EXAMINING THE LEGITIMACY OF POLICE POWERS TO SEARCH PORTABLE ELECTRONIC DEVICES IN QUEENSLAND

MATTHEW RAJ* AND RUSS MARSHALL+

Mobile phones are more than just telephonic devices; they have the capability to store, retrieve and access potentially endless meta-data, including the personal information of an individual and his or her associates. In a landmark decision of 2014, the United States Supreme Court unanimously deemed unconstitutional the warrantless search and seizure of the digital contents of a mobile phone during an arrest. Five years on, in Queensland, the warrantless search by the police of a detained person's mobile phone can be considered standard investigative procedure. This article examines the legitimacy of existing Queensland police powers to conduct a physical search of a detained person's mobile phone. The core argument advanced is that, on a spectrum of property capable of being searched, a mobile phone should be considered more akin to a person's private home than their handbag or wallet. The article highlights the hazards of police searches of mobile phones that are conducted in the absence of an adequate framework of legal control and judicial oversight, and it recommends greater legal safeguards to govern existing police powers to search mobile phones.

I INTRODUCTION

> Modern cell [mobile] phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many [people] "the privacies of life" ... The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[1]

Consider the following scenarios:

1. A police officer stops you on the street and asks you to empty your pockets.

* Assistant Professor, Faculty of Law, Bond University. The authors are grateful to the anonymous peer reviewers for their comments on this article in draft. Author email: mraj@bond.edu.au

+ Semester Teaching Fellow, Faculty of Law, Bond University.

1 *Riley v California*, 573 US 373; 134 S Ct 2473, 2494–5 (2014) ('*Riley*') (Roberts CJ). The pinpoints herein are to the Supreme Court Reporter report of the case.

2. A police officer stops you in your car and asks to search you and the vehicle.

Regardless of the time of day, the location, your relationship status on Facebook, or the size of your bank account, one of the items recovered in either of the above scenarios will almost inevitably be a mobile phone. In what circumstances can the police search your mobile phone? Must they first obtain a search warrant? What will happen if you refuse to provide your passcode or fingerprint required to access your mobile phone data?

This article examines the existing legislative framework for the lawful search, by the Queensland Police Service, of a person's mobile phone. While the term 'mobile phone' appears throughout this article, this is intended to include all forms of portable electronic storage device that may be used to communicate with another (eg an iPad). It is argued that, given the wealth of information accessible from a mobile phone, the proper legal approach to categorising mobile phones is to treat them as 'homes' and not as 'containers'; that is to say, a mobile phone is more like a person's home than his or her handbag. By considering mobile phones to be more akin to homes, a police officer's power to search them will be constrained accordingly. This approach marks an important shift in the current approach to how mobile phones are treated by law enforcement, and it will help to protect individual privacy and prevent indolent policing.

What follows is an overview of the relationship between mobile phones, privacy and the law, which includes a brief comparative analysis of domestic and international law. The article then sets out the current laws governing the police search of a mobile phone in Queensland, while highlighting the impact (and desirability) of broad police search powers in this area. By way of conclusion, several recommendations are made to safeguard individual privacy and maintain public confidence in policing methods.

II Phones, Privacy and the Law

Since the first Australian mobile phone call at 10:42am on 23 February 1987, society has witnessed a 'quantum shift in mobile phone technology'.[2] There are now more mobile phone service subscribers in Australia than there are people.[3] In

---

[2] Australian Mobile Telecommunications Association, 'Mobile Telecommunications come of age in Australia' <http://www.amta.org.au/articles/amta/Mobile.telecommunications.come.of.age.in.Australia>.

[3] As at 29 June 2019, the population of Australia was reported to be 25.394 million <https://www.abs.gov.au/AUSSTATS/abs@.nsf/Web+Pages/Population+Clock?opendocument&ref=HPKI>. As at June 2018, the number of mobile phone service subscribers is reported to be 34.89

Australia, 96 per cent of adults use a mobile phone and 83 per cent of all mobile phone service subscribers use a smart phone (a phone incorporating a mobile internet service subscription).[4] Not only can a modern mobile phone replace possessions like watches, cameras, books, televisions, maps, wallets and laptops, it can also act as a postal service, playground, tracking device, shopping mall, personal secretary, digital diary, filing cabinet, bank and portable office. Simply put, mobile phones are 'containers in a physical sense, homes in a virtual sense and vast warehouses in an informational sense'.[5] The mobile phone in your possession is capable of containing more information than a filing cabinet, and it can retain every file or piece of data it has accessed, including 'information that most users do not know about and cannot control'.[6]

The proliferation of such powerful devices must surely test existing laws and social norms. One area where the mobile phone is challenging the status quo is with respect to police search and seizure powers. As the United States Supreme Court recently observed in *Riley*:

> Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day … A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives — from the mundane to the intimate.[7]

This makes mobile phones target-rich instruments for gathering evidence. For many reasons, an unfettered legislative right conferred on a police service to search the contents of an individual's mobile phone is hazardous. Overseas, precedent has formed to suggest that the warrantless search of a mobile phone by police is too invasive. In *Riley*, a unanimous United States Supreme Court confirmed that, in the absence of a validly obtained warrant, the search and seizure of the digital contents of a mobile phone incidental to an arrest is unconstitutional; in particular, it offends the Fourth Amendment of the *United States Constitution* protecting unreasonable searches and seizures. Writing the Court's opinion, Roberts CJ described mobile phones as 'not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life".'[8] In this judgment, the United

---

million; see Australian Communications and Media Authority, *ACMA Communications Report 2017–18* (Commonwealth of Australia, 2019) 8.

4 Australian Communications and Media Authority (n 3) 15.

5 Orin Kerr, 'Searches and Seizures in a Digital World' (2005) 119 *Harvard Law Review* 531, 533.

6 Ibid 542.

7 *Riley* (n 1) 2490.

8 *Riley* (n 1) 2494–5.

States Supreme Court appears to have recognised that, in many ways, mobile phones are more like a home than a handbag.

In contrast, in *R v Fearon*,[9] a narrowly divided Supreme Court of Canada (4:3) ruled that the warrantless police search of a mobile phone incidental to an arrest is permitted, provided the search is directly related to the circumstances of the arrest. Cromwell J, writing for the majority, rejected the so-called 'blanket exclusion' adopted by the United States Supreme Court in *Riley*. His Honour noted that while mobile phone searches 'have the potential to be a significant invasion of privacy, they are neither *inevitably* a major invasion of privacy nor *inherently* degrading. Looking at a few recent text messages or a couple of recent pictures is hardly a massive invasion of privacy.'[10] Cromwell J stressed that meaningful limits, rather than blanket exclusions, should be placed on the scope of a mobile phone search.[11] Here, then, arguably, the Supreme Court of Canada (by majority) considers mobile phones to be more like a handbag than a home.

