ORDER PROHIBITING PUBLICATION OF THE JUDGMENT AND ANY PART OF THE PROCEEDINGS (INCLUDING THE RESULT) IN NEWS MEDIA OR ON THE INTERNET OR OTHER PUBLICLY AVAILABLE DATABASE UNTIL FINAL DISPOSITION OF TRIAL. PUBLICATION IN LAW REPORT OR LAW DIGEST PERMITTED.

IN THE SUPREME COURT OF NEW ZEALAND

SC 12/2016
[2017] NZSC 42

BETWEEN	THE QUEEN Appellant
AND	GREGORY JOHN ALSFORD Respondent
	PRIVACY COMMISSIONER Intervener

Hearing:	16 June 2016
Court:	Elias CJ, William Young, Glazebrook, Arnold and O'Regan JJ
Counsel:	M J Lillico and P D Marshall for Appellant J H M Eaton QC and F E Geiringer for Respondent J C Edwards (Privacy Commissioner) with J M Hayward
Judgment:	29 March 2017

JUDGMENT OF THE COURT

A **The appeal is allowed. The evidence obtained from the searches conducted on 19 December 2012 is admissible at trial.**

B **Order prohibiting publication of the judgment or any part of the proceedings (including the result) in the news media or on the internet or other publicly available database until final disposition of the trial. Publication in a law report or law digest permitted.**

REASONS

William Young, Glazebrook, Arnold and O'Regan JJ [1]
Elias CJ [103]

WILLIAM YOUNG, GLAZEBROOK, ARNOLD AND O'REGAN JJ
(Given by Arnold J)

Table of Contents

	Para No.
The appeal	[1]
Background	[5]
Power consumption information	[14]
Were the police required to seek the power consumption data by way of a production order?	[18]
Was there compliance with the Privacy Act?	[30]
Use of power consumption information in applications	[47]
Conclusion	[73]
2010 search	[75]
Conclusion	[100]
Decision	[102]

The appeal

[1] Like *Marwood v Commissioner of Police*, this appeal raises questions concerning the use of improperly obtained evidence in contexts other than the criminal proceeding in the course of which the evidence was acquired.[1] We gave a results judgment on 26 October 2016 allowing the appeal.[2] These are our reasons.

[2] The information at issue was obtained as a result of an unlawful search and was ruled inadmissible in an earlier criminal proceeding following the balancing process required by s 30 of the Evidence Act 2006.[3] Consequently, that earlier prosecution of the respondent, Gregory Alsford, based on the information could not proceed. The police used the same information several years later when applying for a production order in respect of Mr Alsford's mobile phone data in the context of further possible offending. Having obtained apparently incriminating texts, the

---

1 *Marwood v Commissioner of Police* [2016] NZSC 139, [2017] 1 NZLR 260.
2 *R v Alsford* [2016] NZSC 140.
3 *Police v Alsford* DC Christchurch, CRI-2010-009-6053, 17 September 2010 [*Alsford* admissibility judgment (DC)].

police then obtained search warrants in respect of several properties owned by Mr Alsford. The search warrant applications simply mentioned that Mr Alsford had been charged previously, without any detail. Information obtained as a result of the production order and the search warrants led to Mr Alsford facing the current drug charges. One of the issues in the appeal concerns the effect of the police using the information that had earlier been ruled inadmissible in this way.

[3] The other issue in the appeal concerns the use by the police of power consumption data provided by electricity supply companies. The data, which was "personal information" in terms of s 2 of the Privacy Act 1993, was provided voluntarily in response to requests from the police. This raises the question of the relationship between the information privacy principles found in s 6 of the Privacy Act and the prohibition on unreasonable search and seizure in s 21 of the New Zealand Bill of Rights Act 1990 (NZBORA).

[4] We emphasise that this aspect of the appeal does not deal with situations where information is obtained by police as a result of physical searches of premises, nor does it deal with situations in which information is protected by other principles, such as legal professional privilege or commercial confidentiality. This judgment must be understood against that background.

Background

[5] The essential facts can be stated briefly. In September 2012, the police received information by way of an anonymous call on the Crime Stoppers telephone line that a person called "Greg" was cultivating cannabis in the garage of a two storey, weatherboard property at 1/21 Pannell Avenue and that he had bypassed the power meter using his skills as an electrician. The caller provided a physical description of "Greg" and said that he had a female partner and two children.

[6] On the basis of this information, the police conducted further investigations. These showed that Mr Alsford was the sole director of the company that owned the Pannell Avenue property; that the company's postal address was 116 Baker Street, a property owned by Mr Alsford and Ms Jeanette Alsford; that two cars parked at the Pannell Avenue property were registered in Mr Alsford's name; that Mr Alsford was

the landline subscriber for the Pannell Avenue address; that Mr Alsford fitted the physical description given by the informant; and that the police had searched the Baker Street property in 2010 and had found there a cannabis growing operation, which Mr Alsford admitted he had established. Mr Alsford had been charged as a result of the 2010 search, but the case did not proceed as the search was held to have been unlawful, and the evidence obtained from it was ruled inadmissible.[4]

[7] The police then sought information concerning electricity usage at the Pannell Avenue and Baker Street properties from the relevant electricity supply companies, on a voluntary basis. The information requested was provided and showed that the electricity consumption at the Pannell Avenue property was uniform throughout the year (rather than being higher in the colder winter months) and was below the national average and at the Baker Street property was much lower than the national average.

[8] On the basis of this information, Detective Sergeant Simpson applied on 1 November 2012 for a production order under s 71 of the Search and Surveillance Act 2012 requiring the production of Mr Alsford's mobile phone records.

[9] The 14 page application included the information provided by the Crime Stoppers informant, the information from the various police inquiries following the Crime Stoppers call, information relating to the 2010 search (including Mr Alsford's admission that he had set up the cannabis operation and the fact that the search had been ruled unlawful and the prosecution dismissed), and detailed information about power consumption at the two addresses. The application explained the relevance of the power consumption figures by noting that high intensity discharge lights were commonly used in hydroponic cannabis growing operations and this increased electricity consumption, so that cannabis growers often bypassed their electricity meters both to avoid detection and to reduce costs.

[10] The production order was granted. Some of the text messages obtained pursuant to this order indicated that the user of the phone was involved in drug dealing. In light of this further information, Detective Simpson applied for warrants

---

4 *Alsford* admissibility judgment (DC), above n 3.

to search the properties at 1/21 Pannell Avenue, 116 Baker Street and another address associated with Mr Alsford. The Detective summarised the information relied on for the purpose of the Pannell Avenue application as follows:

> - the Crimestoppers information refers to Greg who is known to be cultivating cannabis at his home address of 1/21 Pannell Avenue and is said to have bypassed his meter.
> - that Gregory ALSFORD is an electrician and has the knowledge to bypass his meter.
> - that the electricity consumption is low and consistent with being bypassed.
> - that [Mr Alsford] was previously charged with having a substantial indoor cannabis grow at 116 Baker Street in 2010.
> - that the subsequent text messaging evidence supports the Crimestoppers information.

The warrant applications were granted and the warrants were executed. The police discovered cannabis growing operations at both the Pannell Avenue and Baker Street properties. Mr Alsford's fingerprints were found on items that had been used for cultivating cannabis at the Baker Street property.

[11] Mr Alsford was then charged with eight counts of cannabis-related offending – cultivation, possession for the purpose of sale, supply and knowingly permitting premises to be used for cultivation. He sought to have the evidence obtained as a result of the execution of the search warrants excluded. This was on the basis that:

(a) The evidence obtained as a result of the unlawful 2010 search should not have been used to support the application for the production order. Without that evidence, there was not a sufficient basis for the issue of a production order.

