R v Marakah*[47], it was submitted that the privacy interest of the senders of messages which were stored in a mobile phone were also engaged. Mr Pun said the court should tilt in favour of protecting the interests of such third parties.

61. In *R v Beare* at p.413 La Forest J drew a distinction between custodial fingerprinting and the probing into an individual's private life and

---

[46] Affirmation of Yeung Ching Yin of 25 March 2019.

[47] *R v Marakah* [2017] 2 SCR 608.

effects by way of search of his premises. Mr Pun submitted that this judgment does not support a general proposition that an arrested person should have a lower expectation of privacy concerning a search of the contents of his mobile phone.

62. He drew an analogy between such a search and the search of one's private premises. By virtue of the sensitivity and private nature of the large volume of information that is capable of being stored in a mobile phone, the privacy interest engaged is as intense as (if not more intense than) intrusion occasioned by a search of private premises[48]. The retrieval of a key found on an arrested person does not justify the use of that key to search his private premises without warrant. Likewise, the seizure of a mobile phone upon arrest does not *per se* justify the search of its contents without warrant.

63. He reiterated the submissions he advanced before Au J in contending PDPO has no application to the search of a mobile phone. It was contended that plenty of private information stored in a mobile phone does not come within the definition of personal data as defined under section 2 of that Ordinance. Further, inspection of the contents is not a collection of data which would engage principle 1(1) of the data protection principles.

64. Subject to the trimming down of the scope of exigent circumstances as indicated above, he asked the court to uphold Au J's adoption of the approach of Karakatsanis J in *Fearon*.

---

[48] *Fearon*, at [132] and [134].

C3. Submissions of the 2nd interested party

65. Mr McCoy SC, appearing with Mr Wong for the 2nd interested party submitted that this appeal should not be focused on choosing between the different approaches adopted in Canada and the United States. Instead, we should apply the proportionality analysis as discussed in *Keen Lloyd*.

66. In the Respondent's Notice of the 2nd interested party of 17 April 2018, he sought a declaration that Section 50(6) does not authorise the search for and taking into possession of the digital contents of a mobile phone on arrest. He also asked for a declaration that unless it is not reasonably practicable to obtain a warrant, the search and seizure of such digital contents must be authorised by a warrant.

67. Thus, the norm is that a search of the digital contents of a mobile phone without consent[49] should only be done with a warrant. There is an exception in cases where it is not reasonably practicable to obtain a warrant before the search. At the hearing before us, Mr McCoy further refined his formulation of the exception as follows – if it is not reasonably practicable to obtain a warrant, a police officer may lawfully search the digital contents:

(a) no more than is necessary, and

(b) limited to what is reasonably believed to be directly and immediately relevant to the offence(s), the subject of the arrest, and

(c) only if the police officer forthwith provides to the arrestee a written inventory of the files searched and/or copied, and

[49] Mr McCoy submitted that the consent must be informed and in written form.

(d) the arrestee (or other person affected by the seizure of the mobile phone) has a right to apply to a magistrate under section 42 of the Magistrates Ordinance for its return, conditionally or unconditionally, and

(e) the Commissioner shall where the arrestee is not charged or is acquitted, forthwith destroy or, if the arrestee prefers, deliver to that person all copies of the files made.

68. The requirement of reasonable belief under (b) is necessary because, according to Mr McCoy, a test premised on reasonable suspicion offers no protection to an arrested person. He accepted that the written inventory under (c) can be deferred if a senior officer of the rank of Superintendent or above certifies that the immediate supply of an inventory will compromise ongoing investigation.

69. Though he accepted that principle 2 of the data protection principle in PDPO is applicable in relation to digital contents retrieved by the police from the mobile phone of an arrested person, Mr McCoy submitted that more effective redress should be provided by safeguarding against abuse. Thus, a summary application to a judicial officer for the return of the phone should be provided and counsel invited us to construe the expression "a person charged" in section 42 of the Magistrates Ordinance to include an arrested person whose mobile phone has been searched upon arrest.

70. The requirement under (e) is transposed from section 59(2) of the Police Force Ordinance by way of analogy.

71. The concept of reasonable impracticality is familiar in this jurisdiction in terms of justification for search without warrant[50]. Counsel submitted that in light of the judgment in *Keen Lloyd* a statutory provision cannot be construed as granting a law enforcement officer blanket, warrantless power of search and seizure. Thus, given the right of privacy protected by BOR 14 and BL 30, Section 50(6) cannot be construed in a manner to grant the power of a warrantless search of a mobile phone to the police so long as there is an arrest and a phone is found on the person of the arrestee.

72. Unlike Mr Pun, Mr McCoy accepted that there is residual common law power of search incidental to arrest notwithstanding the enactment of Section 50(6). Given the tremendous amount of confidential information that can be stored in a mobile phone, there should not be any distinction between the contents so stored in a phone and the contents stored in a private place or premises. In the light of technological advances, the limits placed on the residual common law power to conduct a warrantless search should at least be on par with the common law power to conduct such a search at private premises. The principles discussed in *Keen Lloyd* are therefore equally apposite.

---

[50] Counsel referred to the following ordinances using this concept to permit warrantless search of premises: Immigration Ordinance, Cap 115, s56; Dangerous Drugs Ordinance, Cap 134, s52; Dogs and Cats Ordinance, Cap 167, s6; Wild Animals Protection Ordinance, Cap 170, s17B; Fisheries Protection Ordinance, Cap 171, s5; Marine Fish Culture Ordinance, Cap 353, s17; Merchant Shipping (Seafarers) Ordinance, Cap 478, s123; Non-local Higher and Professional Education (Regulation) Ordinance, Cap 493, s24; Aviation Security Ordinance, Cap 494, s57; Copyright Ordinance, Cap 528, s123; Prevention of Copyright Piracy Ordinance, Cap 544, s19; Private Columbaria Ordinance, Cap 630, s60. See also the discussions in *Keen Lloyd*, *HKSAR v Indra Agus Setiawati*, and *HKSAR v McCall* HCCC 446/2016, 25 September 2017.

73. The privacy interest on the digital contents of a mobile phone[51] is, according to Mr McCoy, higher than the physical content within private premises[52]. Thus, giving due weight to the rights protected under BOR 14 and BL 30, the balance to be struck in terms of permitting warrantless search should be correspondingly more stringent.

74. He submitted that as the privacy interest in personal information has to be considered as a whole[53], it is no answer to say that the search will often be specific in scope.

75. Mr McCoy argued that it is not necessary for Hong Kong to adopt the doctrine of exigent circumstances as developed in the North American jurisprudence. He preferred the approach of Deputy High Court Judge Bruce in *HKSAR v Indra Agus Setiawati*. Therefore, Mr McCoy's formulation at [67] above is made by reference to the concept of reasonable practicalities instead of confining the exception to the closed parameters under the doctrine of exigent circumstances. Counsel said the concept of reasonable practicalities inherently allows for flexibility depending on the circumstances. In this respect, he alluded to the discussion in *HKSAR v McCall*, HCCC 446/2016, 25 September 2017, in which the test was applied by reference to the knowledge of the team of officers conducting the search.

---

[51] Mr McCoy equated that with the privacy interest in relation to search of computers as discussed in *R v Morelli* [2010] 1 SCR 253.

[52] Counsel relied on the observation of Karakatsanis J in *Fearon*, at [152].

[53] He cited two Canadian articles for this proposition: one by Colton Fehr & Jared Biden at (2015) 20:1 Canadian Criminal Law Review 93 at p.109; another one by Agathon Fric at (2016) 21 Appeal 59.

76. He submitted that the police concern about the threat to investigations are overstated because our rules of admissibility of evidence have always struck a fair balance between an individual's rights and the public interest in criminal investigation and prosecution[54].

77. Ultimately, it is a matter of common sense evaluation. A planned operation including arrest (with ample time to obtain a warrant in advance) is different from an officer acting spontaneously on the spot where an ongoing crime is taking place. Also the nature of the offence involved is relevant. Whilst warrantless search may be necessary in dynamic and serious crimes, there will not be such need with less serious offences. It would be best to leave it to the judge presiding at the criminal trial to determine on the admissibility of evidence with a full grasp of the facts and operational details in accordance with well-established principles.

78. *Rottman* did not decide that search incidental to arrest should not be subject to any constraints by virtue of the need of a law enforcement officer to gain control of anything or information which is incidental to an arrest found upon an arrested person without regard to his interest in privacy. First, a warrant of arrest had been issued in that case and to that extent there was judicial scrutiny beforehand. Second, the case did not deal with the digital contents of a mobile phone which called for more stringent scrutiny. Third, the common law power of search incidental to arrest does not authorize a law enforcement officer to disregard privacy interests. There is no clear right to strip or wash at common law[55]. There is also no right to

---

[54] He referred to *HKSAR v Chan Kau Tai* [2006] 1 HKLRD 400 and *HKSAR v Muhammad Riaz Khan* (2012) 15 HKCFAR 232.

[55] *R v Golden* [2001] 3 RCS 679, at [113].

take fingerprints without consent[56], or to take intimate samples[57] or to conduct medical procedures even though such information would be relevant to the criminal investigation.

79. In light of this analysis, one cannot take the observation of Salmon LJ in *Chic Fashions (West Wales) Ltd v Jones* as supporting a lower level of protection of privacy of an arrested person in all respects. With reference to BOR 11, Mr McCoy submitted that the privacy interest concerning one's digital data in a mobile phone should be enhanced rather than diminished after his arrest.