In so far as the United Kingdom is concerned, a very recent report into the 'digital stop and search' powers of police in that jurisdiction found that 'amongst the various police forces who have disclosed their local guidance, there is uncertainty as to the legal basis under which they can extract data from mobile phones'.[12] Police powers to stop and search a person (and seize property) in Queensland largely mirror those in England and Wales,[13] and it appears that, in these jurisdictions, the use of such powers to search mobiles remains unchallenged. Of note, in England and Wales, law enforcement members (including police) can give notices to individuals requiring them to disclose protected information that will allow access to a mobile phone (eg a passcode).[14] Failure to comply with this notice is an offence punishable by up to two years' imprisonment if the case is not one concerning national security (otherwise it is five years' imprisonment).[15]

In 2014, the High Court of Justiciary (the supreme criminal court in Scotland) was faced with a challenge to the admissibility of an SMS (short message service) text message conversation obtained as a result of a police search of a mobile

---

9 [2014] 3 SCR 621 ('*Fearon*').

10 Ibid [61].

11 Ibid [62]–[63]. The dissenting opinion, written by Karakatsanis J, followed the United States Supreme Court's approach in *Riley*: 'Only judicial pre-authorization can provide the effective and impartial balancing of the state's law enforcement objectives with the privacy interests in our personal computers' (ibid [105]).

12 Privacy International, *Digital stop and search: how the UK police can secretly download everything from your mobile phone* (Report, March 2018) 20 <https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf>.

13 See *Police and Criminal Evidence Act 1984* (UK) ss 1, 2.

14 *Regulation of Investigatory Powers Act 2000* (UK) s 49.

15 Ibid s 53.

phone.[16] In *JL, EI v Her Majesty's Advocate*, one of the appellants, 'JL', submitted that her iPhone 5 was not just a mobile phone, but was also, in effect, a portable computer — indeed, one that was continually connected to the internet. It was submitted that the police had no authority for 'going into the phone' and that it involved going into JL's 'private cyber-space'.[17] The Court refused the appeal and held that the relevant police power used to search included the power to examine. The Court noted that 'what will be required for effective examination will depend on the nature of the item and the nature of the information which it is hoped to elicit from examination'.[18] Further, the Court held that the examination of the mobile phone in question involved little more than connecting the device to a power supply, switching it on, and touching the appropriate portions of the screen, which was clearly within the powers conferred by the relevant search provision and, accordingly, the evidence was admissible, there being no illegality or irregularity in its recovery.[19]

The position in Australia remains uncertain. Of note, in 2017, the Victorian Court of Appeal, by majority (Maxwell P and Beach JA), allowed an interlocutory appeal against a decision by the County Court of Victoria to exclude evidence of the content of two mobile phones that had been downloaded and copied by Customs officers.[20] The decision hinges on whether the phones were 'goods' that were 'imported' or 'exported' and, as such, 'goods subject to the control of Customs'. In so far as the Customs officials were aware of the preconditions for the exercise of their powers to examine the phones, it was noted by the trial judge that there was 'a culture within Customs of an unacceptable level of ignorance and indifference as to what was required by the law and the Instructions'.[21] The Court of Appeal commented on this 'highly adverse finding', stating that, 'plainly, this state of affairs needs to be addressed as a matter of urgency'.[22] Moreover, the Court cited the trial judge's comments regarding the hazards of routine searches of mobile phones:

> [I]f someone downloaded [his or her] iPad, it would not only contain nearly every detail of [his or her] life, (intimate, personal, financial, professional), but also a huge amount of information concerning the operation of [the] court and cases conducted by [him or her] and [his or her] fellow judges.[23]

---

16 *JL, EI v Her Majesty's Advocate* [2014] HCJAC 35.
17 Ibid [6].
18 Ibid [13].
19 Ibid.
20 *DPP (Cth) v Farmer (a Pseudonym)* (2017) 54 VR 420 ('*Farmer*').
21 *DPP (Cth) v [Farmer]* (County Court of Victoria, Judge Allen, 29 May 2017) [26].
22 *Farmer* (n 20) [57].
23 Ibid [223].

The next part of this article explores current laws in Queensland that allow police officers to conduct a search of a mobile phone.

III The Current State of the Law in Queensland

At common law, police do not have the power to stop and search a person; nor can they seize a person's property before an arrest has been made.[24] Queensland statutes, in particular the *Police Powers and Responsibilities Act 2000* (Qld) ('*PPRA*'), have eroded much of the common law's firm position on search and seizures.[25] The effect of the *PPRA* has been to create a spectrum of protections from search. At the upper end of the spectrum sits a dwelling, and at the lower end sits the person and a public place.[26] Dwellings (eg a home or hotel room) assume privileged status because they are the traditional repositories for highly personal effects. Dwellings are locations where 'intimate things are kept from prying eyes, and intimate relationships are carried on away from prying ears'.[27] Put simply, privacy expectations are the strongest in dwellings. Consequently, the law places significant restraint on police powers to enter and search dwellings. One exception aside — the conduct of a search to prevent the immediate loss of evidence[28] — police must obtain a warrant before they enter and search a dwelling.[29]

In contrast, a person, places other than dwellings (eg vehicles and vacant land), and public places (eg roads, parks, shops and beaches) are afforded the lowest level of protection. At this (lower) end of the spectrum, police may search a person without a warrant if they reasonably suspect that the person is in possession of prescribed items and/or evidence of the commission of a 'prescribed offence'.[30]

Rather than falling on the spectrum (eg as a 'person' or 'public place'), mobile phones are considered a 'thing' that is discoverable during the search of a location or a person. That is to say, mobile phones are considered *incidental to* the search. The authority for police to search the contents of a mobile phone depends on whether the search is conducted with or without a warrant and, in the case of a warrantless search, whether the search has been conducted prior or subsequent

---

24 Danielle Andrewartha et al, *Investigating Crime: The Laws of Australia* (Thompson Reuters, 2013) 113.

25 See *George v Rockett* (1990) 170 CLR 104, 110–11.

26 For the definition of the terms 'dwelling', 'place' and 'public place', see *Police Powers and Responsibilities Act 2000* (Qld) sch 6.

27 Cynthia Lee, 'Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us about the Fourth Amendment' (2010) 100(4) *Journal of Criminal Law and Criminology* 1403, 1424.

28 See *Police Powers and Responsibilities Act 2000* (Qld) s 160 ('*PPRA*').

29 Ibid ss 150–1.

30 Ibid ss 29–31, 443.

to the making of an arrest. This section of the article, exploring the current state of the law in Queensland relating to police searches of mobile phones, is divided into two parts: Part A, which examines warrantless searches; and Part B, which examines searches under a warrant.