(b) Without the text message evidence obtained from the production order, there was an insufficient evidentiary basis for the issue of the search warrants.

(c) In addition, the power consumption data was inaccurate and/or misleading and should not have been used in the applications for the production order and the search warrants.

(d) Consequently, the search warrants were unlawful and the evidence obtained as result of their execution should be excluded.

[12] In a detailed judgment, Judge Neave held that the evidence had been obtained improperly and excluded it.[5] On appeal, the Court of Appeal upheld this decision, by a majority.[6] This Court granted leave on the following points:[7]

(a) whether the electricity records were improperly obtained from the electricity suppliers;

(b) whether the Court of Appeal was correct to hold that the evidence that had earlier been excluded as improperly obtained (that is, the evidence produced by the 2010 search) could not be relied upon in the applications; and

(c) whether, if improperly obtained, the evidence presently at issue should be admitted under s 30(2)(b) of the Evidence Act.

[13] We will begin our consideration with the power consumption information, before turning to the use of the evidence resulting from the illegal search in 2010.

Power consumption information

[14] There are three issues in relation to the power consumption information, namely:

(a) Were the police required to utilise the production order process to obtain the information rather than making requests under the Privacy Act?

---

5 *R v Alsford* [2015] NZDC 3489 [*Alsford* (DC)].
6 *R v Alsford* [2015] NZCA 628 (Ellen France P, French and Winkelmann JJ) [*Alsford* (CA)].
7 *R v Alsford* [2016] NZSC 21.

(b) If not, were the releases of the information valid in terms of the Privacy Act?

(c) How do the answers to these questions impact on the production order and search warrant applications in fact made?

[15] Before dealing with these questions, however, we should note two points. First, the Privacy Commissioner, Mr John Edwards, was granted leave to intervene on this aspect of the appeal. We acknowledge the considerable assistance we have derived from his submissions.

[16] Second, Mr Eaton QC submitted that, at the hearing before Judge Neave in the District Court, the issue of the lawfulness of the requests for the power consumption information was not fully argued because all of the relevant information as to the basis of the police requests to the power companies was not available. Judge Neave noted that the police had not provided the relevant information but decided that he had sufficient grounds to resolve the case without it.[8] Mr Eaton submits that, as a result, there have been no findings of fact on the nature of the police requests or whether the power companies concerned undertook any analysis of their obligations under the Privacy Act. Moreover, he submitted, the Court of Appeal did not find it necessary to resolve the issue.[9]

[17] Despite the deficiencies in the evidence, we consider that we are able to address the issues in relation to the power consumption data. This is because, as we explain in more detail below, we consider (in disagreement with the Chief Justice) that the decisive issue is not whether the power consumption records were obtained consistently with the Privacy Act but whether they were obtained as a result of an unreasonable search, contrary to s 21 of NZBORA.[10] Whether there was a "search" depends upon whether the consumption data was information in respect of which Mr Alsford had a reasonable expectation of privacy. If the there was a reasonable expectation of privacy in relation to the data, it would have been obtained as a result

---

8 *Alsford* (DC), above n 5, at [54].

9 *Alsford* (CA), above n 6, at [57] per Ellen France P.

10 Section 21 of the New Zealand Bill of Rights Act 1990 provides that "Everyone has the right to be secure against unreasonable search or seizure".

of a search and the question under s 21 would then be whether the search was reasonable or not.

Were the police required to seek the power consumption data by way of a production order?

[18] Prior to the enactment of sub-pt 2 of pt 3 of the Search and Surveillance Act, there was no production order regime generally available to police to facilitate the investigation of criminal offences.[11] In their 2007 *Search and Surveillance Powers* report, the Law Commission recommended the introduction of such a regime.[12] The Commission conceived of the production orders as an "alternative to search warrants",[13] with the same essential requirements.[14] The Commission specifically rejected having a lower threshold than applied to search warrants, such as reasonable grounds to suspect that the information sought would assist in the investigation of an offence.[15]

[19] The perceived benefit of the production order process over the search warrant process was that it would be less disruptive – the agency concerned would be required to produce the specified information rather than having to allow the police to search through its business or other records to find the information needed. Because a production order would be directed at a particular person or entity rather than at a particular place, the police would not need to specify where they believed the information sought was kept. Overall, the availability of the production order process would make the investigative process more efficient.[16] The Commission envisaged that the production order process would be available to obtain material such as business records, utility use data or telephone records.[17] Given this legislative background, and the reference to "utility use data" in particular, counsel for Mr Alsford argued that the police ought to have used the production order process to obtain the power consumption data.

---

11 There were specific regimes in particular contexts: see, for example, the Serious Fraud Office Act 1990, s 9.

12 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.22] and recommendations 10.1–10.5.

13 At [10.26].

14 At [10.24].

15 At [10.26].

16 At [10.18].

17 At [10.25].

[20] We consider that the enactment of the production order process was intended simply to provide a less intrusive alternative to the use of search warrants, as is indicated by both the legislative history and the fact that similar tests apply in respect of production orders and search warrants, rather than to prevent the police from obtaining information voluntarily (provided they do so lawfully). In particular:

(a) Section 6 of the Search and Surveillance Act provides that a search warrant may be issued where there are reasonable grounds (a) "to suspect that an offence … punishable by imprisonment has been committed, or is being committed, or will be committed" and (b) to believe that the search will find evidential material relating to the offence at a particular place.[18]

(b) Section 72 provides that a production order may be issued where there are reasonable grounds (a) "to suspect that [a qualifying] offence has been committed, or is being committed, or will be committed" and (b) to believe that the documents sought are evidential material in relation to the offence and are, or will be, in the possession or control of the person against whom the order is sought.

Statements in the House by the responsible Minister, Hon Judith Collins, during the passage of the Search and Surveillance Bill[19] confirm that production orders were intended to be an alternative to search warrants.[20]

[21] We think it significant in this context that Parliament has not, despite the existence of the search warrant process, prohibited consent searches by the police where they do not have sufficient information to obtain a warrant. Rather, it has

---

[18] Section 6 requires reasonable suspicion in relation to the commission of an offence and reasonable belief in relation to evidential material being found in a particular place. There is a question, which we leave open, whether this bifurcated approach was intended to change the approach under s 198 of the Summary Proceedings Act 1957. In addition, we note that the term "evidential material" is defined in s 3 of the Search and Surveillance Act 2012 in a way that appears to include not only inculpatory but also exculpatory material. This is consistent with the recommendation of the Law Commission: see above n 12, at [3.27] and [3.35]–[3.39]. Again, however, we leave the point open.

[19] Search and Surveillance Bill 2009 (45).

[20] See (7 March 2012) 678 NZPD 970; (20 March 2012) 678 NZPD 1115; and (22 March 2012) 678 NZPD 1246.

recognised that the police may carry out consent searches (whether or not they have grounds to obtain a warrant) but has regulated them. Such searches are provided for in ss 91–96 of the Search and Surveillance Act. Section 91 provides:

> **91 Application of rules about consent searches**
>
> Sections 92 to 95 apply in respect of consent searches undertaken by an enforcement officer in circumstances where a power of search by an enforcement officer to which this Part applies or any provisions of this Part apply (whether a warrantless power or a power able to be conferred by a search warrant) could be exercised if the officer held a particular belief or suspicion.