80. No matter how desirable it is from a law enforcement point of view, the court should not adopt a construction of Section 50(6) which is not warranted by a construction informed by the purpose of the section. Citing the judgment of French NPJ in *Cheng Ka Yee*[58], counsel emphasized that the court should not identify a purpose which it thinks would be beneficial and then construe the statute to fit it.

C4. Submissions of the Commissioner on the proposed formulation of Mr McCoy

81. Mr Mok submitted that an overriding test of reasonable practicability cannot sufficiently serve the legitimate interests underlying the power of search incidental to arrest. It is difficult for a police officer who may have to make a snap decision on the spot to assess if it is practicable to

---

[56] *Grollo v Bates* (1994) FLR 218, at pp.222G-223E.

[57] *R v Stillman* [1997] 1 SCR 607.

[58] *SJ v Cheng Ka Yee* [2019] HKCFA 9.

wait for a warrant to be issued. He however accepted that the reasonable practicability of obtaining a warrant can be one relevant factor in the overall assessment.

82. There should not be a requirement as per (b) in Mr McCoy's formulation (see [67] above) because the purposes for conducting a search incidental to arrest should not be confined to materials relevant to the offence for which the arrest is made. Nor should there be a criterion of "direct and immediate" relevance. Mr Mok submitted that a reasonable suspicion that the search can be useful in furtherance of the law enforcement objectives for which the power of search incidental to arrest is conferred should suffice. He repeated his earlier submission that a test based on reasonable belief (as opposed to reasonable suspicion) cannot be fulfilled and would practically wipe out the power of search incidental to arrest as far as the contents of a mobile phone are concerned.

83. He had no objection to the supply of an inventory provided that the obligation could be deferred if it would compromise ongoing investigation.

84. As regards summary application, Mr Mok submitted that an application under section 102 of the Criminal Procedure Ordinance is more appropriate than section 42 of the Magistrates Ordinance.

85. As regards the limitation on the retention of search materials, Mr Mok reiterated that sufficient safeguards and redress are provided under PDPO.

C5. The 2nd interested party's submissions on the applicability of section 102

86. With the leave of the Court, Mr McCoy provided short submissions on section 102 of the Criminal Procedure Ordinance after the hearing.

87. He submitted that the section is only engaged if there is proof that the mobile phone was used in connection with any offence (section 102(1)(a)), or that an offence has been committed in respect of it (section 102(1)(b)), or that it has been used in the commission of an offence (section 102(1)(c)). On either limb, the commission of an offence is a prerequisite. An applicant would therefore have to prove the very thing that he may be denying in order to invoke the section.

88. The reality is that the section has only been used after a conviction or by an owner of the seized items where undeniably an offence has been committed by a person unknown.

89. In the context of a mobile phone seized upon arrest, it is more appropriate to apply under section 42 of the Magistrates Ordinance.

D. Discussion

D1. Central issues and general approach

90. Section 50(6) authorizes the police to conduct a search of an arrested person without a warrant in these terms:

> "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."

91. Implicit in the power to search is the power to examine the contents of "any newspaper, book or other document or any portion or extract therefrom and any other article or chattel" seized. For without the power to examine the contents, the power to search is quite meaningless in furtherance of the purpose of Section 50(6).

92. Under our common law, the power of search incidental to arrest entitles the police (or other law enforcement authority) to procure evidence (including the gathering of information) in respect of the crime committed, to prevent its destruction and to protect the officers of law enforcement and the public. These purposes, which may be summarised as procure, prevent and protect, are all dependent on a lawful arrest being made in the first place. It is a power conferred by the common law on all law enforcement officers who have the power of arrest.

93. Whilst the majority in *Riley* seemed to view the common law power, at least in its more modern incarnation, as restricted to prevention (in the sense of preservation of evidence) and protection, Justice Alito, who concurred in part with the majority but voiced his concerns in a separate judgment, was not persuaded that the common law power should exclude the procuring (or gathering) of evidence from its ambit. He cited the English case of *Dillon v O'Brien* in 1893, in which it was held that "it is clear, and

beyond doubt, that … constables … are entitled, upon a lawful arrest by them of one charged with treason or felony, to take and detain property found in his possession which will form material evidence in his prosecution for that crime"[59].

94. The decision in *Riley* has not been without its critics. In a paper entitled "*The Strife of* Riley*: The Search-Incident Consequences of Making an Easy Case Simple"* published in the Louisiana Law Review[60], the author considers that "*Riley* is the deceptively simple beginning of the end of evidence gathering as a justification in a properly limited search incidental to arrest"[61]. He concludes[62]:

> "After *Riley*, evidence gathering seems to have been left in the dust – nothing more than a pit stop on the highway to a search-incident doctrine that is now based exclusively on officer safety and preventing the destruction of evidence. Only Justice Alito recognized the *Riley* Court's error in excluding evidence gathering as a legitimate rationale in a properly limited search incident to arrest. And, judging from the ancient history of the search-incident doctrine and the consequences that *Riley*'s most recent doctrinal reorganization will have, Justice Alito was right."

95. Although the United States have sought to limit the common law power, both the majority and the minority of the Canadian Supreme Court in *Fearon* acknowledged its tri-partite purpose. Their different positions were concerned with how to make the power compliant with section 8 of the Canadian Charter.

---

[59] *Dillon v O'Brien*, 16 Cox Cim Cas 245, 249-251 (1887).

[60] "*The Strife of* Riley: *The Search-Incident Consequences of Making an Easy Case Simple*" by Professor Leslie A Shoebotham, 75 La L Rev 29 (2014).

[61] *Ibid.*, p.30.

[62] *Ibid.*, p.70.

96. The important law enforcement objectives behind the power of search incidental to arrest were summarised in *Fearon* in the headnote to the judgment of the majority as[63]:

> "… to identify and mitigate risks to public safety; locate firearms or stolen goods; identify accomplices; locate and preserve evidence; prevent suspects from evading or resisting law enforcement; locate the other perpetrators; warn offices of possible impending danger; and follow leads promptly".

97. Each of those objectives come within the sweep of the procure, prevent and protect purposes of the common law power and may properly be regarded as truly incidental to a lawful arrest.

98. As will be expanded below, the search incidental to arrest, whether it is authorized by statute or under the common law, reflects important law enforcement objectives. But it is also necessarily an intrusion into the arrested person's privacy, which is protected by BOR 14 and BL 30.

99. Under BOR 14:

> "(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."

100. And pursuant to BL 30:

> "The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual

---

[63] *Fearon*, at p.623.

> 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."

101. The central issue arising from facts similar to the present case is thus: how is a search of the digital contents of a mobile phone or similar device found on or seized from an arrested person incidental to arrest to be conducted in a manner that is compatible with BOR 14 and BL 30? More specifically, is a judicial warrant always required before such a search can be carried out? If yes, Section 50(6) is of no avail. If, however, a judicial warrant is not always required, how is the warrantless search to be conducted, be it under Section 50(6) or the common law, in order to make it compatible with BOR 14 and BL 30?

102. In determining these issues, we adopt the approach laid down by this Court in *Keen Lloyd*.

103. For reasons expanded upon below, we are of the view that a search of the digital contents of a mobile phone (as opposed to the mobile phone itself as an object) as a specie of the power of search by law enforcement officer incidental to arrest is governed by the common law instead of Section 50(6)[64]. Also, as explained below, we do not and need not have the doctrine of exigent circumstances under our common law in Hong Kong. With the familiarity by those responsible for administration of criminal justice in Hong Kong with the concept of reasonable practicality as the guide for search without warrant, we are of the view that this should also be a guide for warrantless search of the digital contents of mobile phone

---

[64] See [160] below.

under our common law when such power is exercised by a law enforcement officer.

104. Thus, instead of choosing between the approach of the majority and that of the minority in *Fearon*, the correct approach for the development of the common law in Hong Kong is to adopt a set of criteria which must also satisfy the proportionality approach as discussed in *Keen Lloyd*.

105. Though the Court was not concerned with the power of search incidental to arrest in *Keen Lloyd*, in our view the general considerations discussed therein on the importance of safeguards by way of prior judicial scrutiny apply equally to a search of the digital contents of a mobile phone even in the context of a search incidental to arrest. As will be discussed below, a warrant can be obtained under Section 50(7) for the search of the digital contents of a mobile phone. Given the engagement of the rights protected under BOR 14 and BL 30 and the potentially high privacy interest of the digital contents stored in a mobile phone (which in many cases would be even higher than the privacy interest engaged in a search of private premises), we hold that even in the context of a search of such materials incidental to an arrest a warrant should be obtained before a search unless it is not reasonably practicable to do so. In processing an application for such warrant, a judicial officer must bear in mind the judicial gatekeeping role discussed under Section B3 in the judgment of *Keen Lloyd*.

106. As held in *Keen Lloyd*, any warrantless search must be subject to scrutiny under the proportionality test. The set of criteria permitting a warrantless search of digital contents of a mobile phone must serve legitimate interests, rationally connected with such interests and the permitted search should be no more than necessary to accomplish such

interests. In the context of the protection of privacy interest when an individual is subject to warrantless search, the courts will be vigilant in ensuring that adequate and effective safeguards against abuse are in place with strict limits on such power of search[65].

