CAN POLICE SEARCH MOBILE PHONES WITHOUT A WARRANT?

A CHANGING DYNAMIC

PREPARED FOR THE CLANT CONFERENCE, BALI
THURSDAY 29 JUNE 2019
RORY PETTIT, TRIAL ADVOCATE, ABORIGINAL LEGAL SERVICE

PARTS

I. Case summary

II. Warrantless searches: *LEPRA* and the *PAA*

III. Relevant case law (*Riley v California* & co)

IV. Do police need a warrant?

1. CASE SUMMARY

Newcastle, March 2019

- Arrest warrant executed at apartment
- Drugs found (12g MDMA)
- Mobile phone taken from bed at the apartment
- Facebook messages accessed at police station
- Phone contents later downloaded using Cellebrite program
- Incriminating messages found
- Defendant charged with deemed Supply

EVIDENCE – VOIR DIRE

- Two witnesses:

1. Arresting police officer

- No request for passcode – ‘guessed it’
- Accessed FB messages while phone online, took screenshots

2. Officer who downloaded phone

- Contents downloaded
- Large part of role in police officer – phone downloads
- Internal process required for download

- Section 138, Evidence Acts
- Invoked when asserted police have obtained evidence improperly/illegally
- Discretion to exclude – competing public policies

➔Here: what was the asserted illegality or impropriety?

➔Effectively: not permitted under police powers relied upon

II. WARANTLESS SEARCHES

LEPRA – SECTION 27

Power to carry out search on arrest

(1) A police officer who arrests a person for an offence or under a warrant, or who is present at the arrest, may search the person at or after the time of arrest, if the officer suspects on reasonable grounds that it is prudent to do so in order to ascertain whether the person is carrying anything:

(a) that would present a danger to a person, or

(b) that could be used to assist a person to escape from lawful custody, or

(c) that is a thing with respect to which an offence has been committed, or

(d) that is a thing that will provide evidence of the commission of an offence, or

(e) that was used, or is intended to be used, in or in connection with the commission of an offence.

LEPRA – SECTION 30

Searches generally

In conducting the search of a person, a police officer may:

(a) quickly run his or her hands over the person's outer clothing, and

(b) require the person to remove his or her coat or jacket or similar article of clothing and any gloves, shoes, socks and hat (but not, except in the case of a strip search, all of the person's clothes), and

(c) examine anything in the possession of the person, and

(d) pass an electronic metal detection device over or in close proximity to the person's outer clothing or anything removed from the person, and

(e) do any other thing authorised by this Act for the purposes of the search.

POLICE ADMINISTRATION ACT (NT)

144 – Search of persons in lawful custody

A member of the Police Force may search a person in lawful custody, including the clothing the person is wearing and any property in the person's immediate possession, and may use the force that is reasonably necessary to conduct the search.

TWO QUESTIONS

1) Should a conceptual distinction be drawn between searches of mobile phones and searches of other items typically found during a search by police?
2) Should this conceptual distinction apply when considering the legality of such searches in NSW (or the NT)?

III. RELEVANT CASE LAW

1) SHOULD A CONCEPTUAL DISTINCTION BE DRAWN?

RILEY V CALIFORNIA 134 S. Ct. 2473 (2014)

- Appellant arrested on weapons charges – mobile phone taken during a search upon arrest: gang-related photos, videos discovered
- Relied upon to later to convict him of attempted murder, other offences
- Appeal challenged the admissibility of evidence obtained in consequence of the mobile phone search
- Asserted violation of 4th Amendment to the US Constitution
- Held: search was unconstitutional – such searches require warrants

1) QUANTITATIVE AND QUALITATIVE DIFFERENCE

The United States [respondent] asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette packet, a wallet, or a purse. […[]

Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

2) VASTNESS OF STORAGE, COLLATION OF DATA

[A] cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr Jones; he would not carry a record of all his communications with Mr Jones for the past several months, as would routinely be kept on a phone.

3) UBIQUITOUS PRESENCE IN MODERN LIFE

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.

4) *LOCATION DATA*

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different.

Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

5) MORE LIKE SEARCHING A HOUSE (OR WORSE)

In 1926, Learned Hand observed (in an opinion later quoted in Chimel) that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him.' If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form – unless the phone is.

6) DATA NOT STORED 'ON' THE PHONE

To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. […] The [respondent] United States concedes that the search incident arrest exception may not be stretched to cover a search of files accessed remotely – that is a search of files stored in the cloud.

Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house.