The effect of this provision is that a consent search may be undertaken in accordance with ss 92–95 even though the officer undertaking it does not have the suspicion or belief necessary to obtain a search warrant. This is made clear by the Law Commission, which specifically rejected introducing a "reasonable grounds" requirement for consent searches.[21]

[22] It appears that the consent search provisions were introduced to meet problems that were perceived to result from the police having an unrestricted ability to conduct consent searches (despite the existence of the warrant process). The effect of the provisions is to restrict the circumstances in which such searches can be conducted lawfully, by setting out the purposes for which a consent search may be conducted and by establishing pre-conditions for a valid consent.[22] The existence of the consent search provisions suggests that Parliament did not see the enactment of the production order process as necessarily restricting the ability of the police to obtain information voluntarily.

[23] There is the complication in this case that the information sought by the police from the power companies concerned a third party, Mr Alsford, even though the records were, in a formal sense, the companies' records and their compilation and retention were necessary to the companies' commercial operations. There are several decisions of the Court of Appeal which have accepted that the police may obtain what can fairly be described as customer information from service providers

---

21 See Law Commission, above n 12, at [3.67]–[3.70].

22 See Law Commission, above n 12, at [3.65] and [3.75]–[3.83].

on a voluntary basis. One example is *R v Thompson*,[23] which we discuss later in these reasons.[24] Another is *R v Harris*.[25] There the defendants were charged with drug offences, money laundering and social welfare fraud. They challenged pre-trial rulings that the evidence of a former bank officer of some of their banking transactions, and further evidence obtained under warrant, was admissible at trial. The bank officer's observations had initiated the police investigation and subsequent prosecution. The argument for the defendants was that evidence from the former bank officer would breach the Financial Transactions Reporting Act 1996, which was a complete code and prohibited reporting other than in accordance with its terms.

[24] The Court rejected the defendants' argument. It held that the common law position continued to apply. While banks owed a general duty of confidence to their customers, there were limits to that duty. These included circumstances where the bank had a duty to the public to disclose or where the bank's interests required disclosure. The Court went on to say:[26]

> … there is no confidence preventing the disclosure of iniquity … . It is significant that in the present case the bank accounts themselves were the vehicles for the offending – namely money laundering. Even in the absence of legislation there would be a power and perhaps even a duty to consider and respond to police questions about that.

The Court considered that the police were free to seek relevant information from banks "at least in the absence of any reason to believe that the disclosure would be unlawful".[27] It concluded:[28]

> … the bank would appear to be completely within its rights under the law as it was before the enactment of the 1996 Act to respond to police inquiries on the basis that it has reasonable grounds to suspect that a customer may be involved in serious criminal activity. Its freedom to take that action has in no way been limited by that Act. On the contrary, the purpose of the legislation is to emphasise those rights or freedoms by supporting them with obligations.

---

23 *R v Thompson* [2001] 1 NZLR 129 (CA).
24 See below at [51]–[52].
25 *R v Harris* [2000] 2 NZLR 524 (CA).
26 At [10].
27 At [10].
28 At [13].

[25] A further case is *R v Cox*.[29] In the course of investigating suspected drug offending, the police advised a mobile phone operator that they would be seeking call data and text messages in relation to several phone numbers associated with the appellants. The operator advised that they would supply the past call data and texts in response to a search warrant and future call data and texts in response to a call data warrant. The operator said that, in the meantime, it would "pre-load" the particular numbers, that is, the operator would store all texts to and from those numbers rather than deleting them within a 32 hour period in accordance with their usual practice. The operator provided the relevant information to the police both before and after the police had obtained call data and search warrants. One of the issues raised by the case was whether there were any legal restrictions on the right of the operator or the police in relation to the collection and release of the text data.

[26] The Court considered whether the actions of the operator and the police involved breaches of (i) confidentiality obligations; (ii) the Privacy Act; and (iii) s 21 of NZBORA, and concluded that they did not. For the purposes of s 21, the Court was prepared to treat what had occurred as a search but held that, in the particular circumstances, the search was not unreasonable. The Court noted that under the law as it then stood the ability of the police to obtain information by statutory processes was not clear and then said:[30]

> The relevant information was in the possession of Vodafone. Vodafone, as a good corporate citizen, should cooperate with the police and assist the police with legitimate enquiries. In circumstances where the police obtain a call data warrant, Vodafone could fairly conclude that there was a legitimate basis for the police operation. This would therefore fairly alleviate confidentiality concerns which might otherwise have discouraged Vodafone from co-operating with police.

[27] In deciding that the search was reasonable, the Court distinguished its earlier decision in *R v H*.[31] In that case, a director of a fishing company was charged with offences under the Secret Commissions Act 1910, on the basis that he corruptly gave money to an agent for the Ministry of Agriculture and Fisheries (MAF), as a reward for favours to the company. The director had instructed the company's accountant to make certain payments to the agent. The accountant became suspicious and

---

29 *R v Cox* (2004) 21 CRNZ 1 (CA).
30 At [66].
31 *R v H* [1994] 2 NZLR 143 (CA).

contacted MAF. MAF laid a complaint with the police, who arranged for the accountant to provide them with company files and photocopies of company documents. He did so over a period of about 20 months. The Court accepted that it was arguable that the accountant had not breached his obligation of confidence to his employer as the public interest required disclosure.[32] However, given the lengthy period over which the supply of documents occurred, the Court considered that there was no practical or other impediment to the police obtaining one or more search warrants to obtain them. In effect, the police had deliberately refrained from obtaining a warrant when they could have done so.[33] Applying the then current prima facie exclusion rule, the Court excluded the evidence on the ground that it had been obtained by an unreasonable search.

[28] Our purpose in referring to these authorities is simply to show that New Zealand courts have accepted that service providers may legitimately provide some customer information to the police voluntarily, at least in some circumstances. We are not to be taken as necessarily approving the relevant reasoning in all the cases, which must now be read against the background of subsequent legislative developments such as the enactment of the Search and Surveillance Act. But we do think it significant that in both *R v Cox* and *R v H*, the central feature of the Court's analysis was s 21 of NZBORA. We will return to this aspect following our discussion of the Privacy Act.

[29] We conclude, then, that the introduction of the production order process in the Search and Surveillance Act was not intended to limit the ability of the police to obtain information such as power usage data voluntarily, provided they do so lawfully. This brings us to the next issue, namely whether there was compliance with the Privacy Act.

Was there compliance with the Privacy Act?

[30] We begin by describing the relevant parts of the Privacy Act. First, "personal information" is defined in the Act to mean "information about an identifiable

---

32 At 148–149.
33 At 149.

individual".[34] Obviously, this is a definition which captures a wide range of information "from the very sensitive to the seemingly banal", as Mr Edwards put it. Although there may be a question whether power consumption data falls within it given that such data relates to a particular place rather than a particular person, we will proceed on the basis that the data is "personal information" in the sense that it indicates the power consumption at a place owned and occupied by identifiable individuals.

[31] Second, s 6 contains a number of privacy principles applying to agencies holding or dealing with personal information. Four are of particular relevance here – principles 1, 2, 4 and 11:

(a) The effect of principle 1 is that the police may not collect personal information about a person unless (i) it is collected for a lawful purpose connected with a police function or activity and (ii) the collection of the information is necessary for that purpose.

(b) Principle 2(1) requires that an agency collecting personal information collect it directly from the person concerned. However, principle 2(2) goes on to say that an agency need not comply with this requirement in a number of specified circumstances, one of which (principle 2(2)(d)(i)) is that non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency (the wording of the exception is identical to that in principle 11(e), which we quote below).

(c) The effect of principle 4 is that an agency may not collect personal information by means that are unlawful or, in the particular circumstances of the case, are unfair or unreasonably intrusive.

(d) Finally, principle 11 provides:

---

[34] Privacy Act 1993, s 2.