A *Warrantless Searches*

1 *Consent*

The common law has long recognised that a person has no legal duty to assist police.[31] In Queensland, where a person voluntarily consents to a request issued by a police officer, and that person understands that she or he has a real choice whether to comply, there is no interference with that person's liberty.[32] As such, where a police officer obtains and relies on informed consent, for example to search a person or his or her property, that police officer does not need to rely on a unique common-law or statutory power to act. This stands in contrast to the position in England and Wales where 'an officer must not search a person, even with his or her consent, where no power to search is applicable'.[33]

At common law, it is incumbent on a police officer to ensure that a person is acting with informed consent; that is, the police officer is required to give a clear indication that the person is free to refuse to comply with the officer's demand or direction.[34] In regard to the search of a mobile phone, this requirement is of significance given the scope of information or evidence that may be accessed. Broadly, consent-based searches are fraught with complexity and, 'given the nature of the relationship between police and citizen (whether suspect or not), an equality of power is extremely unlikely'.[35] Sitting recently in the Supreme Court of Victoria, Bell J emphasised:

> [W]hen drawing the line between the voluntary and the coerced, it is necessary to take into account the imbalance of power between police, especially when in uniform, and ordinary members of the community, as well as the psychological impact on apparent police authority.[36]

Consider *R v Varga*.[37] In that case, police officers were conducting a lawful search of premises, authorised by a search warrant that was not accompanied by what is

---

31 See *Rice v Connolly* [1966] 2 All ER 649.
32 *R v Lavery* (1978) 19 SASR 515, 516–17. See also more recently *R v Kerkhoffs* [2015] QDC 198 [22].
33 *Police and Criminal Evidence Act 1984* (UK), Codes of Practice, Code A, 1.5.
34 *Dedman v The Queen* [1985] 2 SCR 2.
35 David Dixon, *Law in Policing: Legal Regulation and Police Practices* (Clarendon Press, 1997) 92.
36 *DPP v Kaba* [2014] VSC 152, [71].
37 [2015] QDC 82 ('*Varga*').

commonly known as a 'section 154 order'.[38] During the search, a police officer located a mobile phone belonging to Varga and inquired as to the number of the mobile phone. Varga admitted that he did not know the number from memory but, as the number was listed as the first contact in the contact list contained in the phone, Varga gave the police permission to access the mobile phone and look at the stored contacts list. Relying on Varga's consent, a police officer accessed the phone and proceeded to search not only the phone's contact list, but also the SMS text messages stored on the phone. In the words of the trial judge, the SMS texts stored on the mobile phone were a 'fertile source of information about the commission of indictable offences involving dangerous drugs'.[39] No other evidence was found at the premises to support the drug-trafficking or drug-supply charges levelled against Varga. The Court held that Varga's consent to access the phone and view the contact list entitled the police to lawfully search all the data stored on phone.

With respect, the decision in *Varga* is problematic. It turns a limited consensual search into a licence to conduct a general exploratory search (or 'fishing expedition'). Not only did the police exceed the confines contemplated by Varga (the phone's contact list), they also misrepresented the aim of the search. Based on the above, it is submitted that where consent is relied on by police to search a mobile phone, voluntary informed consent should only be made out where the owner or person possessing the mobile phone has been:

1. expressly told the reason for the request;
2. expressly told of the scope of the search (eg to view calls made in the last hour); and
3. properly advised that she or he is free to refuse compliance with the request.

Further, it is argued that the request and consent must (where practicable) be electronically recorded. The purpose of the recording, among other things, is to ensure that it can be demonstrated that the search was based on true consent. Moreover, it is suggested that consent-based searches of mobile phones should be strictly limited to specific request (ie recent call log). Permission to view recent calls should not be considered consent to view nine-month-old SMS text messages.

---

38 See below Part III(B) for further discussion on s 154 orders. In general, a s 154 order is contained in a search warrant and is issued pursuant to s 154 of the *PPRA*. It compels the owner or person in possession of a storage device, such as a mobile phone, to provide the information necessary (eg the passcode) to provide a police officer access to the device and to the information stored on the device. In *Varga*, the search warrant did not contain a s 154 order; consequently, police could only rely on Varga's informed consent to access the device.

39 *Varga* (n 37) [44] (Durward DCJ).

2 *Pre-arrest*

(a) Power to Search

In Queensland, a lawful search can be conducted without a warrant when a police officer reasonably suspects that a prescribed circumstance exists (eg that a person possesses an unlawful dangerous drug or a weapon, or has something, or there is something in a vehicle, that may be evidence of a commission of a seven-year imprisonment offence, which thing may be concealed on the person or destroyed).[40]

In such circumstances, police officers are authorised to conduct a search of (a) the person and anything in the person's possession, and/or (b) an occupied vehicle and anything in it, for anything relevant to the circumstances for which the person or the vehicle and its occupants are detained.[41] The use of the term 'anything' signals a broad discretion, empowering police to search, inter alia, a mobile phone found on the person or in a vehicle.

While the scope of search is broad, it is not limitless. The language of these provisions does not authorise police to use anything found in the vehicle or on the person to search somewhere or something else (eg discovering an office key does not authorise a subsequent search of the person's office). In respect of a mobile phone, police are authorised to search the data stored on the mobile phone (if it can be lawfully accessed); however, they are not authorised to use the mobile phone to access the internet and download information to the mobile phone.[42] In *R v Jaudzems*, Henry J was required to consider the admissibility of Facebook messages uncovered during the search of a Blackberry device, which was found when police were conducting a warrantless search of a vehicle. The admissibility of the Facebook messages was determined on the basis of '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'.[43] On this point his Honour (correctly, in our view) observed that only the former (ie only information stored on the phone) would be admissible.

As noted above, a pre-arrest search requires a police officer to 'reasonably suspect' that a prescribed circumstance exists. 'Reasonable suspicion' is a well-established legal principle. Dalton J thoughtfully defined the concept in *R v Bossley* as follows:

> The term 'reasonably suspects' is defined in Schedule 6 to the PPRA as meaning, 'suspects on grounds that are reasonable in the circumstances'. There is also well-established common law authority in relation to both the concept of suspicion and the

---

40 *PPRA* (n 28) ss 30, 32.
41 Ibid ss 29, 31.
42 See, eg, *R v Jaudzems* [2014] QSC 74.
43 Ibid [24].

> concept of reasonable suspicion. The meaning of suspicion in this context is discussed by the High Court in George v Rockett. A suspicion and a belief are different states of mind. A suspicion is a state of conjure or surmise. It is more than idle wondering. It is a positive feeling of apprehension or mistrust, but it is a slight opinion within sufficient evidence. Facts which reasonably ground a suspicion may be quite insufficient to reasonably ground a belief. Nonetheless, to have a reasonable suspicion some factual basis for the suspicion must exist. There must be sufficient factual grounds reasonably to induce the suspicion. The facts must be sufficient to induce the suspicion in the mind of a reasonable person. The suspicion must be reasonable, as opposed to arbitrary, irrational or prejudiced. If a young man is driving a smart car with some panel damage it is not sufficient to give rise to a reasonable suspicion.[44]

Failure on the part of a person to consent to the search of his or her mobile phone is, without more, in the circumstances, incapable of being considered reasonable to ground suspicion of a prescribed circumstance. Further, should a police officer form reasonable suspicion of a prescribed circumstance, and subsequently request a person to provide warrantless access to a mobile phone (ie provide them with a passcode or fingerprint), then that police officer is under a duty to caution the suspect in line with s 431 of the *PPRA*.[45]

Consider the following hypothetical: A Queensland police officer reasonably suspects that Rachel, a pedestrian walking through Queen Street Mall, is in possession of an illegal handgun. The police officer stops Rachel and searches her pursuant to ss 29 and 30(a)(i) of the *PPRA*. It turns out that Rachel is not in possession of a handgun; the officer was in error. Rachel was, however, in possession of handbag, which contained, inter alia, a mobile phone. Is the officer permitted to search Rachel's phone?