FEARON V THE QUEEN [2014] 3 R.C.S

- Canadian case – considered the same issue in the context of the Canadian Charter of Rights and Freedoms
- Specifically section 8: *Everyone has the right to be secure against unreasonable search or seizure.*
- Split decision – 4:3 in favour of allowing police to search mobile phones without a warrant incident to arrest
- 3 Judges in dissent: agreed with the position in *Riley*
- Majority nonetheless set down four strict conditions

FEARON V THE QUEEN [2014] 3 R.C.S

Ultimately, the purpose of the exercise is to strike a balance that gives due weight to the important law enforcement objectives served by searches incidental to arrest and to the very significant privacy interests at stake in cell phone searches. Consequently, four conditions must be met in order for the search of a cell phone or similar device incidental to arrest to comply with s. 8. First, the arrest must be lawful. Second, the search must be truly incidental to the arrest. […] Third, the nature and the extent of the search must be tailored to its purpose. […]Finally, the police must take detailed notes of what they have examined on the device and how they examined it.

AUSTRALIAN CASES

MCELROY; WALLACE V THE QUEEN [2018] VSCA 126

- Police entered a house to execute a search warrant of appellant's house, found associate of appellant's phone – searched it without warrant
- Challenge thereafter to admissibility of seizure and search of the phone under s 138 of the *Evidence Act* (*Vic*).
- VSCA granted leave to appeal, but dismissed the appeal because evidence insufficient to consider the question
- Left door open to consider *Riley* principles in future cases

MCELROY; WALLACE V THE QUEEN [2018] VSCA 126

Relying upon *Riley v California,* Wallace also contended that the power to search as an incident of arrest does not extend to a search of the contents of a modern mobile phone.

It should be observed at the outset that no evidence was led at trial with respect to most, if not all, of the issues that are raised in the second proposed ground of appeal.. […] What type of content can be stored on the Aziz phone? What type of content can be accessed using the Aziz phone? How does an application on the Aziz phone operate? […]

The lack of such evidence also makes it difficult to consider meaningfully whether the observations in *Riley v California* have any application in the present case. The technical issues in that case, some of which are relevant to the present case, were canvassed in written briefs filed with the Supreme Court.

R V JAUZDEMS [2014] QSC 74

- Recognised distinction between material held ‘on’ phone and ‘online’:

The second order sought, that the evidence of Facebook messages displayed on the Blackberry found in the search should be excluded, remains for consideration. As was observed in argument, determination of that limb of the application likely turns upon whether the messages were stored in the phone or whether the phone was used by police to access the internet and download the applicant’s messages to the phone. That distinction is of significance because s 31 [of the *PPRA*] only empowers a search of ‘a vehicle and anything in it’. It does not empower police to use the vehicle or anything found in it to search something or somewhere else.

2) CONCEPTUAL DISTINCTION IN AUSTRALIA?

- Come back to 'examine anything in possession of a person' under s 30, *LEPRA*
- Questions of statutory interpretation:

a) Should we assume that the drafters of *LEPRA* in 2002 foresaw the way in which mobile phones developed in subsequent years?

b) If not, should legislation be interpreted to allow that phrase to justify the wholesale download of mobile phones just because a person is carrying one when they're arrested?

➔ Complicated legal question

PRINCIPLE OF LEGALITY

In the absence of clear, unmistakable and unambiguous language to the contrary, the principle of legality precludes the adoption of a broad interpretation of a statutory expression that would abrogate, or abrogate further, from a fundamental right or privilege.

➔Common law right to privacy?

➔Common law right (or privilege against) self-incrimination?

By adopting broad interpretation of legislation, do we offend the principle of legality?

In matter from earlier: determined in broad way

LUPPINO V FISHER [2018] FCA 2106

- Federal Court decision – plaintiff, challenged validity of Magistrate's order to provide passcode to mobile phone to police
- Order ruled to be invalidly made it infringed the right against self-incrimination
- Not because of material on the *phone* but because it would require the acknowledgement (by affidavit) that he had previously lied to the police when he said he didn't know the passwords
- Would that apply material contained on the phone? Unclear

IV. DO POLICE NEED A WARRANT?

- In NSW, methods exist under which police can apply for a warrant to access information on a mobile phone – same likely in the NT
- Question is whether police powers legislation allows them to access phones after personal searches
- 2nd reading speech to *LEPRA*, 2002:

This Parliament, as representatives of the community, and the Courts have over time given police certain powers required to fulfil their role in law enforcement effectively. In return for these powers, however, police are required to exercise them responsibly, particularly where these powers affect the civil liberties of members of the community whom police serve.

CONCLUDING THOUGHTS

- Should a conceptual distinction be drawn between mobile phones and other items ordinarily found on personal searches? Should material stored online be excluded?
- In other words: will Australia follow the international trends?
- And if yes: how do we interpret warrantless search powers as a result? Unresolved
- Case law provides little guidance so far – remains a crucial and unresolved question