> An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—
>
> …
>
> (e) that non-compliance is necessary—
>
> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
>
> (ii) for the enforcement of a law imposing a pecuniary penalty; or
>
> …
>
> (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); …
>
> Besides appearing in principle 2(2)(d), the exception in principle 11(e) also appears in principle 3(4)(c), which deals with advising individuals of the collection of their personal information, and in principle 10(c), which deals the use of personal information by the holding agency.

[32] Principles 2(2)(d) and 11(e) are, in effect, different sides of the same coin. Under principle 2(2)(d), the police may request personal information about a person from an agency holding such information provided that the requirements in the exception are met; under principle 11(e), the holding agency may supply the requested information to police provided that the exception's requirements are met.

[33] Two features of the language of the exception require emphasis in the present context. The first is that an agency may not gather personal information indirectly (principle 2) or disclose personal information (principle 11) unless it believes on reasonable grounds that non-compliance with the relevant principle is necessary for one of the specified purposes. Focussing on principle 11(e), this implies that the requesting agency must provide the holding agency with sufficient information to enable it to reach a reasonably-based view about whether or not the information is required for an authorised purpose. On this basis, it would not be sufficient for the

police simply to request information without giving any indication of why it was sought – as Mr Eaton submitted, the mere fact that police request information will not meet the threshold. On the other hand, as Mr Edwards noted, requiring the police to disclose the detail of an investigation to an agency holding sought-after information may compromise the investigation and may itself involve further disclosure of personal information. We return to this issue when discussing the facts of the present case.

[34] The second feature is that the authorised purposes in the exception are broadly stated. They refer to avoiding "prejudice to the maintenance of the law by any public sector agency". They then go on to include within that broad principle, avoiding prejudice to "the prevention, detection, investigation, prosecution, and punishment of offences". Focussing again on principle 11(e), the references to "the maintenance of the law" and to avoiding "prejudice to", together with the breadth of the included purposes, particularly prevention, detection and investigation, are relevant to the nature of the reasonable grounds test that the holder of the information is required to meet to justify disclosure. They suggest that the test – belief on reasonable grounds that non-compliance is necessary – is a relatively low one. The language (particularly the reference to "detection") also suggests that a holding agency would be justified in providing personal information to the police even where the police did not have sufficient grounds to obtain a warrant or a production order. So, for example, if the police request personal information at the early stages of an investigation, they may not be able to say much more by way of justifying the request than that they are investigating a particular offence and that power consumption records may be relevant to the investigation, with some indication as to why they are relevant. In short, what is required is an indication of why the police are requesting the information. We observe that information obtained by police from a holding agency will still be subject to the provisions of the Privacy Act in the hands of the police.

[35] We do not consider that the use of the word "necessary" means that the police must indicate to the holding agency why they are seeking the information informally rather than by means of a formal process such as a production warrant. In the case of an investigation, for example, it is up to the police to determine what investigatory

tools are available to them in light of the then current state of their investigation. If they decide to seek information voluntarily rather than by way of a formal process, on the approach we adopt they will face the risk that they will be found to have acquired the information by means of a "search", which will then engage s 21. We do not think that a holding agency is in a position to make any sensible assessment of the reasons why the police have chosen one investigatory mechanism over another. That does not mean, of course, that the protection afforded to a holding agency by principle 11(e) will necessarily apply where it hands over sensitive personal information in response to a request from the police. In those circumstances, not only will there be a "search", but the holding agency (and the police) may also be in breach of the privacy principles, depending on the particular circumstances.

[36] There is a third point to be made about principle 11. By virtue of s 7 of the Privacy Act, nothing in principle 11 derogates from any statutory provision that authorises or requires personal information to be made available or regulates the manner in which personal information may be obtained or made available. The provisions of the Search and Surveillance Act provide an obvious example.

[37] Finally in relation to the Privacy Act, we note that the privacy principles do not, for the most part, create rights that are enforceable through the courts. Rather, the Act contains its own enforcement mechanisms. This is made clear by s 11, which provides:

> **11 Enforceability of principles**
>
> (1) The entitlements conferred on an individual by subclause (1) of principle 6, in so far as that subclause relates to personal information held by a public sector agency, are legal rights, and are enforceable accordingly in a court of law.[35]
>
> (2) Subject to subsection (1), the information privacy principles do not confer on any person any legal right that is enforceable in a court of law.

[38] The fact that the privacy principles do not create rights that are enforceable through the courts (apart from the exception noted in s 11(1)) does not mean that

---

35 Principle 6(1) gives individuals the right to find out from agencies whether they hold personal information about them and, if so, to have access to that information.

breaches of those rights are irrelevant in a court setting, however. The privacy principles may affect the interpretation of the Search and Surveillance Act given that the Act's purpose is "to facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values" by (among other things) providing rules that recognise the importance of rights and entitlements affirmed in other legislation including the Privacy Act.[36] Further, in some circumstances a breach of a privacy principle may be relevant to the assessment whether evidence has been obtained unfairly in terms of s 30(5)(c) of the Evidence Act[37] or to the balancing process to be carried out under s 30(2).

[39] Two points should be noted about this possibility, however. First, there is a need for caution given (a) the breadth of the term "personal information", which, as we have said, covers information from highly personal to insignificant; and (b) the range of possible breaches, which will cover the spectrum from minor to significant. So the nature of the personal information at issue and the particular way in which the privacy principles were breached will be important. Second, even where the information at issue is personally sensitive and the breach of the privacy principles is serious, those circumstances may add little to the s 30 analysis, given the approach to police accessing of personal information which we outline later in these reasons.

[40] Accordingly, while we accept the possibility that the fact that personal information was obtained in breach of the privacy principles will be relevant under s 30, we think it unlikely that it will be of any independent significance in many instances. This is because what will be significant to the s 30 assessment is the nature of the conduct at issue rather than the fact that it constitutes a breach of the privacy principles. For the sake of completeness, we should also note that *compliance* with the privacy principles does not eliminate the possibility that the information at issue may be found to have been improperly obtained for the purpose of s 30. Again, we do no more than identify the possibility.

---

[36] Search and Surveillance Act, s 5.

[37] The effect of s 11 of the Privacy Act is that information obtained in breach of the privacy principles would not, for that reason alone, be unlawfully obtained in terms of s 30(5)(a) of the Evidence Act 2006. However, if the police obtained information in a way that was for some other reason unlawful (for example, pursuant to an invalidly issued production order), they would have obtained the information unlawfully in terms of principle 4.

[41] Turning to the facts of this case, the police requested power consumption records from three electricity supply companies in relation to the Pannell Avenue and Baker Street properties. A request to Contact Energy was made on a form entitled "Request for information under the Privacy Act 1993", a request to Genesis Energy was made by email under the Privacy Act and a request to Meridian Energy was made on a form headed "Request for Information under the Official Information Act 1982". In terms of the reasons for the requests:

(a) The Privacy Act request form addressed to Contact Energy said:

> Intelligence has indicated that cannabis is possibly being grown at these addresses.

In fact, the request related to only one address, namely 1/21 Pannell Avenue.

(b) The email request under the Privacy Act to Genesis Energy said:

> To assist Police with an investigation we are currently undertaking, information is sought in relation to the following addresses/persons.

The request related to the Pannell Avenue address.

(c) The request to Meridian Energy, misdescribed as an Official Information Act request, said that the police were investigating alleged criminal activity and that "intelligence has indicated that cannabis is possibly being grown at this address". The address identified was the Baker Street address.