The answer to this question hinges on an interpretation of s 29(1)(b) of the *PPRA*. In its entirety, s 29(1)(b) provides that a police officer, without a warrant, may 'search the person and anything in the person's possession *for anything relevant to the circumstances for which the person is detained*'.[46] The phrase 'for anything relevant to the circumstances for which the person is detained' would appear, in some circumstances, to curtail a police officer's power to search a mobile phone. If a mobile phone is not a thing relevant to the circumstances for which the person is detained, then a police officer is prohibited from searching the mobile phone, unless that officer formed subsequent reasonable suspicion of a prescribed circumstance that would permit a search of the mobile phone.[47]

---

44 *R v Bossley* [2012] QSC 292, [14] (citations omitted).

45 See *R v Ford* [2017] QSC 205 (Flanagan J).

46 Emphasis added.

47 A police officer is not necessarily prohibited from conducting a further or subsequent search in circumstances where the initial search failed to uncover incriminating evidence. See, eg, *R v N* [2015] QSC 91; *R v Peirson* [2014] QSC 134 ('*Peirson*').

In *R v Peirson*,[48] police officers encountered Peirson exiting a taxi with a group of friends in Fortitude Valley, Brisbane. Based on Peirson's physical appearance and demeanour,[49] the police officers reasonably suspected that he was under the influence and in possession of a dangerous drug. Acting pursuant to ss 29(1) and 30(a)(ii) of the *PPRA*, police conducted a warrantless search of Peirson, which failed to uncover any evidence that he was in possession of a dangerous drug. The search did, however, uncover a mobile phone. Despite a negative search (ie no drugs were found on Peirson), police retained possession of the mobile phone and proceeded to question Peirson as to whether he had any drug-related messages on it. In response, Peirson purportedly said, 'Ah, there shouldn't be.'[50] The police officer then searched the phone (presumably the mobile phone was unlocked) and found drug-related messages. This search was justified by the police officer because, according to him, 'in his experience … people in possession of drugs use mobile phone text messages to obtain the drugs'.[51]

Following the discovery of the messages, Peirson was cautioned and subsequently charged with possessing property (a mobile phone) suspected of being used in connection with the commission of a drug offence. He was further charged with trafficking due to an investigation based on the text messages. Peirson argued that the second search — the search of his mobile phone — was illegal and that 'once it had been established that [he] was not in possession of drugs, the authorisation for detaining him was exhausted and he should have been released or cautioned'.[52] Douglas J rejected this argument and noted that asking questions about the phone, which Peirson responded to, 'formed reasonable suspicion justifying the continuation of [the police officer's] search of it as well'.[53]

Peirson highlights the hazards of allowing pre-arrest searches of mobile phones, specifically, the risk that indolent police investigative practices will be encouraged. With respect, the decision of *Peirson* is problematic for several reasons. First, it should be noted that Peirson was only cautioned after the 'second search' (ie the search of the mobile phone). At the point that Peirson was asked by the officer whether he had any drug-related messages on his phone, Peirson had not been informed that he had the right to stay silent. This would appear to be in

---

48 *Peirson* (n 47).

49 Peirson was said to be 'unsteady on his feet, that his pupils were dilated, he was sweating a bit but he was "licking his lips profusely"': ibid [3].

50 Ibid [5].

51 Ibid.

52 Ibid [20].

53 Ibid [30]. Carmody CJ, in obiter, confirmed his support for this decision in *R v N* (n 47) [42].

breach of the *PPRA*.[54] Secondly, while the purported response by Peirson, 'Ah, there shouldn't be', can be considered equivocal, arguably, it is not, by itself, sufficient to form reasonable suspicion. That is to say, it is conceivable that a person with no drug-related text messages on their phone could provide the same (equivocal) response. Third, and finally, this is a situation where a mobile phone was considered a 'thing' '*relevant to the circumstances for which the person is detained*' and therefore capable of being searched.[55] While it is accepted that the reasonableness of a suspicion held by a police officer will be relative to the circumstances, it must be remembered that, given the strong association between our daily lives and our reliance on mobile phones, it is difficult to conceive of a situation where a mobile phone would not be thought of as 'relevant to the circumstances', that is, worth searching to find more information about a person's activity, criminal or otherwise. Notwithstanding this clear relationship between our activities and our phones, a balance must be struck between the routine police search of mobile phones to detect crime and an individual's privacy.

It is submitted that the search in *Peirson* was more akin to a fishing expedition than a well-founded, authorised search. The decision demonstrates that, in Queensland, a mobile phone is considered property similar to a handbag. For completeness, based on the facts provided in the case, it is presumed that the mobile phone was unlocked (ie not encrypted), but in circumstances where it was locked, then, in the absence of Peirson's (informed) consent or compliance, police would have been required to obtain an 'access order' from a magistrate or a judge (s 154A *PPRA* (*ex post*)) before the text messages could be retrieved.

As mentioned above, the reasonableness of a suspicion will be relative to the situation. Indeed, reasonable suspicion can, at any given moment, form in the mind of a police officer, but, equally, it may subsequently fade. The case of *R v N* is a prime example of a search performed in circumstances where 'reasonable suspicion' had faded.[56] There, N and a group of friends were detained in a hotel room while police conducted an exigent search[57] in relation to drugs. N was subject to an initial strip search by a police officer (K), which produced a negative result (the initial search). K, wrongly believing that drugs had been discovered elsewhere in the hotel room, then searched N's handbag (the second search). A mobile phone and $305 in cash was found. Believing the money to be drug proceeds, K seized the mobile phone and searched its data base (the third search). Incriminating SMS text messages were found during the third search. On appeal, N argued that the second and third searches where illegal: 'Any power to detain N ceased at the end of the first search, and that K had no legal authority to search

54 *PPRA* (n 28) s 431.
55 Ibid s 29(1)(b).
56 *R v N* (n 47).
57 See below Part III(A)(4) for discussion on exigent searches.

the handbag or its contents beyond that.'[58] The Court held that the search of the mobile phone was unauthorised. Carmody CJ found that

> a reasonable person in the circumstances of K would not have held the required suspicion based on the same information, observation or reasoning … N's possession of $305 or so … is not, either of itself or in combination with other material circumstances, logically suggestive of N's drug dealing … An unreasonable suspicion is an insufficient legal basis for K's seizure and warrantless search of the [mobile phone].[59]

The above cases involving pre-arrest searches demonstrate, among other things, an over-reliance on finding mobile phone data in circumstances where there has been a 'negative search' (ie nothing obviously incriminating has been found). The cases demonstrate that, currently, mobile phones are considered a 'thing' capable of being discovered as part of a search of a person and therefore capable of being searched — similar to a handbag or wallet.