107. Whilst adequate and effective safeguards can be provided through after-the-event judicial redress, Strasbourg jurisprudence[66] (which, as held in *Keen Lloyd*, was good reference for the assessment of proportionality in the Hong Kong BOR 14 and BL 30 context) suggests that in order to be effective and adequate the power of warrantless search cannot be of such width that applicants face formidable obstacles in showing that the search is an abuse of power and make it difficult for judicial redress to provide a real curb on arbitrary interference and abuse of power.

108. In the recent case of *Beghal v The United Kingdom*[67], the European Court of Human Rights summarized at [88] the general principles on assessment of legal protection against arbitrary interference with the right to respect for privacy as follows:

> "… In matters affecting fundamental rights it would be contrary to the rule of law … for a legal discretion granted to the executive to

---

[65] See the discussion at [58] to [70] of *Keen Lloyd*.

[66] See *Gillan and Quinton v The United Kingdom,* Application No. 4158/05 at [79] to [87] where the breath of the discretion was described at [83] as follows: "Not only is it unnecessary for him to demonstrate the existence of any reasonable suspicion; he is not required even subjectively to suspect anything about the person stopped and searched. The sole proviso is that the search must be for the purpose of looking for articles which could be used in connection with terrorism, a very wide category which could cover many articles commonly carried by people in the streets. Provided the person concerned is stopped for the purpose of searching for such articles, the police officer does not even have to have grounds for suspecting the presence of such articles." See also *Ivashchenko v Russia,* Application No. 61064/10 at [85] and [88] and *Beghal v The United Kingdom* Application No. 4755/16 at [94], [103] to [105].

[67] See citation in footnote 66.

> be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise … The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed."

109. At [89], the European Court identified several factors for assessing the adequacy of safeguards against arbitrary interference:

> "… In making this assessment, it will consider the following factors: the geographic and temporal scope of the powers; the discretion afforded to the authorities in deciding if and when to exercise the powers; any curtailment on the interference occasioned by the exercise of the powers; the possibility of judicially reviewing the exercise of the powers; and any independent oversight of the use of the powers."

110. As *Keen Lloyd* had been decided before the fourth limb of the proportionality test was adopted by the Court of Final Appeal in *Hysan*[68], the set of criteria should also take into account the severity of the deleterious effects of a measure on the individual concerned so that a fair balance is struck between the societal benefits of the encroachment and the inroads on the privacy interest of the individual.

111. There are several considerations which provide the necessary contextual framework for the proportionality analysis in resolving the issues before us. We will discuss them in turn in Sections D2 to D6.

D2. Privacy interest of digital contents on mobile phones

112. When they were first introduced a few decades ago, mobile

[68] *Hysan Development Co Ltd v Town Planning Board* (2016) 19 HKCFAR 372.

phones were still relatively novel and unsophisticated. Thanks to the technological advent of mobile communications and computing technology, today they are ubiquitous and intelligent. They have evolved from telephones simpliciter available to a few who could afford them into multifunctional minicomputers used regularly by the vast majority.

113. We no longer use mobile phones simply as telephones. We regularly use them to conduct many aspects of our daily life. We use them as instantaneous communication tools, cameras, voice or video recorders and players, calendars, diaries, albums, televisions, maps or newspapers. We use them for emails, social media, the internet, millions of apps covering all aspects of our life. We even use them to conduct our bank or financial affairs. As Roberts CJ observed in *Riley* at p.2484, mobile phones are now such a pervasive and insistent part of daily life that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy".

114. In terms of privacy interest, three important characteristics arising from the use of a mobile phone distinguish it from other objects that might be kept on an arrestee's person: (1) the vast amount and unique nature of the personal information stored in it; (2) storage of such information on "cloud" accessible by the mobile phone; (3) the portability and accessibility of such information.

D2.1. Amount and nature of personal information

115. The regular use of a mobile phone as a multifunctional minicomputer to conduct one's daily life generates a wealth of information about the intimate details of the user, including the user's interests, habits,

identity, familial, political, professional, religious and even sexual associations without the knowledge or intent of the user. It is also a special repository of such personal data. See *Fearon*, per Cromwell J at [51], and *Riley*, per Chief Justice Roberts at p.2490. As Karakatsanis J in *Fearon*, at [101] put it:

> "[mobile phones] record not only our core biographical information but our conversations, photos, browsing interests, purchase records, and leisure pursuits. Our digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas. [They] are windows to our inner private lives."

116. In short, a mobile phone is capable of providing a very detailed and accurate profile of its user. The privacy interest involved in a search of the contents of an arrestee's mobile phone would necessarily go beyond the ordinary level of privacy that would be intruded upon in a traditional search of things found on his person on arrest.

D2.2. "Cloud" storage and technology

117. The data that a user views on his mobile phone may not in fact be stored on the device itself. The data may in fact be stored on a remote server known commonly as "cloud" and the user views it by using the "cloud computing" technology. In simple terms, "cloud computing" enables internet-connected devices, mobile phones included, to access and display data stored on remote servers rather than on the device itself. In tapping the information stored on the "cloud", mobile phones function not as a storage but as a key to the remote server. That means that the mobile phone enables access to additional personal information of its user not already stored on the device. It adds an additional dimension to the privacy interest

involved in a search of the contents of the mobile phone. The scope of the privacy interest at stake may become wider than what is already stored on the mobile phone.

D2.3. Portability and accessibility

118. In the past, people did not typically carry a cache of sensitive personal information with them as they went about their daily lives. But in the digital age, the person who is not carrying a mobile phone, with all that it contains and with all that it can gain access by the cloud technology, is the exception. See *Riley*, per Roberts CJ at p.2490.

119. The fact that modern technology allows an individual to carry with him such intimate personal information on his mobile phone and the means of access to such information stored remotely by his mobile phone, of course, does not detract from the full protection against unlawful intrusion of his privacy to which he is entitled under BOR 14 and BL 30. On the contrary, subject to the protection afforded by various security measures which we will come to shortly, the user's intimate personal information, whether it is stored on or accessible by the mobile phone, is so vulnerable to unlawful intrusion upon inspection by just a tap on the screen that the law must ensure that his privacy interests under BOR 14 and BL 30 are sufficiently protected.

D3. Security features impacting on obstruction and access of digital contents on mobile phones

120. For obvious reasons, mobile phones are equipped with security features to safeguard the digital contents stored in them from unauthorized

access. However, from the perspective of the police, the security features might impede their timely access to the digital contents stored on or accessible by the device for law enforcement purposes. In his affirmation filed on 23 October 2018, Chief Inspector Raymond Cao Wai Ki, of the Forensics Investigation Section of Technology Crime Division, Cyber Security and Technology Crime Bureau of the Hong Kong Police Force, described the common and nowadays security features of digital devices and characteristics of computer hardware and online services that allow the destruction of, and obstruction of access to, the digital contents of a seized device at the time after an arrest pending a warrant. He raised four main points.

D3.1. Strong encryption

121. First, most of the smartphones these days employ a strong encryption function. Once it is screen-locked or powered-off, accessing its data contents would be extremely difficult, if not impossible, without the password. Typically, upon arrest, there is only a small window of time or opportunity to examine the data contents before the arrestee's mobile phone is powered-off or screen-locked, whether automatically or manually. And it is extremely rare that the arrestee's mobile phone is not protected by a password. It follows that if his mobile phone is screen-locked or powered-off during the time needed to apply for a search warrant, there is a real risk that the police would not be able to, and in any event only with great difficulty, access the encrypted data even if a search warrant were later obtained.

122. Any suggestion that the police de-activate the screen-lock or power-off function pending a warrant is impractical. That is because, given

the modern security features of smartphones, a person would need to input the password (whether alpha-numerical or biometric) in order to de-activate the screen-lock or power-off function. A police officer not provided with the password (and in this respect, we would point out, the police could not under the law compel the arrestee to provide the password), simply could not de-activate the function.

D3.2. Multi-access to cloud platforms

123. Data contents of a digital device can be stored on cloud platforms or its local disk storage. Frontline police officers examining the contents of the digital device would not typically know whether the information they are viewing is stored locally at the time of the arrest or has been pulled from the cloud. Cloud platforms such as "Google Drive", "One Drive" and "Facebook" are widely used by internet users. With the same set of login credentials, users can access these digital contents by using different network-connected digital devices at any time and place instead of being limited to the physical position of the phone. Some of the cloud platforms even support multiple concurrent accesses by different users using different digital devices at the same time. There is also a possibility that the digital data may not be stored in the digital device itself, and that it may be downloaded from the internet whenever necessary and stored temporarily in the memory of the digital device, hence all such data cannot be viewed from the digital device itself once it is powered-off.

124. Thus, practically the only available chance to discover and fully preserve such digital evidence is when the seized digital devices are still switched on and connected to the cloud platforms via the internet. The risk of remote access to the volatile digital contents stored on cloud platforms by

other users via other digital devices, pending the obtaining of a search warrant, should not be negated. The risk cannot be sufficiently addressed by sealing the seized digital devices in a single shielded bag because the data stored on cloud platforms can be accessed, amended and/or deleted by the device owner and any other persons who have knowledge of the login credentials or any other digital devices with the login credentials preset on it. A delayed examination would hamper the retrieval of vulnerable digital evidence and may jeopardize the whole investigation.