[42] There can be no sensible expectation that the police will outline in detail the course of their investigations to date in justifying a request to an agency such as an electricity supplier. That may compromise the investigation and/or involve the disclosure of other personal information (although such disclosure by the police may itself be justified under principle 11(e)). The police do not have to meet the same standard as would be required when they seek a search warrant or production order, and the holding agency cannot be expected to act as a judicial officer would on such an application. Nevertheless, the Act contemplates that an agency disclosing

personal information will have to justify the disclosure if a complaint of unjustified disclosure is made.[38] This supports the view that the requirement for reasonable grounds is a meaningful one, and indicates that any disclosure request should contain sufficient information to enable the holding agency to form a view about whether there are reasonable grounds to believe that disclosing the information is necessary to avoid prejudicing an investigation. In principle, this will require the police to indicate briefly the perceived link between the suspected offence and the power consumption records.

[43] In the present case, two of the requests noted that the police were investigating whether cannabis was being grown at the relevant addresses. Given that the electricity supply companies were likely well aware of the link between power consumption and cannabis growing operations from their general experience,[39] that advice was probably sufficient to allow the companies to conclude that there were the necessary reasonable grounds (although obviously it is preferable that the link be spelled out even if the police think the recipient understands it). In other situations, however, it will be necessary for the police to give a brief indication of why the information sought is relevant to the offence being investigated.

[44] The email request to Genesis Energy under the Privacy Act simply said that the police were investigating an offence. That statement was too general to enable the electricity supply company concerned to reach a view about whether or not there were reasonable grounds to believe that disclosure was necessary to avoid prejudice to the investigation. Further detail should have been given. Accordingly, the release of the power consumption data by this company was not justified in terms of principle 11(e). However, this breach does not necessarily mean that the police obtained the information in breach of principle 4.[40] The information was not obtained by means that were "unlawful" in terms of principle 4, given the effect of

---

38 Privacy Act, pt 8.

39 Given the possibility of illegal bypass of meters, power companies are potentially victims in the case of large scale cannabis growing operations. In his production order application, Detective Simpson described discussions with an investigator from Genesis Energy, who discussed the significance of the power consumption figures and noted the possibility that the meters were being bypassed.

40 See above at [31](c).

s 11 of the Act.[41] Nor do we consider that the information was obtained by means that were, in the circumstances, "unreasonably intrusive".

[45] As to whether the information was obtained by means that were "unfair" for the purpose of principle 4, it might be argued that because the breach of principle 11(e) resulted from the failure of the police to provide sufficient information about the reason for the request, they obtained the information by unfair means. We do not accept that, however. The police were entitled to ask for the information: objectively, their request was justified; if they had given a brief explanation of the type given in support of the other requests, the electricity company would have been entitled to conclude that they should supply the information under principle 11(e). In these circumstances, we do not see the police failure leading to non-compliance by the particular company as constituting unfair means. Moreover, even if the information was unfairly obtained in terms of principle 4, that would not necessarily mean it was unfairly obtained for the purpose of s 30(5)(c) of the Evidence Act.

[46] To the extent, then, that one of the power companies did not have sufficient justification to release the data it released on the basis of the information supplied by the police, we conclude that there was a breach of the Privacy Act. But what, if any, impact does that have?

Use of power consumption information in applications

[47] The applications for the production order and the search warrants referred to the power consumption data, at least some of which was obtained inconsistently with the Privacy Act. Given that the privacy principles do not confer legal rights enforceable in the courts, the fact that some of the power consumption data was obtained in breach of the privacy principles does not mean that it was unlawfully obtained in terms of s 30(5)(a) of the Evidence Act. Nor, standing alone, does it necessarily mean that the data was unfairly obtained in terms of s 30(5)(c). As in *R v H* and *R v Cox*, the critical question is whether the data was obtained as a result of an unreasonable search or seizure in terms of s 21 of NZBORA. To answer this

---

[41] See above at [37].

question, it must first be determined whether there has been a "search", and that depends on the nature of Mr Alsford's privacy interests in the information at issue.

[48] In *Hamed v R*, Blanchard J concluded that there would be a search where the information-gathering activity "invades a reasonable expectation of privacy".[42] The Judge identified two elements to the inquiry: whether the person affected had such an expectation in fact and whether the expectation was one that society is prepared to regard as reasonable. The Judge noted that this was consistent with the approach adopted by the Supreme Court of Canada in *R v Wise*.[43] Although it is not entirely clear, there appears to have been majority support for Blanchard J's approach on this point.[44]

[49] By contrast, Tipping J took a broader view of what constitutes a search. He considered that the word "search" in s 21 had its ordinary sense of "consciously looking for something or somebody"[45] and did not consider that the "reasonable expectation of privacy" test was helpful in this context.[46] He did, however, say that if a search had occurred, reasonable expectations of privacy, and the level of such expectations, would be relevant to the question whether the search was unreasonable in terms of s 21.[47] Ultimately, then, the difference between Blanchard and Tipping JJ does not relate to the relevance of reasonable expectations of privacy to a s 21 analysis but to the point at which they become relevant.

[50] While there is some academic support for Tipping J's approach,[48] we will proceed on the basis of the approach expounded by Blanchard J, which was accepted by both parties in argument before us and appears to reflect the approach adopted by the Law Commission in its *Search and Surveillance* report.[49] When applying that

---

42 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305, at [163] and following. See also *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48 at [103]–[120], where McGrath J took a similar approach to the meaning of "search", although the case was argued on the assumption that there was a search: see Tipping J at [41].

43 *R v Wise* [1992] 1 SCR 527.

44 See the discussion in *Lorigan v R* [2012] NZCA 264, (2012) 25 CRNZ 729 at [15]–[22].

45 *Hamed*, above n 42, at [220].

46 At [223].

47 At [223].

48 Chris Gallivan and Justin Wall "*Hamed*: s 21 BORA" [2012] NZLJ 85 at 86; and Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis, Wellington 2015) at [18.9.4]–[18.9.6].

49 Law Commission, above n 12, at [2.32] and following.

test, we will proceed on the assumption that Mr Alsford had, subjectively, an expectation of privacy in relation to the data.[50] Despite that assumption, however, we are satisfied that such an expectation was unreasonable in relation to the data at issue, as we now explain.

[51] The data at issue was simply aggregate monthly power usage data. In the context of a pre-trial appeal, a Full Bench of the Court of Appeal held in *R v Thompson* that the police were entitled to ask a power supply company for information about power supplies to a particular address, and the power company was entitled to supply that information.[51] The police had received an anonymous tip that cannabis was being grown at a particular property. The police made an enquiry of the local power supply company and received advice that the electricity consumed at the premises was very high and would not be considered normal. This and other information formed the basis for an application for a search warrant in relation to the address. The police discovered a cannabis growing operation in the course of executing the warrant.

[52] The Court of Appeal dealt with various issues, only one of which is presently relevant. In relation to the advice about power consumption, the Court said that it was not unlawful for the police to ask for and obtain information from the power supply company:[52]

> … that limited disclosure for law enforcement purposes and the use of that information by the detective constable in seeking a search warrant … came squarely within exception (e) of Principle 11 of the Privacy Act 1993.

The Court did not specifically address the question whether obtaining the information amounted to a "search" for the purposes of s 21 of NZBORA, although that section was relevant to other issues in the appeal.[53] However, the logic of the decision is that s 21 was not engaged.

---

50 The terms of supply between a service supplier and its customers may be relevant to the question whether a particular customer has an expectation of privacy in relation to his or her data.

51 *R v Thompson*, above n 23.

52 At [54]. It is implicit in this holding that the Court considered the power consumption data to be "personal information" within the meaning of the Privacy Act.