(b) Power to Seize

In addition to search powers, the *PPRA* provides police officers with the power to, without a warrant, 'seize all or part of a thing that may provide evidence of the commission of an offence'.[60] The thing seized does not need to be a thing for which a police officer conducted the search. The term 'seize' has been defined according to its ordinary meaning: 'to take possession of by legal authority or to confiscate'.[61] It includes the power to retain but not impound the thing,[62] the power to examine the thing,[63] and the power to arrange for someone else to examine the thing.[64]

The power to examine a thing seized (ss 618–19 of the *PPRA*) has the potential to create the greatest mischief. These provisions were introduced into the *PPRA* in 2006.[65] The term 'examine' is not defined in the *PPRA*, and the accompanying explanatory notes and parliamentary debates on the Bill introducing the provisions do not provide any relevant context or additional interpretative guidance.[66] The ordinary definition of 'examine' is 'to inspect or

---

58 Ibid [42].
59 Ibid [43]–[45].
60 *PPRA* (n 28) ss 29(2), 31(5).
61 *R v Lloyd* [2014] QDC 181, [17].
62 *PPRA* (n 28) sch 6.
63 Ibid s 618(a).
64 Ibid s 618(b).
65 Initially inserted as ss 337B and 337C of the *PPRA* by the *Police Powers and Responsibilities and Other Acts Amendment Act 2006* (Qld) s 54.
66 Explanatory Notes, Police Powers and Responsibilities and Other Acts Amendment Bill 2006 (Qld) 25; Queensland, *Parliamentary Debates*, Legislative Assembly, 23 May 2006, 1818.

scrutinize carefully; inquire into or investigate'.[67] A strict interpretation of the statutory provisions mentioned above suggests that once a mobile phone has been seized, it can be accessed, and its contents inspected. It is suggested that it could not have been the intention of the legislature to circumvent the inherent limitations of the powers of search with these seize-and-examine provisions. If the contrary position were true, in circumstances where a mobile phone was seized and, relying on the power to examine, a police officer directed a person to provide a passcode or fingerprint to access the mobile phone for the purposes of inspecting its contents, and that person refused to follow that direction, it would follow that the police officer may seek to charge that person with obstruction.[68]

It may be questioned why the offence would be obstruction and not contravening a direction.[69] The offence of contravening a direction provides for an excuse not to comply. Section 791(2) of the *PPRA* states:

> A person must not contravene a requirement or direction given by a police officer, including a requirement or direction contained in a notice given by a police officer, under this Act, unless the person has a reasonable excuse.

Critically, then, s 791(4) of the *PPRA* states:

> Unless otherwise expressly provided, it is a reasonable excuse for a person not to comply with a requirement or direction to give information if giving the information would tend to incriminate the person.

The right of an individual to claim privilege against self-incrimination provides a lawful excuse to not provide the access information to one's mobile phone.

Unlike s 791 of the *PPRA*, s 790 (obstructing a police officer) does not expressly provide for a reasonable excuse. Section 790 provides that 'a person must not assault or obstruct a police officer in the performance of the officer's duties'. To be liable for an offence under s 790, the police officer must have been acting in the performance or execution of his or her duty. As to the meaning of 'performance of the officer's duties', the powers of a police officer are not exhaustively defined. Indeed, s 9(a) and (b) of the *PPRA* expressly provide that the *PPRA* does not affect powers that a constable has at common law or as an individual. In *Rice v Connolly*,[70] Lord Parker CJ observed that 'there is no exhaustive definition of the powers and obligations of the police, but they are at least those, and they would further include the duty to detect crime and to bring

---

67 *Macquarie Dictionary* (online at 27 April 2019) 'examine'.

68 *PPRA* (n 28) s 790.

69 Ibid s 791.

70 [1966] 2 QB 144 ('*Rice*'); MJ Shanahan et al, *Carter's Criminal Law in Queensland* (LexisNexis, 21st ed, 2016) [240,060].

an offender to justice'.[71] In *Innes v Weate*, Cosgrove J, endorsing Lord Parker CJ's observations, said:

> [T]he range of circumstances in which the duty to act may arise is too wide, too various, and too difficult to anticipate for the compilation of an exhaustive list … It is important that a constable should have a wide discretion to act swiftly and decisively; it is equally important that the exercise of that discretion should be subject to scrutiny and control so that he should not too easily or officiously clothe himself with the powers of the State and by so doing affect the rights and duties of other citizens.[72]

The term 'obstruct' is defined in s 790(3) of the *PPRA* as including 'hinder, resist and attempt to obstruct'. Concerningly, then, the broad powers of a police officer so as to be considered in the 'performance of his or her duties' means that a person may be liable to an offence under s 790 of the *PPRA* for failing to provide his or her mobile phone to a police officer or, indeed, for failing to permit the mobile phone to be accessed.

The Queensland District Court decision in *R v Charlton*[73] illuminates, among other things, the current position of pre-arrest searches and demonstrates that police officers may warn suspects that failing to provide access to a mobile phone may constitute an offence. *Charlton* was an application to exclude evidence — in particular, incriminating text messages located on the mobile phone belonging to Charlton (the applicant). In July 2014, as part of covert police operations in Brisbane nightclubs, Charlton and another (S) were seen inside a bar exchanging what looked to be a 50-dollar note. Based on this 'close and low'[74] transaction, followed by immediate separation of the pair, Charlton was suspected of supplying an unlawful dangerous drug. Charlton was stopped and searched. A mobile phone was recovered and the police officer requested that Charlton allow him to search his (Charlton's) phone records. Charlton's phone was PIN-protected and he initially refused to access to the phone. Charlton was advised that if he did not provide the PIN the phone would be subject to seizure and Charlton could be charged with obstructing a police officer. Charlton supplied the PIN and incriminating text messages dated some nine months earlier were found.

Relying on the power to search a person in a prescribed circumstance (s 29 of the *PPRA*), and the power to prevent the loss of evidence (s 160 of the *PPRA*), the police officers led evidence to the effect that they reasonably suspected that Charlton was engaged in the act of supplying a dangerous drug to S. As part of this evidence, one officer stated:

---

71 *Rice* (n 70) 419.

72 *Innes v Weate* [1984] Tas R 14, 51; Shanahan et al (n 70) [251,265.1].

73 *R v Charlton* (District Court of Queensland, Dearden DCJ, 18 March 2016) ('*Charlton*').

74 Ibid [2].

> My reasons for seizing the phone was [sic] that in my experience drug suppliers and users utilise their phones to arrange the transactions and that messages are normally contained in the phone that would provide supporting evidence to the commission of a seven-year offence.[75]

In excluding the text messages, Dearden DCJ stated:

> [A]ny suspicion raised by the observations of police officers … was no longer 'reasonable' at the point at which the applicant [Charlton], and the other male [S] were strip searched and no drugs were located, nor was there (apparently) an amount of cash on the applicant which was referable to the fifty-dollar note described by police …[76]

Dearden DCJ then considered whether, despite the unlawful search of the mobile phone and its contents, it was in the public interest to admit the text messages and bring to conviction those who commit criminal offences.