D3.3. Retrieval of volatile and temporary memory

125. It is of paramount importance for police officers to timely capture all data contents on Random Access Memory ("RAM") or other volatile data on a mobile phone as they are only temporarily stored for the purpose of performing quick-access computations. All the memory contents on RAM will be lost once the host computer (ie the seized mobile phone) is powered-off. Therefore, when handling a malware infected computer at the scene of crime, police officers, upon the technical advice offered by a forensic examiner, should extract crucial data from the memory contents on RAM for tracing suspicious programmes which are initiated by a specific malware. Such information will never be recovered in the later stage of investigation if the computer is powered-off. Further, memory contents stored on RAM will be overwritten by the data from other system activities during the on-going operations of the host computer. Such crucial data may be permanently lost whilst waiting for a search warrant.

D3.4. Other difficulties

126. There are some other difficulties occasioned by technological developments.

127. First, some files stored on certain smartphones would be automatically erased after a preset time period. Forensically speaking, such erased data cannot be retrieved or recovered. Should there be a delay in the examination or preservation process, there is a risk that files that are crucial to the investigation may be permanently erased.

128. Second, suspects can use special devices such as Thin-Client computers, ie computers without permanent storage function, or specially designed "USB" thumb drives, which leave no trace on the computer itself throughout the entire operation. In such cases, on-site data extraction is the only practicable and necessary means to prevent the loss of vulnerable digital evidence.

129. Third, facial recognition, fingerprint, and iris sensors are just some of the already established security features designed to prevent unauthorized access to the digital contents of a smartphone today. The enhanced security also means that there would be an increasingly small window of opportunity to obtain crucial digital evidence, which is often only available at the crime scene. If the examination of the contents of a digital device is further delayed by a search warrant application, the likelihood of unearthing relevant evidence could be further diminished especially without prior knowledge of the security features of the target device.

130. In consequence, Chief Inspector Cao maintains that in light of technological developments, there is a real risk of destruction of, or obstruction of access to, the digital contents of mobile phones in the time needed to apply for a warrant. As the matter now stands, there are no reasonable and practicable solutions as an alternative to address the risk satisfactorily, which would seriously undermine legitimate law enforcement objectives.

D4. Practical considerations

D4.1. The use of mobile phone and digital technology for criminal purposes

131. The advent of information technology and the popular use of mobile phones also present new modes for criminal activities to be conducted. As observed by Cromwell J in *Fearon* at [48], in the modern world drugs traffickers use mobile phones to conduct their illicit trade[69]. Since the illicit communications are often conducted electronically, the digital data stored in the mobile phones of such criminals are of high probative value in the proof of their involvement in those crimes.

132. Another example of the use of mobile phones for criminal activities can be found in the case of *R v Powell*[70] where kidnappers used texted messages and audio clips through a highly secure application called "Silent Circle" to perpetuate the offence. Messages were sent under the application without the intermediate intervention of an independent

[69] See also *R v Jones* [2015] SKPC 29 at [55], [62] and [64].

[70] *R v Powell* [2017] ONSC 6482.

computer server so that such communications were very difficult to trace, see [9] of the judgment.

133. The law should recognize the new challenges presented by the use of mobile phones as instruments of crime and the legitimate need for law enforcement officers to search such phones in appropriate circumstances with appropriate safeguards. The digital world should not become a haven for criminals where a black-hole is created so that crucial evidence for the proof of their unlawful activities could become out of reach for law enforcement officers.

134. In his separate judgment in *Riley*, Justice Alito referred to the anomaly of the courts striking the balance in favour of privacy interests where the information or evidence in issue happens to be contained in a mobile phone rather than some other hard copy form[71]:

> "Suppose that two suspects are arrested. Suspect number one has in his pocket a monthly bill for his land-line phone, and the bill lists an incriminating call to a long-distance number. He also has in his wallet a few snapshots, and one of these is incriminating. Suspect number two has in his pocket a cell phone, the call log of which shows a call to the same incriminating number. In addition, a number of photos are stored in the memory of the cell phone, and one of these is incriminating. Under established law, the police may seize and examine the phone bill and the snapshots in the wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out."

135. Interestingly, the two examples given by Justice Alito exemplify two distinct types of evidence which may be relevant to the investigation of an offence. The first type of evidence is concerned with the fact that the defendant made a particular phone call which happens to

---

[71] *Riley*, at p.2497.

incriminate him. The privacy that is compromised is related not to the content of any conversation or communication in the phone call but to fact that the defendant has actually made the call.

136. By contrast, the second type of evidence is concerned with evidence which, by its very content, inculpates the defendant in the crime itself (in *Fearon*, the texted admission to the robbery and the photograph of the handgun contained in the mobile phone). The privacy that is compromised in this situation is the defendant's actual private communications with others, which have then been stored in his mobile phone.

137. During the course of argument, we put to the parties two examples adapted from previous cases before the criminal division of our Court of Appeal. The first concerned a gang of foreign pickpockets who were observed operating in a department store. The police believed that they were in communication by telephone: one defendant stealing goods at the instruction of a second defendant, while the third and fourth defendants acted as lookouts inside and outside the store. The police were not so much interested in what the accomplices were actually saying to, or texting, each other – indeed, the police officers involved would not immediately have understood the language being used – as the fact that they were in communication with each other by telephone at the material time.

138. The second example concerned a defendant who was observed driving dangerously and erratically by the police. It was suspected that the driver was sending or reading text messages on his mobile phone while driving. Again, the police were not interested in what the defendant was

writing to, or reading from, another but with the fact that he was using his mobile phone whilst he was driving.

139. In both of the Court's examples, as with Justice Alito's first example, the police were not concerned with what the accused had communicated, but with the fact of the communication itself. The monthly telephone record showed complicity in the offence; the fact that four thieves were in communication was evidence of conspiracy; whilst the use of the mobile phone when driving was relevant to a very element of the offence, namely the dangerousness of his driving. In none of these examples was it relevant to know what the accused had actually communicated with another.

140. It is difficult to see why, in these circumstances, a police officer should not be able to *procure* such evidence of the commission of the offence (or *prevent* its destruction), assuming such a search is incidental to an otherwise lawful arrest.

141. By contrast, it may be argued that a texted admission and the photograph of a gun used in the robbery (as in *Fearon*), or the incriminating photograph in Justice Alito's second example, all of which were stored in a mobile phone as a result of the accused communicating with another is different; for in any of those situations, the search clearly and directly impinges on the accused's private communications with other people.

142. However, if the privacy of the individual weighs so heavily in the balance when weighed against the objective of law enforcement, the nature and extent of the intrusion must surely be relevant to that equation. As our assessment of these examples makes clear, a relevant consideration is what the police officer is looking for (or reasonably believes he is looking

for) and how the individual's privacy right is in fact infringed. The majority in *Fearon* considered that[72]:

> "… while cell phone searches … may constitute very significant intrusions of privacy, not every search is inevitably a significant intrusion. Suppose, for example, that in the course of the search in this case, the police had looked only at the unsent text message and the photo of the handgun. The invasion of privacy in those circumstances would, in my view, be minimal. So we must keep in mind that the real issue is the potentially broad invasion of privacy that may, *but not inevitably will*, result from law enforcement searches of cell phones."

143. The Court in *Fearon* went on to distinguish between the seizure of bodily samples and strip searches, which were described as "very great invasions of privacy and are, in addition, a significant affront to human dignity"[73], something that could not be said of mobile phone searches incidental to arrest. Furthermore, "a person who has been lawfully arrested has a lower reasonable expectation of privacy than persons under lawful arrest"[74]. Nevertheless, the Court accepted that there must be "some meaningful limits" on the scope of a telephone search. It held[75]:

> "The search must be linked to a valid law enforcement objective relating to the offence for which the suspect has been arrested. This requirement prevents routine browsing through a cell phone in an unfocussed way".

144. The Court was clearly concerned to provide protections for the suspect "against the risk of wholesale invasion of privacy which may occur if the search of a cell phone is constrained only by the requirements that the

---

[72] *Fearon*, at [54].

[73] *Ibid.*, at [55].

[74] *Ibid.*, at [56].

[75] *Ibid.*, at [57].

arrest be lawful and that the search be truly incidental to arrest and reasonably conducted"[76].

145. We acknowledge that a higher privacy interest arises where the police (or other law enforcement authority) seek to discover and rely upon what was actually said in a text message, or an email, or what is recorded in the content of a file in a mobile phone.

146. That higher interest, however, only arises when the police officer has decided what he is looking for in the mobile phone. In reality, he may not know. That is why the majority in *Fearon* described the search incidental to arrest power as an "extraordinary"[77] one; not simply because it allows searches to be made without a warrant, but that it does so in circumstances in which the grounds to obtain the warrant do not necessarily exist. Yet, the necessity for the police officer "to be able to promptly pursue their investigation upon making a lawful arrest is an important consideration underlying the power to search incidental to arrest"[78].

147. The balance between individual and societal privacy interest on the one hand and law enforcement objectives on the other highlights the difference between the *Riley* approach and the *Fearon* approach. The Supreme Court of the United States has adopted a policy that is certainly principled, clear-cut and of universal application, save in circumstances of exigency and emergency:

---

[76] *Ibid.*, at [58].

[77] *Ibid.*, at [16].

[78] *Ibid.*, at [17].

> "Our answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple – get a warrant."[79]

148. Even though the Court in *Riley* accepted that "an individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving"[80], the Court still held that the police would not be entitled to examine the driver's telephone without a warrant. Yet this particular example is perhaps the least intrusive of the individual's privacy rights, and one which many ordinary people would readily understand and accept should yield to more important considerations of public safety.