53 Scott Optican "What is a "Search" under s 21 of the New Zealand Bill of Rights Act 1990? An Analysis, Critique and Tripartite Approach" [2001] NZ L Rev 239 criticises the Court of Appeal for failing to address this issue, but expresses the view that the power consumption information "is minimally intrusive and reveals nothing of a truly personal nature": at 249 and 269–270.

[53] It may be that the Court of Appeal in *Thompson* considered that information obtained consistently with principle 11(e) could not, for that reason, have been obtained as a result of an unreasonable search. That view was taken in *R v R*.[54] The defendant was charged with murder and sexual violation. GPS data placed him at the location where the victim had last been seen. The data had been collected by the Department of Corrections as a result of electronic monitoring which had been imposed on the defendant as a condition following his release from prison for other serious offending. The police initially sought the data from Corrections on a voluntary basis because they were concerned about the victim's safety and were aware that the defendant had been in the general area where the victim had disappeared. Later data provided by Corrections led to the discovery of the victim's body. Both the High Court[55] and the Court of Appeal[56] held that the disclosure of the GPS data for this purpose was permitted by s 15A(2)(b) and (c) of the Parole Act 2002 as it was one of the purposes for which the data was collected.

[54] Relevantly to the present case, the defendant had argued that the police had obtained the GPS data in breach of s 21 of NZBORA and that the data was obtained unfairly because it was obtained in breach of the privacy principles. In considering the preliminary question whether the police request for the GPS data was a "search", Winkelmann J in the High Court applied the reasonable expectation of privacy test.[57] She expressed the view that reasonable expectations of privacy in relation to personal information could be determined by reference to the Privacy Act.[58] The Judge said:[59]

> I take the approach that if [the Privacy Act] allows for the sharing of the information in a particular circumstance, and that circumstance applies, the sharing of the information will not amount to a search. It follows, on the particular facts of this case, that the questions of whether there has been an unreasonable search and whether the evidence has been obtained unfairly by breach of the privacy principles will be determined by reference to the same matters.

---

54 *R v R* [2015] NZHC 713; and *R (CA201/2015) v R* [2015] NZCA 165.
55 *R v R*, above n 54, at [67]–[70].
56 *R (CA201/2015)*, above n 54, at [29]–[32].
57 *R v R*, above n 54, at [62].
58 At [63].
59 At [63].

As an alternative to its argument based on s 15A(2)(b) and (c) of the Parole Act, the Crown had argued that the release of the information was permitted by privacy principle 11(e). Winkelmann J accepted that submission. She said:[60]

> The disclosure of the information was necessary for the detection, investigation and prevention of an offence. The situation may have been different if the Police were not dealing with such an urgent situation. I expressly leave open the possibility that in some cases it may be unreasonable for the Police to rely on this exception to obtain the private information. In some circumstances it may be that proceeding to obtain information in this way without a warrant is not *necessary* to avoid prejudice to the maintenance of the law. Those may be circumstances where there is not the same degree of urgency in obtaining the information.

The Court of Appeal agreed with this analysis.[61]

[55] The scope of reasonable expectations of privacy has been considered by the Supreme Court of Canada in a number of cases, four of which we now briefly discuss. In *R v Plant*,[62] the Supreme Court held that power consumption data[63] does not attract a reasonable expectation of privacy. The facts of *Plant* have some similarity to those in the present appeal. The police received a Crime Stoppers tip-off that cannabis was being grown at a house in a particular vicinity. The police identified the house and obtained details of the power consumption at the address for the preceding six months. They then compared the consumption figures with those of two other comparably-sized homes and found that they were four times the average of the other two over the same period. Two officers then went to the property and knocked on the door. When no one answered, they went round to the backdoor. The officers noticed that the basement windows had an opaque covering and that there was an outside vent. They sniffed at the vent, but smelt nothing. Looking inside the vent, they saw that it had been stuffed with plastic.[64] They left when one of the residents arrived. On the basis of the tip-off, the power consumption data and their observations at the house, one of the officers obtained a search warrant. When they executed the warrant, the police found a cannabis growing operation. Mr Plant appealed his conviction.

---

60 At [77]. (Italics in original).

61 *R (CA201/2015) v R*, above n 54, at [33]–[35].

62 *R v Plant* [1993] 3 SCR 281.

63 It is not clear from the judgments in the case how detailed the information was, that is, whether it consisted of monthly aggregate usage figures as in the present case or was more detailed.

64 The Court described this as a "perimeter search".

[56] The Supreme Court was required to address a number of issues, including whether the power consumption records were protected by s 8 of the Canadian Charter of Rights and Freedoms (the Canadian equivalent of s 21 of NZBORA). Writing for the majority,[65] Sopinka J said that the purpose of s 8 was "to protect against intrusion of the state on an individual's privacy" and went on to say that the limits on state action were determined "by balancing the right of citizens to have respected a reasonable expectation of privacy as against the state interest in law enforcement".[66] Sopinka J held that the test for a determination under s 8 was whether the information seized was of a personal and confidential nature.[67] The Judge said that it was necessary to apply a contextual approach when answering this question:[68]

> Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allow for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.

The Judge went on to say:[69]

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.

Sopinka J considered that the nature of the relationship between the appellant and the supplier could not be characterised as confidential, nor could the transaction

---

65 Sopinka J delivered the judgment of himself and Lamer CJ, La Forest, Gonthier, Cory and Iacobucci JJ.

66 At 291.

67 At 293.

68 At 293. From the early days of the New Zealand Bill of Rights Act, the New Zealand Court of Appeal also emphasised the need for a contextual or situational approach to s 21: see the discussion in Optican, above n 53, at 245–247.

69 At 293.

records.[70] The Judge said that because it was possible for members of the public to enquire about power consumption at particular addresses, the information at issue was publicly available.[71] Moreover, as the police were able to obtain the information online by agreement with the power supplier, the acquisition of the records did not involve intrusion into places ordinarily considered to be private.[72]

[57] The minority Judge, McLachlin J, agreed that the critical issue was whether there was a reasonable expectation of privacy in relation to the records,[73] but disagreed concerning the application of the principle to the facts. The Judge considered that power consumption records were "capable of telling much about one's personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there".[74] McLachlin J did not accept that the information was available to the public,[75] but noted that if it had been, she may have come to a different conclusion as to whether there was a reasonable expectation of privacy.[76]

[58] Later decisions of the Supreme Court of Canada illustrate the scope of the reasonable expectation of privacy test in this context. In *R v Tessling*, the Court held unanimously that there was no reasonable expectation of privacy in the heat profile of a house obtained from an aeroplane by way of an infrared camera, so that the profile was not obtained as a result of a "search".[77] The profile led the police to believe that Mr Tessling had a cannabis-growing operation and he was charged and convicted accordingly.

[59] In *R v Gomboc* a majority of the Supreme Court held that information about patterns of power consumption, produced by a digital recording ammeter installed on a power line going into Mr Gomboc's home by an electricity supply company at the

---

70 At 294.
71 At 294.
72 At 295.
73 At 301.
74 At 302.
75 While the police could access the database containing the power consumption records, McLachlin J held that they could do so only by reason of a special arrangement and that there was no evidence that the information was publicly accessible: at 302 and 303.
76 At 303.
77 *R v Tessling* 2004 SCC 67, [2004] 3 SCR 432.

request of the police, did not infringe a reasonable expectation of privacy.[78] This was despite the fact that the ammeter allowed cyclical high usage patterns to be recorded that were strongly suggestive of cannabis growing operations. On the basis of this and other information the police had obtained a search warrant, which revealed the existence of a cannabis-growing operation in Mr Gomboc's home.