> In my view, the incriminating text messages located on the mobile phone … so substantially predate the search of the applicant … arising as it did out of a purported exchange between two persons, one of them the applicant, in a bar, not resulting in any criminal charge, given no evidence was located in respect of any such exchange — that it justifies the exclusion of such unlawfully obtained evidence. In the words of Carmody CJ in *R v N* …: 'The desirability of admitting the texts does not outweigh the undesirability of the illegal and overly intrusive means of obtaining them.'[77]

For completeness, we also note that there are several other provisions of the *PPRA* that provide police with powers to undertake warrantless searches and potentially to seize mobile phones. For example:

1. Section 33(1): A police officer has the power to enter and search a public place and seize a thing found at a public place, if he or she reasonably suspects that the thing may be evidence of the commission of an offence.
2. Section 33(1)(f): A police officer, in a public place, has the power to open anything that is locked.
3. Section 196: If a police officer lawfully enters a place, or is in a public place, he or she has the power to seize anything that he or she reasonably suspects to be evidence of the commission of an offence.

In respect of s 33(1)(f), it is accepted that a police officer should have a power to determine whether an apparently abandoned or forgotten backpack, suitcase or package left unattended in a public place, such as in a park or a train station, is hazardous (eg whether it contains explosives), and to identify the owner.

---

75 Ibid.
76 Ibid [16].
77 Ibid [19].

However, relying on this power to access a mobile phone for any other purpose would certainly not be acceptable.

Further, provisions of the *PPRA*, when used in conjunction with other legislation, for example the *Transport Operations (Road Use Management — Road Rules Regulations) 2009* (Qld) ('*TORUM*'), provide police with additional scope to exercise warrantless search and seize powers. For example, if a police officer reasonably suspects a person of using his or her mobile phone while driving (an offence under s 300 of the *TORUM*), the police officer may stop the vehicle (pursuant to s 60 of the *PPRA*) and ask to view the data on the mobile phone to confirm his or her suspicions. If the driver refuses to comply, the police officer may seize the mobile phone (pursuant to s 196 of the *PPRA*).

Concluding this part of the article, we argue that, currently, a pre-arrest search of a mobile phone is ungoverned, hazardous and erodes not only the privacy of individuals, but also public confidence in policing trends and practices. In the light of *Peirson*, *R v N* and *Charlton*, pre-arrest searches should only occur, if ever, with the informed consent of the person (which must, if practicable, be electronically recorded). In those circumstances, the police officer must clearly communicate the scope of the search to the individual (eg calls made and received in the last hour), and be held to these limits in scope. In the absence of informed consent, where a police officer reasonably suspects that there may be incriminating evidence contained in a mobile phone, the item should be seized as evidence and any subsequent search or examination of the phone should be authorised by a warrant.

The chief concern and, therefore, justification for a quantum shift in current police practice is that, given that mobile phones have the potential to store and retrieve lots of data, pre-arrest searches can yield not only deeply private information, but also incriminating evidence for which a person may not have been stopped and searched. A corollary of imposing judicial oversight (ie a warrant) to access phone data is that a police officer cannot demand immediate access to the mobile phone and, as such, this avoids a situation where a person may be charged with obstructing an officer for failing to provide access to the phone (eg a passcode or fingerprint). Such a remedy upholds an individual's right not to self-incriminate. In any event, s 790 of the *PPRA* ought to be amended to include a defence of 'reasonable excuse' to obstructing a police officer if providing the information would tend to incriminate the person. A change will also signal that a police officer cannot, based on a fruitless search of a person or his or her personal effects, resort to examining the person's phone to justify a stop and search.

3 *Post-arrest*

A search of a person that is incidental to arrest has been the feature of landmark cases overseas.[78] Unlike most pre-arrest warrantless powers to search, in particular s 29(1) of the *PPRA* — which authorises the search of 'the person and anything in the person's possession' — when a person is lawfully arrested, the powers of search are confined to 'the person' only.[79] If a phone is found during the search of a person incidental to arrest, the powers conferred under s 443 of the *PPRA* limit the authority of police to (a) *seize* the phone as evidence of the commission of an offence, or (b) *take and retain* the phone in safe custody until the person is released. The provision does not authorise a warrantless search of the phone, except in so far as the powers to examine a thing seized (ss 618 and 619 of the *PPRA*) are not construed as providing a power to access a mobile phone to inspect its contents (as discussed above). In this regard, Queensland law is consistent with the position of the United States Supreme Court in *Riley*.

We consider that s 443 of the *PPRA* provides adequate privacy protections. If a police officer wants to search a mobile phone seized incidental to an arrest, he or she must obtain a warrant. What is troubling is the realisation that the *PPRA* may incentivise the police to delay an arrest in order to exploit the broader search powers provided for under the existing pre-arrest warrantless searches provisions.

4 *Exigent Search to Prevent Loss*

A police officer may, pursuant to s 160 of the *PPRA*, enter a place and exercise search warrant powers (which includes the power to search the place, open anything relevant that is locked, and seize anything), if he or she reasonably suspects, for example, that a thing is evidence of the commission of an indictable offence and that thing may be destroyed unless the place is immediately entered and searched. It is incumbent on the police officer exercising this power to obtain a 'post-search approval order' as soon as reasonably practical after exercising powers under s 160.[80] The power to seize any evidence is provided under s 196 of the *PPRA*.

This power to search (and seize) to prevent the loss of evidence has been relied on in several authorities that have already been visited.[81] It is clear that, in determining whether a police officer has acted lawfully in relying on exigent powers to search, not only must the police officer reasonably suspect that a thing

---

78 *Riley* (n 1); *Fearon* (n 9).
79 *PPRA* (n 28) s 443(1).
80 *PPRA* (n 28) s 161.
81 See *R v N* (n 47); *Charlton* (n 73).

in the possession of a person at a place is evidence of the commission of a pt 2 offence, the police officer must also reasonably suspect that the evidence may be concealed or destroyed unless the place is entered and the thing in the possession of the person is searched.[82] This raises concerns about the ability for someone to remotely access and erase or modify information stored on a mobile phone even after it has been seized and secured by police. To overcome this issue, the Queensland Police Operational Procedures Manual recommends that, when seized, a mobile phone should be disconnected from wireless networks and potentially stored in a sealed metal container.[83] Of course, this assumes that police have access to the mobile phone's setting options in the first instance.