149. The Supreme Court of Canada has preferred a less categorical approach to the power of search incidental to arrest, and one to which safeguards could be prescribed and attached. For reasons we have stated elsewhere, we prefer the less categorical approach, albeit one moulded to the particular conditions and circumstances of Hong Kong. As Lamer CJ held in the earlier Canadian Supreme Court decision of *R v Caslake*[81], the scope of search incidental to arrest engages many different aspects of the search: for example, the nature of the items seized, the place to be searched and the time between arrest and search. And as the majority in *Fearon* also observed, arrests will relate to many different crimes and will be made in many different circumstances[82]:

---

[79] *Riley*, at p.2495.

[80] *Riley*, at p.2492.

[81] *R v Caslake*, at [15] and [16].

[82] *Fearon*, at [13].

> "It follows that the permissible scope of searches incident to arrest will be affected by the particular circumstances of the particular arrest. The courts will rarely be able to establish any categorical limit applicable to all arrests and all purposes incidental to them".

150. The New Zealand Court of Appeal in *R v Grayson and Taylor*[83] has likewise preferred a less categorical approach in this particular area of the law:

> "Reasonable expectations of privacy are lower in public places than on private property. They are higher for the home than for the surrounding land, for farm land and for land not used for residential purposes. And the nature of the activities carried on, particularly if involving public engagement or governmental oversight, may affect reasonable expectations of privacy. An assessment of the seriousness of the particular intrusion involves considerations of fact and degree, not taking absolutist stances. In that regard, and unlike the thrust of the American Fourth Amendment jurisprudence, the object of s 21 is vindication of individual rights rather than deterrence and disciplining of police misconduct."

151. The difficulty for the courts is in delineating what are the "meaningful limits" on the scope of mobile phone search in a search incidental to arrest situation, so that both the police officer (or other law enforcement officer) and the accused can know with reasonable certainty what the officer is entitled to do. That difficulty is exacerbated where the officer may not know precisely what he is looking for in searching the mobile phone but reasonably believes that it comes within the procure, prevent or protect purpose which grounds the common law power. Moreover, it may be expecting much of an officer to distinguish between a search which engages the content of the accused's private communications and one which does not; which seeks to find out what an accused said to, or received from, another person and one which simply seeks to show whether he in fact communicated with that other person. We are not to be taken as saying that

---

[83] *R v Grayson and Taylor* [1997] 1 NZLR 399, at p.407.

the former will not be permitted in a search incidental to arrest, whereas the latter will be: much will depend on the circumstances. However, it will be easier to justify the search of an accused's mobile phone without a warrant when it does not involve a direct intrusion into the accused's private communications with others; but see the discussion on filtering the contents of a mobile phone in [201] and [206] below.

D5. Scope of the power of search incidental to arrest

152. We have referred to the common law power of search incidental to arrest as a power to procure, prevent and protect. The doctrine of exigent circumstances, whilst certainly concerned with two of those purposes, namely, preventing the imminent destruction of evidence and the protection of law enforcement officers and members of the public, exists separately from, and should not be confused with, the common law power. The Court in *Riley* certainly appreciated the difference between the two doctrines, explaining that[84]:

> "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."

153. With respect to the minority in *Fearon*, there seems to have been an eliding of the doctrine of search incidental to arrest with the doctrine of exigent circumstances, and a consequent assumption that the latter represents the common law. Certainly, that was how Au J interpreted the judgment of Karakatsanis J, on behalf of the minority in *Fearon*, for he held[85]:

---

[84] *Riley*, at [19].

[85] Judgment, at [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." *(Emphasis supplied)*

154. However, in our judgment, the common law power of search incidental to arrest is not coterminous with, nor dependent upon, exigent circumstances, although in many cases, particularly where evidence risks being lost or destroyed, a law enforcement officer will need to act fast. The purpose of procuring or gathering evidence, which we consider to be an equally important facet of the common law power, but not, it would seem, one justified by circumstances of exigency, may necessarily require a police officer to act prudently and promptly in circumstances which may not strictly be characterised as an emergency.

155. As Mr Pun acknowledged, the doctrine of exigent circumstances has not been applied in the United Kingdom. The precise point at which the doctrine first found articulation is not entirely clear. In 1993 in *Grant*, the Supreme Court of Canada held that "[s]ection 10 of the Narcotic Control Act ("NCA"), which authorizes a warrantless search of a place other than a dwelling-house where a peace officer has reasonable grounds to believe that it contains a narcotic by means of or in respect of which an offence under the NCA has been committed, should be read down to restrict its availability to situations in which exigent circumstances make it impracticable to obtain a warrant. Exigent circumstances will generally be held to exist if there is imminent danger of the loss, removal, destruction

or disappearance of the evidence if the search or seizure is delayed[86]". The Court in *Grant* referred [87] approvingly to a 1987 decision of the Saskatchewan Court of Appeal in *R v D (ID)* [88], where the Court had cited the doctrine of exigent circumstances as an exception to a pre-authorised search warrant, the authority for which was identified as the 1951 decision of *United States v Jeffers*[89].

156. In *Riley*, Roberts CJ referred[90] to the Court's earlier decision in *Kentucky v King*[91], which cited the 1978 judgment of the Court in *Mincey v Arizona*[92], where "the exigencies of the situation" were said to provide a well-recognised exception justifying a warrantless search. *United States v Jeffers* was also referred to in *Mincey v Arizona*[93].

157. It would seem therefore that the doctrine of "exigent circumstances" is of fairly recent origin, emerging in the second half of the twentieth century, initially in the United States, before crossing the border into Canada. However, the important statutory context in which these decisions should be viewed must be the Fourth Amendment in the United States, and section 8 of the Canadian Charter. The doctrine has not passed

---

[86] *R v Grant* [1993] 3 SCR 223, at p.224.

[87] *Ibid.*, at pp.241-243.

[88] *R v D (ID)* [1987] SJ No 653; 38 CCC (3d) 289.

[89] *United States v Jeffers* 96 L Ed 59 (1951).

[90] *Riley*, at [18].

[91] *Kentucky v King* 131 S Ct 1849 (2011).

[92] *Ibid.*, at p.460.

[93] *Mincey v Arizona* (1978) 437 US 385, at p.391.

into the jurisprudence of the United Kingdom nor, save in the instant case, been considered applicable in Hong Kong.

158. As we have explained at [92] to [97] above, under our common law, the power of search incidental to arrest entitles the police (or other law enforcement authority) to procure evidence of the crime committed, to prevent its destruction and to protect the officers of law enforcement and the public.

159. It is here that we should briefly deal with Mr Pun's argument that the common law power, as we have defined it, is displaced by the statutory scheme, in particular Section 50(6). We cannot accept this argument, which was not joined by either Mr Mok or Mr McCoy.

160. Section 50(6) is specifically directed at enabling a search by a police officer of, and in the vicinity of, an apprehended suspect, with the appropriate state of mind as to its connection with the investigation. It is concerned with procuring evidence only: it has nothing to do with preventing the loss or destruction of evidence; nor with protecting law enforcement officers or members of the public; nor with promoting the wider objectives behind the power identified by the majority in *Fearon*[94]. The common law power is accordingly directed at wider objectives in respect of all law enforcement officers than the statutory provision relating to searches by police officers.

[94] See [96] above.

161. At this juncture, it is opportune for us to address the power of a magistrate to issue a warrant to authorize the search of the digital contents of a mobile phone. Section 50(7) is in these terms:

> "Whenever it appears to a magistrate upon the oath of any person that there is reasonable cause to suspect that there is in any building, vessel (not being a ship of war or a ship having the status of a ship of war) or place any newspaper, book or other document, or any portion or extract therefrom, or any other article or chattel which is likely to be of value (whether by itself or together with anything else) to the investigation of any offence that has been committed, or that is reasonably suspected to have been committed or to be about to be committed or to be intended to be committed, such magistrate may by warrant directed to any police officer empower him with such assistants as may be necessary by day or by night—
>
> (a) to enter and if necessary to break into or forcibly enter such building, vessel or place and to search for and take possession of any such newspaper, book or other document or portion of or extract therefrom or any such other article or chattel which may be found therein; and
>
> (b) to detain, during such period as is reasonably required to permit such a search to be carried out, any person who may appear to have such newspaper, book or other document or portion thereof or extract therefrom or other article or chattel in his possession or under his control and who, if not so detained, might prejudice the purpose of the search."

162. Before us, it is common ground among all counsel that a magistrate has the power to issue such warrant. Since it is a matter of general importance and a necessary part in our analysis of the lawfulness of warrantless search, we have to satisfy ourselves that such common ground is correct in law.

163. Having considered the submissions and the authorities cited to us, we are able to adopt the view that a magistrate can issue a warrant under Section 50(7) to authorize a search of the digital contents of a mobile phone.

164. Whilst there is no building or vessel to be entered into, the digital world has been regarded as a separate place in Canadian jurisprudence in respect of search and warrant. In *R v Vu*, Cromwell J held at [51] that when the contents of a computer and a mobile phone are searched, it should be treated as a separate place and for that reason a specific warrant should be obtained. The decision was followed by Hughes J in the Court of Queen's Bench of Alberta in the case of *R v KZ*[95]. The learned judge held at [32] that a warrant could be issued for the search of a computer on the basis that it was a "place" where there are reasonable grounds to believe evidence may be found.