[60] There were two majority judgments. Deschamps J delivered the principal judgment.[79] She concluded that several factors weighed against finding a reasonable expectation of privacy in the power consumption data. In particular, no reliable inference could be drawn from the information provided[80] about the occupants or their activities inside the house apart from the possibility of a cannabis growing operation, so that the information was remote from the protected "biographical core" of personal information.[81] Less importantly, in the particular circumstances of the case, the legislative scheme permitted disclosure of customer information to authorities investigating offences[82] and the supply company had a legitimate interest in obtaining the data itself as it was a potential victim of electricity theft.[83] In her concurring judgment, Abella J noted that the cyclical usage pattern produced by the ammeter led to a strong inference that that a cannabis growing operation was taking place in the residence. Because this was information about an activity occurring inside the home, it was presumptively information in respect of which individuals were entitled to expect privacy.[84] However, Abella J concluded that the legislative scheme was decisive and that Mr Gomboc could not reasonably expect privacy in relation to his power consumption records when the law provided that such information could be disclosed to police without his consent (he having made no request for confidentiality).[85] The minority, McLachlin CJ and Fish J, agreed with

---

78 *R v Gomboc* 2010 SCC 55, [2010] 3 SCR 211.

79 Deschamps J delivered the judgment of herself and Charron, Rothstein and Cromwell JJ; Abella J delivered a separate concurring judgment for herself, Binnie and LeBel JJ; and McLachlin CJ delivered the minority judgment of herself and Fish J.

80 A single line graph showing power usage on a daily basis over five days: see the appendix to the decision at 279.

81 At [43].

82 The Alberta legislation provided that a customer could request confidentiality for customer information, in which case such information could not be provided to anyone including the police; in the absence of a confidentiality request, however, the information could be provided to the police for investigatory purposes. Mr Gomboc had not requested confidentiality.

83 At [42]–[43].

84 At [79]–[82].

85 See, for example, at [72]–[73] and [82].

Abella J that the information attracted a privacy interest but disagreed that the legislative scheme was decisive.[86]

[61] Finally, in *Spencer v R* the Supreme Court held unanimously that the police, who were investigating offences involving child pornography, had conducted a "search" when they requested an internet service provider to provide subscriber information (name, address and phone number) associated with a particular IP address.[87] The police relied on the information to obtain a search warrant to search the home of Mr Spencer's sister (with whom Mr Spencer lived) and seize Mr Spencer's computer. A search of Mr Spencer's computer revealed many child pornography images and videos. Mr Spencer was convicted on counts of possessing child pornography and making it available over the internet.

[62] The Supreme Court held that the police did not have lawful authority to conduct the search (that is, obtain the subscriber information matching the IP address) but went on to hold that the evidence should not be excluded,[88] so that his convictions stood. Delivering the judgment of the Court, Cromwell J considered that Mr Spencer had, subjectively, a reasonable expectation of privacy in the subscriber information, which could "readily be inferred from his use of the network connection to transmit sensitive information".[89] Moreover, he concluded that this expectation was reasonable in light of the nature of the privacy interests at stake and the relevant contractual and regulatory framework.[90] In assessing the relevant privacy interests, Cromwell J considered not simply what information was sought from the internet service provider (the subscriber information) but also what access to that information was capable of revealing about the particular individual. The police had requested the subscriber data so that they could link a specific individual to specific on-line activities. This engaged a "high level of informational privacy".[91]

[63] To summarise, the question whether there is a reasonable expectation of privacy in personal information has both subjective and objective elements. The

---

86 See summary at [105].
87 *Spencer v R* 2014 SCC 43, [2014] 2 SCR 212.
88 Under s 24(2) of the Canadian Charter of Rights and Freedoms.
89 At [19].
90 At [52]–[66].
91 At [51].

objective component asks whether the subjective expectation of privacy held by the person involved is an expectation that society is prepared to recognise as reasonable. The court's approach to the determination of that question is a contextual one, requiring a consideration of the particular circumstances of the case. On the Canadian authorities, these circumstances could include:[92]

(a) the nature of the information at issue;

(b) the nature of the relationship between the party releasing the information and the party claiming confidentiality in the information;

(c) the place where the information was obtained; and

(d) the manner in which the information was obtained.

The reasonable expectation of privacy is directed at protecting "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state" and includes information "which tends to reveal intimate details of the lifestyle and personal choices of the individual".[93]

[64] We consider that this approach provides an appropriate framework for analysis in the New Zealand context in a case such as the present. It follows that we do not agree with the approach taken in *R v R* that if information is obtained consistently with the privacy principles, in particular principles 2(2)(d) and 11(e), there will be no "search".[94] This suggests that these privacy principles effectively confer on the police a power to obtain information. However, the principles do not create any such power – in combination, they allow the police to seek personal information other than directly from the person involved and allow (but do not compel) an agency to release information to police provided the statutory pre-conditions are met. Whether a police request for information amounts to a "search" will depend on whether it relates to personal information in respect of

---

92 These are the factors identified by Sopinka J for the majority in *Plant*: see above at [56].
93 See above at [56].
94 *R v R* and *R (CA201/2015) v R*, both above n 54.

which there is a reasonable expectation of privacy, which depends on a consideration of factors such as those identified at [63] above. If there is a reasonable expectation of privacy in the information, there will be a search and the question will become whether the search is unreasonable. In circumstances of exigency such as applied in *R v R*, the search (the voluntary provision of information) may not be unreasonable. But where there is time to obtain a production order or search warrant, the search may well be unreasonable.[95] If there is no reasonable expectation of privacy in the information, there will be no search for the purpose of s 21 and the issue will simply be whether the requirements of the exception in principles 2(2)(d) and 11(e) are met. If they are, that will be the end of the matter. If they are not, then the question will be whether there is any issue of unfairness under s 30; if there is, a proportionality analysis will be required.

[65] As previously noted, we are assuming that the subjective element is met in the present case, so that our focus is on the objective element. In addressing the objective element, we have regard to the context, in particular to the nature of the information obtained, the circumstances in which it was obtained and the nature of Mr Alsford's arrangements with the power supply companies.

[66] First, dealing with the nature of the information obtained, the power companies provided what the police described as billing information, that is, the power consumption figures for each billing month, with an indication whether the monthly figure was an estimate or was based on a reading. There was no breakdown of usage within the month, simply an aggregate figure. Although generally relevant to the investigation into whether Mr Alsford was running a cannabis growing operation, the data in the form obtained did not reveal intimate details of Mr Alsford's lifestyle and personal choices. This is not to say that that power consumption data could never reveal such details,[96] simply that this power

---

[95] There is a further difficulty with the reasoning in *R v R*, which is that it requires the holding agency to determine whether there are circumstances of urgency which make it "necessary" that the information be provided. As previously noted, we do not consider that it was intended that a holding agency should consider both the reasons for the request (in terms of an investigation, for example) and the justification for obtaining the information by request rather than by warrant or production order.

[96] Some types of smart meter may collect power consumption data in a way that does reveal intimate details of a person's lifestyle and other choices.

consumption data did not. This supports the view that any subjective expectation of privacy was unreasonable.