B *Searches Under Warrant*

A search warrant is issued for the purpose of entering and searching a place to, inter alia, obtain evidence of the commission of an offence.[84] A search warrant is not issued to search a thing, such as a mobile phone. It is for this reason that a mobile phone seized and retained in custody at a watch-house can only be searched under a search warrant issued to enter and search the watch-house itself. Given that a mobile phone can store and access so much data, we argue that warrants that allow for the seizure and search of a mobile phone should include the 'virtual boundaries' of the search (eg the search is limited to those SMS text messages received and sent in the last six months that are stored on the phone). The following part of this article details (1) '154 orders', (2) '178 orders', and (3) non-compliance with these orders.

1 *Section 154 Orders*

All search warrants issued under ch 7 of the *PPRA* allow for the recovery of a mobile phone (and the data stored on it) as evidence of the commission of an offence. However, not all search warrants are the same when it comes to gaining access to a mobile phone (and the data stored on it). Search warrants distinguish between electronic storage devices (including mobile phones) that are passcode-protected or encrypted and electronic storage devices that are not passcode-protected or encrypted. This distinction was created in 2006 by the introduction of s 154 of the *PPRA* (commonly referred to as a 's 154 order'). As depicted in

---

82 See *R v Koning* [2001] QSC 131, [13]; *R v Pohl* [2014] QSC 173.

83 Queensland Police Service, *Operational Procedures Manual* (Public Edition Issue 69, 11 April 2019) ch 2.6.10, 69–70.

84 See *PPRA* (n 28) s 150.

Figure 1 below, the effect of the provision is to create a search power that extends beyond those generally available in a general search warrant.[85]

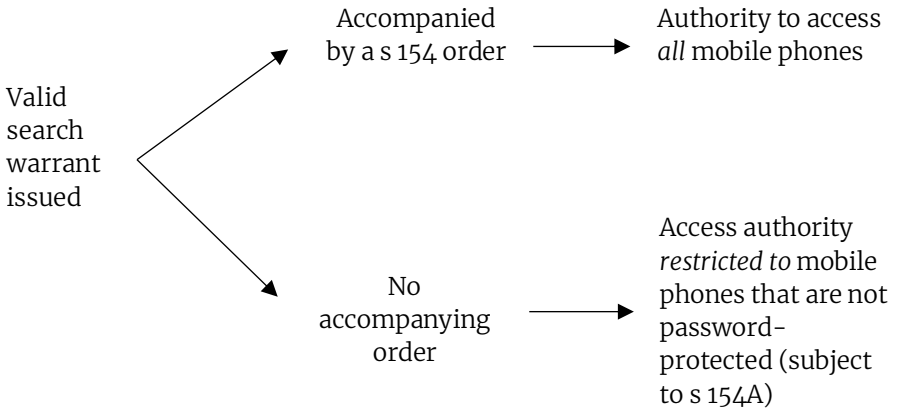

Figure 1: Effect of the s 154 order on searching mobile phones

Section 154 was introduced to overcome the issue that while police are able to seize a mobile phone, in a growing number of instances where mobile phones were protected by a passcode or the information was encrypted, it was impossible for police to access and obtain the stored evidence in order to investigate or to prosecute an offender.[86] A s 154 order compels the owner or person possessing the mobile phone to provide the information necessary to allow a police officer access to the device and to the information stored on the device. A person who fails to provide the information commits a crime.[87]

In 2016, the Queensland legislature introduced an *ex-post* provision that effectively allows police officers to rectify a defective search warrant (ie a search warrant that did not originally contain a s 154 order).[88] Section 154A of the *PPRA* provides police with a mechanism to obtain an order compelling a person to provide access information any time after a storage device has been seized and removed from a place.

The scope of the search powers under a s 154 order is the same as the scope under the *PPRA*'s warrantless-search provisions; that is, s 154 explicitly restricts the scope of the search to stored information only. This interpretation is

---

85 See also *Varga* (n 37), [30]: '[Section 154] is plainly an additional power beyond those generally available in a search warrant'.

86 See *Varga* (n 37), [32].

87 See *Criminal Code 1899* (Qld) s 205A ('*Criminal Code*').

88 See *PPRA* (n 28) s 154A (introduced by the *Serious and Organised Crime Legislation Amendment Act 2016* (Qld) s 303).

consistent with the accompanying explanatory notes, which confirm that the provision only grants police access 'to data that has already been downloaded or received' by the mobile phone.[89] Police cannot use the phone to access data stored elsewhere, including on a remote server. For, as the United States Supreme Court has observed, '[s]uch 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'.[90] An obvious problem for law enforcement is the realisation that advancements in technology and improvements in connectivity will make it more difficult to determine whether particular information is stored on the phone or in 'the cloud' (data stored and accessed using the internet).

2 *Section 178A Orders*

In 2018, the Queensland legislature amended the *PPRA* to permit police officers to obtain the equivalent of a s 154 order for storage devices (including mobile phones) discovered at or seized from a crime scene ('a s 178A order').[91] In order to obtain this access-approval order, a police officer is required to demonstrate that there are 'reasonable grounds for suspecting that the information stored on the storage device may be evidence of the commission of the offence for which the crime scene was, or is to be, established'.[92] A 'crime scene' is defined as either (a) a place where an indictable offence carrying a maximum penalty of at least four years' imprisonment has been committed ('an Offence'), or (b) a place containing evidence of sufficient probative value of the commission of an Offence that happened at another place.[93] These provisions were introduced to facilitate the 'forensic examination' of locked electronic storage devices, such as mobile phones and computers. An inability to access such devices, which are not easily unlocked, was said to be frustrating investigative efforts.[94]

3 *Failure to Comply with a s 154, s 154A or s 178A Order*

Failure to comply with an access-approval order issued under either s 154, s 154A or s 178A of the *PPRA* constitutes a crime punishable by a maximum of five years' imprisonment.[95] This raises a contentious issue: what of the right of an individual

---

89 Explanatory Notes (n 66). See also *Varga* (n 37) [32].

90 *Riley* (n 1) 2491.

91 See *PPRA* (n 28) s 178A (introduced by the *Police Powers and Responsibilities and Other Legislation Amendment Act 2018* (Qld) s 25).

92 See ibid s 178A(2).

93 See ibid ss 163A, 163B.

94 Explanatory Notes, Police Powers and Responsibilities and Other Legislation Amendment Bill 2018 (Qld) 3.

95 See *Criminal Code* (n 87) s 205A.

to claim privilege against self-incrimination? This right was abrogated by the passage of the *Serious and Organised Crime Legislation Amendment Act 2016* (Qld) ('*SOCLA Act*').

The *SOCLA Act* introduced s 154B into the *PPRA* and s 205A into the *Criminal Code*.[96] These provisions provide clear and unambiguous intention on the part of the Queensland legislature to abrogate the privilege. Section 154B reads:

> A person is not excused from complying with an order made under section 154(1) or (2) or 154A(2) on the ground that complying with it may tend to incriminate the person or make the person liable to a penalty.