165. We also agree with counsel that to give the Section 50(7) power a purposeful construction in respect of a search of a mobile phone as a place, the electronic data or files contained in it can be regarded as "documents" or a portion thereof or an extract therefrom.

166. Accordingly, a magistrate can issue a warrant for the search of a mobile phone or other electronic devices if the other requirements in Section 50(7) are satisfied.

D6. Personal Data (Privacy) Ordinance

167. PDPO contains provisions protecting the privacy of individuals in relation to personal data. It sets out some data protection principles which a data user has to follow. The principles (as stated in Schedule 1 to PDPO) govern the collection, accuracy and duration of retention, use, security, information on and access to personal data. Mr Mok submitted

[95] *R v KZ* (2014) ABQB 235.

that PDPO is part of the overall regime safeguarding the rights of privacy in relation to mobile phone searches, including mobile phone search incidental to arrest. In particular, counsel referred to the limited purposes for which data can be collected[96] and the limit on the duration for the retention of personal data[97].

168. Au J accepted the submission of Mr Pun that the reliance on PDPO is misplaced[98] because, firstly, a search without collecting the information does not come within the scope of PDPO. Further, plenty of information stored in a mobile phone does not satisfy the three conjunctive requirements of attribution, identification and retrievability in section 2 of PDPO, and therefore is not protected by the data protection principles.

169. Before us, counsel only reproduced the written submissions placed before Au J. With respect, the assistance we received from counsel is inadequate for us to reach a concluded view on the applicability of PDPO.

170. We have difficulty with a general proposition that the search of the contents of a mobile phone *per se* would not involve collection or use of data. A cursory search without examining at length the contents may not come within the scope of PDPO. However, if a police officer actually finds something which may be relevant to crime detection or crime prevention and

---

[96] Principle 1(1) in Schedule 1 provides that personal data shall not be collected unless it is collected for a lawful purpose directly related to a function or activity of the data user, the collection is necessary for or directly related to that purpose and the data is adequate but not excessive in relation to that purpose.

[97] Principle 2(2) provides that all practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose for which the data is or is to be used. See also section 26 of PDPO.

[98] Judgment, at [71].

studies and uses the subject data for questioning an arrested person, the data is collected and used by the police officer.

171. Though there is undoubtedly information in the mobile phone which is not personal data, there is also information which is personal data. Personal data is defined in section 2 of PDPO as follows:

> " ***personal data*** … means any data—
>
> (a) relating directly or indirectly to a living individual;
>
> (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
>
> (c) in a form in which access to or processing of the data is practicable."

172. In the recent case of *TLT v Home Secretary*[99], in the context of the Data Protection Act 1998 which contains a concept of personal data[100] similar to PDPO, the English Court of Appeal alluded to the approach that one should take account of all the means likely to be used by any third party to identify a data subject in determining if a data subject is identified or identifiable in a particular setting[101]. It also rejected the submission that a

---

[99] *TLT v Home Secretary* [2018] 4 WLR 101.

[100] Under section 1 of the Data Protection Act, there are two limbs for identification: direct and indirect, see *Vidal-Hall v Google Inc* [2016] QB 1003 at [108] and [109]. The latter being identification from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller. PDPO refers to direct and indirect relating to and identification of individual.

[101] See [38] in *TLT v Home Secretary*, based on European Parliament and Council Directive 95/46/EC recital (26) cited at [19].

narrow meaning should be given to the words "relate to"[102] in a context similar to limb (a) in our definition of personal data.

173. Bearing in mind the purposes for which a police officer would collect and use the data in a mobile phone seized upon arrest, it is likely that the data in which the police would be interested would relate to the arrested person or his associates.

174. For example, if the police find a photograph of a crime scene without showing any person on it in a search of a mobile phone, the significance can rest upon the fact that the photograph is found in the phone of the arrested person. Looking at the matter from such angle, the data is not the photograph alone but also the photograph plus the fact that it appears in the phone (or other information that can be retrieved like the date and time of the taking of the photograph). The definitions of "data" and "document" in section 2 of PDPO are arguably wide enough to embrace the composite representation of information in a phone. Viewed thus, the data retrieved includes the photograph as well as other information derived from its storage in the phone and it is related to the arrested person as owner of the phone. Element (a) in the definition can therefore be satisfied.

175. Element (b) can also be resolved if one can adopt the approach of composite representation of information in the data stored in a phone as discussed above. The ascertainment of the identity of the individual

---

[102] See [39] to [43] of *TLT v Home Secretary*, supra. The narrower interpretation in the earlier case of *Durant v Financial Services Authority* [2003] EWCA Civ 1746 was subject to criticism from the European Commission, discussed at §4-10 of *Data Protection Law and Practice* 4th Edn by Rosemary Jay.

directly or indirectly is achieved by regarding the phone as a personal identifier (as defined under section 2 of PDPO).

176. Similar analysis can be applied in respect of WhatsApp or other social media communications between the owner of the phone and some third parties.

177. Whether or not a particular piece of data relates to a particular individual is ultimately a question of fact. Obviously, much depends on the ownership of the phone, the nature of the information retrieved and the surrounding circumstances in which the information came to be stored in the phone.

178. Whilst section 58 of PDPO contains exemptions in respect of personal data held for the purposes of the prevention or detection of crime and the apprehension, prosecution or detention of offenders, the exemptions are limited in scope and duration. Under section 58(1), the exemption is only in respect of the provisions of data protection principle 6 (concerning access to personal data) and section 18(1)(b) (concerning data access request). Under section 58 (2), the exemption is only in respect of the provisions of data protection principle 3 (concerning the use of personal data for a new purpose). These exemptions are only applicable when the application of those provisions would be likely to prejudice such objectives.

179. As we have mentioned, counsel did not make any in-depth submissions on PDPO before us at the hearing of the appeal. The English cases referred to above were not cited and the argument on composite representation was not explored. In the circumstances, whilst we respectfully disagree with Au J in ruling out altogether the operation of

PDPO in the context of mobile phone search, it is not desirable for us to express any final view on the applicability of PDPO without adequate submissions and in an abstract setting.

180. It is also unnecessary for us to determine in the context of the present appeal the extent of the applicability of PDPO in respect of a search of the contents of a mobile phone. We do not find it helpful to analyse the extent to which the provisions in PDPO give similar safeguards[103] as those laid down in the majority judgment in *Fearon* since we shall not decide this appeal by choosing between the different approaches in North America. As discussed below, we shall develop the common law in Hong Kong and provide adequate safeguards in a warrantless search. With such safeguards in place a fair balance is struck with due regard to the right of privacy protected under BL 30 and BOR 14 in accordance with the proportionality analysis. These common law safeguards are in place without any need to show that the data in question comes within the scope of PDPO.

181. At the same time, these safeguards are provided without prejudice to the rights of a data subject from pursuing his complaint and seeking remedies under PDPO if he is of the view that in his particular case his personal data is taken or used and there is a breach of the data protection principles. In particular, he may lodge a complaint with the Privacy Commissioner for Personal Data under Part 7 of PDPO or seek compensation in the District Court under section 66 of PDPO.

---

[103] As set out in the written submissions placed before Au J, this was the approach advocated on behalf of the Respondent in the court below.

D7. Proportionality analysis

182. At Section D1 above, we have alluded to the proportionality analysis and in the context of mobile phone search adopted the approach in *Keen Lloyd* as supplemented by the fourth step discussed in *Hysan*. We shall now explain our formulation of a common law regime in Hong Kong for mobile phone searches and how it fits within the proportionality analysis. It is accepted by all counsel before us that for law enforcement purposes, it is necessary for the police to have the power to conduct a warrantless search of the contents of the mobile phone of an arrested person under certain circumstances. The disagreements are on the precise limits of those circumstances and the safeguards that should be in place.

183. As stated above, though Mr Mok invited us to adopt the majority approach in *Fearon* and Mr Pun supported the judge's adoption of the minority approach in that case, we are of the view that Mr McCoy is correct in his submission that the common law in Hong Kong on mobile phone search upon arrest should develop by reference to the concept of reasonable practicability in which due regard is paid to the proportionality requirement in terms of intrusion into privacy interest by a search for law enforcement purposes.

184. In other words, a police officer cannot search the contents of a mobile phone of an arrested person without warrant unless it is not reasonably practicable to obtain a warrant under Section 50(7) before doing so.

185. The striking of the balance at this point, with the further safeguards discussed below, is in line with our law on the power of search

and seizure in other instances as provided in various statutes and the general discussion of such power in our case law. Given the potentially great privacy interest and volume of data stored in a mobile phone, we agree with the submissions of Mr Pun and Mr McCoy that the privacy interest engaged in such a search is potentially higher than a search conducted of private premises. Thus, there should be further safeguards as discussed below.

186. As the power is to be exercised as a power incidental to arrest, it is relevant to bear in mind the following preconditions for the exercise of the power. First, the police must have a reasonable suspicion that the person arrested (and subject to the search) has committed an offence.

187. Second, the scope and purpose of the search must be truly incidental to the arrest in question. In other words, the police officer must have a reasonable basis for having to conduct the search immediately as being necessary (1) for the investigation of offence(s) for which the person was suspected to be involved, including the procurement and preservation of information or evidence connected with such offences; or (2) for the protection of the safety of persons (including the victim(s) of the crime, members of the public in the vicinity, the arrested person and the police officers at the scene).

