Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/Information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

1.1. *To search or not to search? Does the right to privacy prevent the police from seizing and searching mobile phones in Hong Kong?*

A protester who participated in the July 1 march this year has made headlines by filing an application for leave to apply for judicial review before the Court of First Instance in Hong Kong for breach of his right to privacy.[1] The breach relates to police officers searching mobile phones incidental to an arrest without a warrant. This, according to the application for leave, is unconstitutional and a breach of a person's right to privacy.

1.1.1. *Background*

On 4 July 2014, four protesters were arrested by the police in connection with an alleged offence that occurred during the July 1 protest in Hong Kong. Police officers seized and briefly inspected the mobile phones of the protesters without a warrant, on the basis that the mobile phones were required as part of their investigation to determine whether or the protesters had collaborated in the alleged offence.

On 3 October 2014, one of the protesters (the "**Applicant**") filed an application for leave to apply for judicial review before the Court of First Instance (the "**Judicial Review**"), seeking (amongst other things):

(a) a declaration that Section 50(6) of the Police Force Ordinance (Cap. 232) ("**PFO**") does not authorise police officers to search the contents of mobile phones seized on arrest;
(b) if it is found that Section 50(6) of the PFO does empower police officers to search the contents of mobile phones without a warrant, a declaration that such power is unconstitutional and inconsistent with Article 14 of the Hong Kong Bill of Rights and Article 30 of the Basic Law of Hong Kong;
(c) an order that the decision of the police officer to seize the mobile phones for the purpose of searching their contents be brought up and quashed; and
(d) an expedited hearing of the application.

This is the first case brought in Hong Kong based on an allegation of infringement of an individual's right to privacy under the Basic Law and the Bill of Rights.

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong. Tel.: +852 2843 2211.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.
URL: http://www.mayerbrown.com

[1] HCAL 122/2014.

http://dx.doi.org/10.1016/j.clsr.2014.12.004
0267-3649/

1.1.2. *Right to privacy*

Article 30 of the Basic Law and Article 14 of the Bill of Rights grants Hong Kong residents the right to freedom and privacy of communication, and to not be subjected to unlawful or arbitrary interference with his privacy or correspondence. The only exception is where the relevant authorities must inspect personal communications, in accordance with legal procedures, in order to meet the needs of public security or to investigate a criminal offence.

Under Section 50(6) of the PFO, the police are empowered to seize, without a warrant and during a person's arrest, any "newspaper, book or other document…or any other article or chattel" that is found on such person or in the place he is arrested. The Applicant argues that the correct interpretation of this Section does not include the right to search the contents of mobile phones seized on arrest. Even if Section 50(6) of the PFO is found to have granted this power to the police, the Applicant still maintains that without a warrant such exercise of power is unconstitutional and infringes the Applicant's fundamental right to privacy under the Basic Law and the Bill of Rights.

1.1.3. *Mobile phones*

The amount of information that can be stored and accessed on a mobile phone, especially a smartphone, is substantial and will inevitably contain personal data, e.g. email correspondence, instant messages, social networking content, photographs, Internet browsing history, location history and even credit card information where the mobile is used for, say, NFC payments. Mobile phones may even contain content that is subject to legal professional privilege. The modern mobile phone is essentially comparable to a computer. In fact, the Hong Kong courts have previously determined that a mobile phone should be treated as a computer due to the functions and level of information that can be stored on a mobile phone.[2]

Any review of the information stored in a mobile phone will therefore be highly intrusive, and will give the police access to a substantial amount of information, most of which is unlikely to be relevant to the investigation. As stated by the Applicant in his application for Judicial Review:

> *mobile phones are markedly different in nature from other documents, articles or chattels that may be found on an arrestee's person or in a place of arrest…searches of digital data stored on mobile phones cannot be treated as comparable with searches of physical items that may be found on an arrestee's person.*

The Applicant argued in his application for Judicial Review that whilst a police officer may seize a mobile phone upon a person's arrest in order to ensure the integrity of the data, the police officer should not be able to search the content of the phone without first obtaining a warrant – to allow otherwise would amount to a disproportionate interference with the person's right to privacy.

1.1.4. *Conflicting interests*

There is a clear conflict between a person's right to privacy versus a police officer's duty to investigate and prosecute offenders. The goal is to achieve a balance, which is in the best interests of the public.

Whilst it may be argued that the police can simply secure a mobile phone in order to protect its contents from being erased, and to then obtain a warrant in order to review the information stored on it, the latest developments in technology mean that offenders can remotely wipe the data on their mobile phones whilst they are in police custody. There is therefore a risk that key evidence may be deleted before the police have a chance to discover it. One way to overcome this is for the police to place the mobile device in a radio-frequency shielded bag to prevent the data from being compromised, rather than in a microwave, which apparently is also an effective means of blocking any attempts to remotely erase its contents.

On the other hand, the risk associated with providing the police with unrestricted access to an arrestee's mobile phone is illustrated in a currently ongoing U.S. case where an individual has brought an action against the U.S. government for creating a Facebook page containing photographs of her obtained from her mobile phone. The U.S. Department of Justice had arrested the plaintiff in July 2010 in relation to a drug charge. At the time of her arrest, she had surrendered her mobile phone and consented to the police officers accessing its content in order to assist in a related criminal investigation. As part of this investigation, the police created a fake Facebook page in the name of the plaintiff, and included photos of her, her son and her niece. The plaintiff is therefore suing the U.S. government for breach of her right to privacy. The U.S. government argue that the plaintiff had "relinquished any expectation of privacy she may have had to the photographs on her cell phone" when she agreed to let police officers search and use information on the device.[3]

1.1.5. *Other jurisdictions*

The question of a person's right to privacy versus a police officer's right to conduct a warrantless search has also been considered in other common law jurisdictions. For example, in Canada and the U.S. the courts currently appear to take the view that searching an individual's mobile phone upon their arrest without first obtaining a warrant, will in certain circumstances violate the individual's right to privacy against unreasonable searches and seizures.[4] In particular, it was recognised by the Canadian courts that due to the quantity and quality of personal data that may be contained in a mobile phone, any search conducted by the police of the entire content of a phone would be highly invasive and should therefore not be conducted without a warrant.[5]

---

[2] See Secretary for Justice v Wong Ka Yip Ken (HCMA 77/2013) and our previous article entitled "How Smart is a Smartphone and How about its User?": http://www.mayerbrown.com/files/Publication/8eb13951-767e-47cf-ae1d-5f7e713d8958/Presentation/PublicationAttachment/8d26ced7-6527-4470-8a78-711e3e60818c/IP-%26-TMT-Quarterly%20Review_Q42013.pdf.

[3] Sondra Arquiett v. United States of America et al (Civil Action No. 13-CV-0752 (TJM/TWD)).

[4] Riley v. California, 573 US (2014); R v. Mann, 2014 BCCA 231.

[5] R v. Mann, 2014 BCCA 231. However, although the court found that Canadian law does not allow police to conduct a warrantless search of the entire contents of a person's mobile phone, the admission of the evidence obtained from searching the phone would not bring the administration of justice into disrepute and so the evidence was not excluded.