Prior to the commencement of the *SOCLA Act*, the right of an individual to claim privilege against self-incrimination constituted a lawful excuse to not providing the access information to one's mobile phone. This was confirmed by the Queensland Court of Appeal in *Wassmuth v Commissioner of Police*.[97]

Wassmuth involved the execution of a search warrant in relation to the supply and possession of dangerous drugs. The search warrant included a s 154 order and was issued in August 2016 (several months before the passing of the relevant provisions of the *SOCLA Act*). During the search, police officers located a mobile phone and asked Wassmuth for the access code. This request was not complied with and Wassmuth was charged and convicted of an offence under s 205 of the *Criminal Code* (disobeying a lawful order).[98] Relevantly, Wassmuth appealed the conviction on the ground that her right to insist on her privilege not to incriminate herself constituted a lawful excuse under s 205 of the *Criminal Code* to not comply with the order contained in the search warrant to provide the access passcode to her mobile phone. In a unanimous decision, the Court of Appeal agreed.[99]

IV Dangerous Drugs and Mobile Phones

As a convenient form of communication, mobile phones are frequently used to facilitate the supply of drugs.[100] In Queensland, it is an offence to possess 'anything' that has been or is used in connection with a drug offence,[101] or 'any property' reasonably suspected of having been used in connection with a drug

---

96 *SOCLA Act* ss 75, 303.

97 [2018] QCA 290 ('*Wassmuth*').

98 Section 205 reads: 'Any person who without lawful excuse, the proof of which lies on the person, disobeys any lawful order issued by any court of justice, or by any person authorised by any public statute in force in Queensland to make the order, is guilty of a misdemeanour, unless some mode of proceeding against the person for such disobedience is expressly provided by statute, and is intended to be exclusive of all other punishment.'

99 *Wassmuth* (n 97) [29]–[31].

100 See ibid [27].

101 See *Drugs Misuse Act 1986* (Qld) s 10(1).

offence.[102] Here, problematically, the terms 'anything' or 'any property' include a mobile phone.

Darwen v Smith[103] provides a powerful example of how this provision can be used by police in respect of mobile phones.[104] In that case, Darwen happened to be on private premises when police executed a lawful search warrant in relation to the possession of dangerous drugs. Darwen was not a resident of the premises; he was unknown to police before the execution of the warrant, and he was not found to be in possession of any drugs at the time. Darwen did, however, have a mobile phone in his possession, which he produced at the request of the police. The mobile phone was found to contain a SMS text, which purportedly could 'reasonably be seen as a message relating to a proposed supply of drugs to the recipient of the message'.[105] Based on this message, Darwen was charged and convicted under s 10A(1)(b) of the *Drugs Misuse Act 1986* (Qld). It sufficed that the mobile phone was reasonably suspected of having been used in connection with the supply of drugs, even though the drugs may not have been supplied at all.[106]

V The 'Search Spectrum' and Mobile Phones

It is apparent from the above discussion that the law in Queensland treats a locked mobile phone differently to that of an unlocked mobile phone. Both are repositories for highly personal effects. Why should the existence of a passcode alter the treatment of a mobile phone?

Leaving a mobile phone without passcode protection cannot be said to constitute a waiver of the owner's privacy interest in the vast array of information accessible through the mobile phone; nor can it be held to demonstrate a subjectively diminished expectation of privacy. Like the private sphere of the home, mobile phones remain intensely personal, even when we do not take every possible precaution to protect them. A person who leaves his or her front door unlocked does not forfeit to the state his or her privacy interest in his or her home; the same should also be true of a mobile phone.

The use of mobile phones creates a need for the existing legislation to be examined carefully. It is submitted that, without the consent of a person or a warrant, a police officer may only seize a mobile phone. Given that it is difficult to conceive of a sphere of privacy more intensely personal — or indeed more pervasive — than that found within an individual's mobile phone, when viewed

---

102 Ibid s 10A(1).
103 [2007] QDC 30 ('*Darwen*').
104 See also *Peirson* (n 47); *R v N* (n 47).
105 *Darwen* (n 103) [3].
106 Ibid [7].

on the privacy spectrum afforded to property, mobile phones should be considered on an equal footing with a private dwelling. Judicial pre-authorisation to search a mobile phone should be considered 'an essential bulwark against unjustified infringements of individual privacy'.[107]

VI Recommendations

To date, the question of whether police should have the power to search a mobile phone in Queensland has not been challenged. It is unclear what, if any, impact the *Human Rights Act 2019* (Qld) will have on the issues and concerns expressed in this article. We argue that, because of the gravity of this topic and the public interest, a parliamentary review is necessary. This is for several reasons, among them the need for greater transparency. Existing police powers need to be examined through a lens that considers mobile phones as akin to private homes. The situation in Queensland can be considered similar to the United Kingdom, which, according to Privacy International, was very recently outlined in the following terms:

> Across the country the police have expanded their use of mobile phone extraction without public attention and without effective oversight. It is not enough to rely on PACE [the *Police and Criminal Evidence Act 1984* (UK)] to search mobile phones — a piece of legislation written long before a phone became a device that could be used as a pocket surveillance tool. Traditional search practices, where no warrant is required, are wholly inappropriate for such a deeply intrusive search.[108]

Notwithstanding, it is recommended that terms contained within the *PPRA* be improved to provide clarity and consistency. The terms 'examine', 'search', 'seize', 'access' and 'inspect' appear in various sections of the *PPRA* but are silent as to the question of whether a police officer can require a person to grant access to his or her mobile phone and allow a police officer to explore its content. Legislation seeking to curb individual rights and freedoms must employ clear and unambiguous language.[109]

Generally, clearer guidelines are needed to identify the circumstances in which a police officer can seize a mobile phone without a warrant, but not explore its content. Given the invasive nature of the search of a mobile phone, it may be considered appropriate for the threshold of 'reasonable suspicion' of a prescribed circumstance (eg ss 30, 32 and 160 of the *PPRA*) to be raised to one of 'reasonable belief' in the case of search or seizure of a mobile phone. Such a burden does not seem too great when viewed in the light of the fact that an application for a

---

107 *Fearon* (n 9) [197] (Karakatsanis J).
108 Privacy International (n 12) 64.
109 *Coco v R* (1994) 179 CLR 427.

warrant to enter and search a place must have a special provision included so as to afford officers the power to require access to electronic storage devices (s 154 of the *PPRA*).

New and improved legal safeguards are necessary to prevent indolent police practices. One suggested improvement noted at various junctures of this article concerns the procedure for obtaining consent to search data stored on a mobile phone. In circumstances where a person's consent to search his or her phone is being relied on, additional steps should be taken to ensure that the police officer expressly makes it known that the person is free to refuse.[110] The suggestion that consent-based searches are problematic and require further examination is not new.[111] The proliferation of powerful portable technology calls for greater attention to the complexities of consent-based searches. Other recommendations include limiting the scope of the search of a mobile phone, as well as ensuring that detailed records be kept on the data examined (including the justification for accessing that data). The downloading of entire data sets from a detained person's mobile phone would, in most circumstances, be unnecessary and extreme. The retention and later use of that data by the police service is worrying, and the subject for another article entirely.

[110] *Dedman v The Queen* [1985] 2 SCR 2.

[111] Dixon (n 35) 124.