188. Further, whilst a police officer would need to access the phone generally for cursory filtering examination, he should limit the scope of the detail examination of its digital contents to relevant items by reference to the criteria in the preceding paragraph.

189. In this connection, in light of the legitimate law enforcement objectives served by such a search, we reject the submission of Mr Pun that

the purpose of search should not include discovery of information or evidence. We do not see any reason why the procurement of information or evidence connected with the offence(s) for which the arrested person was suspected to be involved should be excluded from those objectives. The scope of English common law search incidental to arrest as discussed above embraced such an objective.

190. The same appears to be the case in Canada, see *Fearon* at [80] and [121]; *R v Caslake* at [19]; and *Cloutier v Langlois*[104] at p.175 to p.183. In the latter case, at p.182 and p.183, L'Heureux-Dubě J explained the rationale for power of search incidental to arrest as follows:

> "Our system of criminal justice is based on the punishment of conduct that is contrary to the fundamental values of society …The system depends for its legitimacy on the safe and effective performance of this function by the police. In the context of an arrest, these requirements entail at least two primary considerations. First, the process of arrest must be capable of ensuring that those arrested will come before the court. An individual who is arrested should not be able to evade the police before he is released in accordance with the rules of criminal procedure, otherwise the administration of justice will be brought into disrepute. In light of this consideration, a search of the accused for weapons or other dangerous articles is necessary as an elementary precaution to preclude the possibility of their use against the police, the nearby public or the accused himself…Further, the process of arrest must ensure that evidence found on the accused and in his immediate surroundings is preserved. The effectiveness of the system depends in part on the ability of peace officers to collect evidence that can be used in establishing the guilt of a suspect beyond a reasonable doubt. The legitimacy of the justice system would be but a mere illusion of the person arrested were allowed to destroy evidence in his possession at the time of the arrest."

[104] *Cloutier v Langlois* [1990] 1 RCS 158.

191. In *R v Caslake*, Lamer CJ related the limits on the search to the justification for the power at [17] and summarized the law as follows at [19] and [20]:

> "[17] In my view, all of the limits on search incident to arrest are derived from the justification for the common law power itself: searches which derive their legal authority from the fact of arrest must be truly incidental to the arrest in question. The authority for the search does not arise as a result of a reduced expectation of privacy of the arrested individual. Rather, it arises out of a need for the law enforcement authorities to gain control of things or information which outweighs the individual's interest in privacy… This means, simply put, that the search is only justifiable if the purpose of the search is related to the purpose of the arrest.
>
> …
>
> [19] As L'Heureux-Dubě J stated in *Cloutier*, the three main purposes of search incident to arrest are ensuring the safety of the police and public, the protection of evidence from destruction at the hands of the arrestee or others, and the discovery of evidence which can be used at the arrestee's trial. The restriction that the search must be 'truly incidental' to the arrest means that the police must be attempting to achieve some valid purpose connected to the arrest. Whether such an objective exists will depend on what the police were looking for and why. There are both subjective and objective aspects to this issue. In my view, the police must have one of the purposes for a valid search incident to arrest in mind when the search is conducted. Further, the officer's belief that this purpose will be served by the search must be a reasonable one.
>
> [20] To be clear, this is not a standard of reasonable and probable grounds, the normal threshold that must be surpassed before a search can be conducted. Here, the only requirement is that there be some reasonable basis for doing what the police officer did. To give an example, a reasonable and probable grounds standard would require a police officer to demonstrate a reasonable belief that an arrested person was armed with a particular weapon before searching the person. By contrast, under the standard that applies here, the police would be entitled to search an arrested person for a weapon if under the circumstances it seemed reasonable to check whether the person might be armed. Obviously, there is significant difference in the two standards. The police have considerable leeway in the circumstances of an arrest which they do not have in other situations. At the same time, in keeping with the criteria in *Cloutier*, there must be a 'valid objective' served by the search. An objective cannot be valid if it is not reasonable to pursue it in the circumstances of the arrest."

192. Thus, with respect to Mr Pun, there is no reason why the discovery (or procuring) of evidence cannot be a legitimate objective for search. Further, the dictum of Lamer CJ explained the threshold of reasonable basis (which is lower than the normal standard of reasonable and probable grounds) for triggering the exercise of the power of search incidental to arrest.

193. We are of the view that these expositions on the concept and legitimate scope of a search incidental to arrest are equally apposite with regard to the similar power in Hong Kong. The standard of reasonable basis, as explained by Lamer CJ, is partly subjective and partly objective. Such a standard takes account of the circumstances under which the power will be exercised and the conundrum arising from the impossibility of having a "belief" on the part of a police officer on the utility of the search (as highlighted by Mr Mok in his submission that the test of Karakatsanis J is not workable) is resolved. At the same time, the objective element in the reasonable basis test serves as a protection to the arrested person against arbitrary intrusion of his privacy. Subject to the further safeguards explained below, we are of the view that the reasonable basis test strikes a fair balance and the intrusion on the privacy right, as explained below, by reference to that test in the context of search incidental to arrest can meet the proportionality requirement in Hong Kong.

194. The dictum of Lamer CJ also highlighted the fact that the justification for the intrusion does not lie in the lower expectation of privacy of an arrested person. Though there are general statements in some of the cases suggesting that an arrested person has a lower expectation of

privacy[105], it is also well established in Hong Kong that the fundamental rights of a person under lawful incarceration is protected and any incursion into such rights must meet the proportionality requirement[106]. In *McCann v State Hospitals Board* [2017] 4 All ER 449, Lord Hodge SCJ held at [51] that a person who is compulsorily detained enjoys all the civil rights which are not taken away expressly or by implication as a result of that detention. At [54], His Lordship applied the principle by testing if a restriction on a fundamental right (in that case the right to private life) is inherent in the loss of liberty occasioned by the detention.

195. In our judgment, the privacy interest of an arrested person (who is subject to lawful custody and detention by police upon arrest) must necessarily be subject to a lawful search which is truly incidental to the arrest as an incidence of his arrest and the investigation of the offence for which he was arrested. The right of privacy does not operate to shield incriminating evidence from legitimate criminal investigation process.

196. At the same time, his privacy interest in the digital data stored on his phone outside the proper and legitimate scope of such search must remain intact. The law must therefore protect him against the disproportionate intrusion into his privacy interest in such other data.

197. In the context of a search of the digital contents of mobile phone, it follows from the above discussion that the problem does not lie in

---

[105] *R v Beare* at 413; *Fearon* at [56]; *Riley* at 2488 [11]. A contrary view was expressed by Karakatsanis J in *Fearon* at [145].

[106] See *HKSAR v Wan Thomas* [2016] 5 HKLRD 656 (reversed on appeal on other grounds: (2018) 21 HKCFAR 214) and *HKSAR v Fong Kwok Shan* Christine (2017) 20 HKCFAR 425 at [52].

the lack of legitimate law enforcement objectives for such a search. The legitimate interests are those advanced by Mr Mok[107], which are similar to those discussed in the Canadian authorities cited above[108]. It is also plain that a search of the mobile phone for the relevant data and information is rationally connected with the advancement of such interests. Confining a warrantless search to situations where it would not be reasonably practicable to obtain a warrant before the search is a restriction to ensure that the intrusion is no more than is necessary to achieve legitimate interests.

198. Rather, the real problem stems from the potentially large amount of private and possibly sensitive data (which does not fall within the legitimate scope of search) stored in the phone alongside the information and data which fall within the legitimate scope of such search. Thus, there must be adequate safeguards to protect the arrested person against arbitrary and unlawful interference.

199. Hence, the restrictions as set out at [187] and [188] above should be imposed. Moreover, to provide a further safeguard by way of documentation of the purpose and scope of the warrantless search, a police officer should make an adequate written record of the same as soon as practicable after the performance of the search. A copy of the written record should be supplied forthwith to the arrested person unless doing so would jeopardize the ongoing process of criminal investigation.

200. We are of the view that the criteria at [187] and [188] are sufficiently clear and circumspect in terms of the scope of any warrantless

---

[107] See [37] to [39] above.

[108] *R v Caslake*; *Cloutier v Langlois*.

search and the safeguards at [199] are adequate. We note that Au J also referred to the same criteria as those at [187] as valid purposes for warrantless search though he framed the same by way of exigent circumstances[109].

201. Admittedly, since a police officer would have to conduct a cursory examination of the contents of a mobile phone in order to filter out materials outside the scope of relevant data and information, some minor intrusion on the privacy interest in the irrelevant materials is inevitable. However, such intrusion is inherent in any search of mobile phone, whether with or without warrant and irrespective of how the criteria for warrantless search is set. *Ex hypothesi* a search involves the differentiation of relevant information from irrelevant information. Even in the context of a search of private premises for physical (as opposed to electronic) evidence, a law enforcement officer would have to briefly go through items which have no relevance to the purpose of the search before disregarding the same. Thus, some intrusion of privacy arising from a cursory inspection cannot be avoided once it is accepted that the search of a mobile phone for evidence or information for the purpose of criminal investigation is legitimate.

202. Two further concerns were raised on permitting warrantless search by police officers: (1) a non-categorical exclusion of mobile phone search provides insufficient guidance to police; and (2) the police are not in the best position to determine whether the law enforcement objectives outweigh the intrusion on privacy in the search of a mobile phone. It is

[109] See Judgment, at [56].

further said that after-the-fact review and relief does not provide an adequate remedy.

203. With respect, if these concerns were taken to their highest, they would rule out the possibility of warrantless mobile phone search altogether. In the context of the debate in Canada, the approach of Karakatsanis J also involves the assessment by the police on whether a situation comes within exigent circumstances. Like the intrusion by way of a cursory search, the empowerment of the police to conduct some form of mobile phone search without warrant must entail some exercise of judgment by the police officer conducting the search.

204. As we have discussed, the test we propose to adopt in Hong Kong, reasonable practicality, is a concept familiar to our law enforcement officers and has been applied consistently. As the formulation based on reasonable practicability was not advanced at the court below, this is a factor which Au J did not address. As regards the limit of a cursory search, with the above guidance on the limited purposes for search which are truly incidental to arrest, plus the safeguards discussed at [199] to facilitate an effective judicial review on the search, we are of the view that the overall protection is adequate and effective.

205. For the purpose of examining the adequacy and effectiveness of safeguards as part of the proportionality analysis[110], the adequacy of an after-the-fact review should be weighed more in terms of its impact on preventing abuse than its adequacy in providing relief (though the latter is also relevant). The European jurisprudence does embrace the possibility of such review as

[110] See [102] to [104] above.

an adequate and effective safeguard. Again, Au J did not have the benefit of the citations of the relevant European authorities and arguments in this respect when he held that after-the-fact review does not provide adequate redress.

206. In light of our analysis above, the intrusion into the privacy interest in a warrantless mobile phone search will be conducted within the bounds of a search truly incidental to arrest when it is not reasonably practicable to do so after a warrant is obtained. Its intrusion into data and information which are not relevant to the legitimate purpose of a search incidental to arrest would be mitigated by the necessary safeguards to ensure such intrusion is confined to cursory inspection for filtering purposes and the scope of the detail search is documented by contemporaneous record. Such search could be subject to effective supervision by way of after-the-event judicial review. As such, there would be adequate and effective safeguards against abuse and the permissible warrantless search would not be more than necessary for the legitimate law enforcement objectives incidental to the arrest.

207. As held by the Court of Final Appeal in *Hysan*, the fourth step of the proportionality test requires the court to consider the deleterious effects of a measure on the individual concerned. Ribeiro PJ explained the need to include the fourth limb at [78] of *Hysan* as follows:

> "…Without its inclusion, the proportionality assessment would be confined to gauging the incursion in relation to its aim. The balancing of societal and individual interests against each other which lies at the heart of any system for the protection of human rights would not be addressed. This requires the Court to make a value judgment as to whether the impugned law or governmental decision, despite having satisfied the first three requirements, operates on particular individuals with such oppressive unfairness

> that it cannot be regarded as a proportionate means of achieving the legitimate aim in question…"

208. At [135], the fourth step was expressed in this way:

> "…where an encroaching measure has passed the three-step test, the analysis should incorporate a fourth step asking whether a reasonable balance has been struck between the societal benefits of the encroachment and the inroads made into the constitutionally protected rights of the individual, asking in particular whether pursuit of the societal interest results in an unacceptably harsh burden on the individual."

209. The fourth step can be applied at two different levels. First, one can assess generally the common deleterious effects of a mobile phone search by reference to a notional search against a person arrested for an unspecified offence. On such a level of generality, the fourth step adds little to what has already been considered in the first three steps in the striking of a fair balance between the societal benefit derived from permitting a warrantless search within the limitations and the intrusion into the privacy interest of the arrested person. We have already alluded to such privacy interest in general and how it is to be weighed against the legitimate law enforcement objectives to be served by a warrantless search incidental to an arrest.

210. Second, the fourth step can be applied on the specific facts and circumstances of the case at hand. At that level, the court will have to examine the specific offence for which the person is arrested and the underlying facts pertaining to the criminal investigation, the specific pieces of digital data and information that have been searched and the specific actions taken by the law enforcement officer(s) to mitigate the invasion of privacy and the safeguards put in place to assure the arrested person that there is no abuse.

211. In the context of the present appeal, by reason of the absence of any actual search of the contents of the mobile phones on the factual matrix of the case (thus no finding on the manner and scope of search if one were executed and the relevance of the results of such search to the criminal investigation against the arrested persons as well as the extent of the invasion against their privacy), it is not possible for us to assess the severity and consequences of the interference on the individuals concerned had there been searches of the digital contents of the phones.

212. Further, the appeal has been argued before us on a general level without much debate on the specifics.

213. Thus, it is not profitable for us to consider the application of the fourth step in a specific context in this judgment.

214. However, there is one aspect relevant to this topic we can usefully mention. Mr McCoy submitted that there should be built into the test for warrantless search of mobile phone contents as a search incidental to arrest a criterion that such search should only be conducted in respect of dynamic and serious crimes. Whilst we agree that the seriousness of the offence in question would be relevant to the societal benefit to be weighed as part of the analysis under the fourth step, such analysis should not be geared towards the seriousness of the offence alone. There could be other factors relevant to the overall assessment in coming to a fair balance.

215. We do not think it is appropriate to add the fourth step to our guidance to the police on the common law power of search of a mobile phone incidental to arrest. As Ribeiro PJ emphasised at [130] of *Hysan*:

> "…It should be emphasised that it is the Court which has the ultimate responsibility for determining whether any restriction imposed by the Board can be subjected to a successful constitutional challenge. The Board's role is to carry out its duties and to exercise its powers in accordance with the TPO. To adapt what Lord Hoffmann said in *R (SB) v Governors of Denbigh High School*, members of the TPB cannot be expected to make the Board's planning decisions with textbooks on human rights law at their elbows. … it is not the Board's task to conduct a proportionality analysis, much less to mouth incantations about proportionality in rendering its decisions."

216. Likewise, in the exercise of the power of search incidental to arrest, a police officer must have regard to the common law constraints discussed above. At the same time, similar to the exercise of other law enforcement and criminal investigation power, a police officer must have regard to the specific circumstances in the case at hand to decide if it is appropriate to exercise the power. After the power has been exercised, it is a matter for the court to consider if the proportionality test, including the fourth step, has been satisfied if there is a legal challenge to the specific exercise of power.

217. We do not find it helpful or necessary for us to discuss in this judgment the provision for the destruction or return of the mobile phone or materials copied from it. In particular, we do not wish to pre-empt the course a party may take in the event of dispute whether under section 102 of the Criminal Procedure Ordinance or section 42 of the Magistrates Ordinance or a provision under PDPO or seeking relief under common law. There is no basis to suggest (and Mr Mok has made no suggestion) that the police would have a right to retain the phone or copied materials after the criminal investigation and criminal proceedings (if any) have been concluded.

218. In summary, we hold that the power to conduct a mobile phone search upon arrest can be exercised if:

(a) a warrant is obtained under Section 50(7); or

(b) when it is not reasonably practicable to obtain such warrant before a search is conducted, the police officer must also have a reasonable basis for having to conduct the search immediately as being necessary (i) for the investigation of the offence(s) for which the person was suspected to be involved, including the procurement and preservation of information or evidence connected with such offences; or (ii) for the protection of the safety of persons (including the victim(s) of the crime, members of the public in the vicinity, the arrested person and the police officers at the scene);

(c) for a warrantless search conducted under (b) above, other than a cursory examination for filtering purpose, the scope of the detail examination of the digital contents of a phone should be limited to items relevant to objectives set out in sub-paragraph (b);

(d) in addition, a police officer should make an adequate written record of the purpose and scope of the warrantless search as soon as reasonably practicable after the performance of the search and a copy of the written record should be supplied forthwith to the arrested person unless doing so would jeopardize the ongoing process of criminal investigation.

219. Whilst the exercise of such power would interfere with the interest of an arrested person under BL 30 and BOR 14, we also hold that the conferment of such power to the police is proportionate. As regards the specific exercise of the power on a particular occasion, it is not a matter we can determine in this judgment without the necessary factual matrix before us.

E. Dispositions

220. For the above reasons, we would allow the appeal and set aside the declaration granted by Au J and grant instead a declaration that a police officer can conduct a search of the digital contents of a mobile phone found on an arrested person in accordance with the conditions set out at [218] above and the power is compatible with BL 30 and BOR 14.

221. Instead of making a costs order nisi, we shall invite written submissions on costs as follows:

(a) the Commissioner shall lodge and serve submissions on costs within 14 days from the handing down of the judgment;

(b) the other parties shall lodge and serve submissions on costs within 14 days thereafter;

(c) the Commissioner shall lodge and serve submissions in reply within 14 days after the submissions of the other parties.

222. Last but not least, we wish to express our gratitude to all counsel for their thorough research and able assistance.

(Jeremy Poon) Chief Judge of the High Court	(Johnson Lam) Vice President	(Andrew Macrae) Vice President

Mr Hectar Pun SC leading Mr Anson Wong Yu Yat, instructed by JCC Cheung & Co., assigned by the Director of Legal Aid, for the applicant

Mr Johnny Mok SC leading Mr Jonathan Chang, instructed by the Department of Justice and Mr Derek Lau (Senior Public Prosecutor), of the Department of Justice, for the respondent

Mr Adrian Lo, instructed by Ho Tse Wai & Partners, on watching brief on a *pro bono* basis, for the 1st, 3rd and 4th interested parties

Mr Gerard McCoy SC leading Mr Albert NB Wong, instructed by Ho Tse Wai & Partners, assigned by the Director of Legal Aid, for the 2nd interest party