[67] Second, looking at the circumstances in which the information was obtained, the information was gathered and held by three commercial entities for business purposes. They provided it to the police when requested to do so. Although the data provided related to residential properties owned by Mr Alsford or entities associated with him, it was the companies' data, collected for legitimate commercial reasons, and no search of the properties was required to obtain it. While this does not necessarily mean that there could be no reasonable expectation of privacy in the data, it does mean that the special protection recognised in respect of a person's home is not engaged directly.[97] Moreover, the companies had a direct interest in providing the information to the police, in the sense that large scale cannabis growing operations often involve the theft of electricity as a result of meters being bypassed. While this possibility was not raised in the police requests to the supply companies, it is clear from the evidence that at least one of the companies, Genesis Energy, was well aware of potential theft of electricity in this situation.[98] Overall, this consideration also tends to support the view that there was no reasonable expectation of privacy.

[68] Third, there is the nature of the arrangements between the power supply companies and Mr Alsford. Contractual terms of supply may contain provisions relevant to the supply of customer information to third parties and so are relevant to whether or not there is a reasonable expectation of privacy. The existence of contractual provisions permitting disclosure will not necessarily be determinative, however, and the caution expressed by Deschamps J in *Gomboc* must not be overlooked. In the course of addressing the relationship between the supply company and its customers in that case, Deschamps J said:[99]

---

97 This is subject to the qualification expressed above at n 96, that there might be a reasonable expectation of privacy if the power consumption data was collected or broken down in a way which revealed the intimate details of the occupants' lifestyle in their home.

98 We do not agree with the Chief Justice (below at [189]) that a company's self-interest in detecting theft of its electricity by a customer is irrelevant to the operation of the privacy principles. We do not think it can seriously be suggested that a power company which suspects electricity theft by a customer cannot report that to the police without breaching the privacy principles.

99 *Gomboc*, above n 78, at [33].

> That [the supply company] was at liberty to disclose the information weighs heavily against giving the asserted expectation of privacy constitutional recognition. However, in view of the multitudinous forms of information that are generated in customer relationships and given that customer relationships are often governed by contracts of adhesion (while noting that in this case Mr. Gomboc was at liberty to prevent the disclosure but did not elect to do so), there is every reason for proceeding with caution when deciding what independent constitutional effect disclosure clauses similar to those [in issue] may have on determining a reasonable expectation of privacy.

Cromwell J, delivering the judgment of the Supreme Court in *Spencer*, reaffirmed these points.[100]

[69] In the present case, all three power supply companies had privacy policies:

(a) The Contact Energy policy said that the company would "keep your personal information secure and it'll be held by us in our customer database in accordance with the Privacy Act 1993 and as set out in our energy supply agreement".[101] When outlining the circumstances in which personal information would be disclosed, the policy referred to releasing personal information in various circumstances including "if we're legally required to".

(b) The Genesis Energy policy said that the company held information "in accordance with the Privacy Act 1993 and in particular, the Privacy Principles contained in that Act". It went on to say that the company would not disclose personal information to third parties "except in accordance with the strict exceptions contained in the Privacy Act, or where authorisation has been given by you for that disclosure".

(c) The Meridian Energy policy said the company would collect personal information but would not use or disclose it "except for purposes set out in this privacy policy, or as allowed by the Privacy Act". Later the policy stated that information might be disclosed "if we believe that

---

100 *Spencer*, above n 87, at [54].

101 We were not provided with a copy of the energy supply agreement, so we do not know whether it contained relevant clauses and, if so, what they provided.

> the … disclosure is reasonably necessary to assist a law enforcement agency".

[70] All three policies stated that personal information would be held in accordance with the Privacy Act and referred to the possibility of disclosure – the Contact Energy policy to disclosure if legally required, the Genesis Energy policy to disclosure in accordance with the Act and the Meridian Energy policy to disclosure to law enforcement agencies. The latter two policies, then, identified the possibility that customer information could be disclosed in accordance with the Privacy Act, which includes principle 11(e). However, the statement in the Contact Energy policy that the company would release information "if we're legally required to" is problematic. The Privacy Act does not require those holding information to comply with police or other requests for information, even legitimate requests.[102] More importantly, the "if we're legally required to" language may well suggest to a reasonable consumer that the company would release customer information only in response to a production order or a search warrant, which is not what happened in this instance.

[71] The fact that two of the policies contemplated disclosure in accordance with the Privacy Act might suggest that Mr Alsford's expectation of privacy in his customer data was not "reasonable", at least in circumstances where there was compliance with the Privacy Act's requirements – he ought to have been aware that the information could be released. On the other hand, the fact that one of the policies suggests that disclosure would only be made pursuant to a production order or similar process points in the opposite direction. When these points are considered against the background that caution must be exercised when assessing the impact of customer contracts in this context, the nature of the contractual arrangements does not advance matters much, if at all.

[72] Overall, we consider that Mr Alsford did not have a reasonable expectation of privacy in the particular power consumption data at issue.

---

[102] Law Commission *Review of the Privacy Act 1993* (NZLC IP17, 2010) at [12.25].

Conclusion

[73] By way of summary:

(a) The enactment of the production order regime did not mean that the police were not entitled to ask the power suppliers to provide information as to power consumption at the properties on a voluntary basis.

(b) Whether the power consumption information was obtained consistently with, or in breach of, the Privacy Act may be relevant to whether it was obtained improperly in terms of s 30(5) of the Evidence Act and/or to the balancing process under s 30(2) but will not be determinative.

(c) Where the police seek information from service providers about customers on a voluntary basis, they must not infringe s 21 of NZBORA.

(d) In considering whether s 21 has been infringed, the first question to be determined is whether the information in issue was obtained as a result of a "search". The answer depends first, on whether the person concerned in fact had an expectation of privacy in relation to the information and second, on whether any such expectation was reasonable. If it is determined that there was a "search", the second question under s 21 arises – was the search "unreasonable"?

(e) We consider that Mr Alsford did not have a reasonable expectation of privacy in the particular power consumption information obtained in this case.

[74] The consequence is that the police were entitled to use the power consumption information, and any inferences that could fairly be drawn from it, in the applications for the production order and later the search warrants.

2010 search

[75] As we have said, the information obtained as a result of the illegal 2010 search was referred to in the application for a production order in respect of Mr Alsford's mobile phone data. The texts obtained as a result of the production order were a substantial basis for the search warrant applications.[103] Mr Eaton argued that because the 2010 search was unlawful and the information obtained from it was ruled inadmissible, the application for the production order should not have referred to it. If the production order through which the police gained access to the text messages was improperly obtained, it followed that the search warrants were also improperly obtained, given the significance of the text messages to those applications. Consequently, the information obtained as a result of the execution of the warrants was improperly obtained.

[76] There were four essential points to Mr Alsford's submissions:

(a) The police were required to disclose the full circumstances of the 2010 search in the production order application.

(b) Such disclosure was necessary to enable the issuing officer to determine whether or not he or she would permit the police to rely on the information previously ruled inadmissible.

(c) Such inadmissible information could be properly relied upon only in limited circumstances. The issuing officer was required to weigh up the public interest in maintaining the integrity of the justice system against the public interests in the investigation of offending. Generally, reliance will constitute an abuse of process.

(d) In this case, the issuing officer could not properly have allowed the information to be relied upon.

---

[103] The 2010 offending was referred to in the search warrant applications only briefly – there was simply a reference to the fact that Mr Alsford had been charged with "a substantial indoor cannabis grow at 116 Baker Street in 2010".

[77] To examine this issue, we must first set out more of the background. In the application for the production order, Detective Simpson described the background to the 2010 search in the following way. He said that the police had received an anonymous letter on 21 April 2010, which stated:

> Greg ALSFORD has two houses. He lives mostly at his house in Pannell Ave, at his house in Baker Street he has a major hydroponic dope growing set-up in the garage on the rear of the property. He boasts of making upwards of $150,000 per annum.

[78] Detective Simpson said the police followed up on the letter by making enquiries, which showed that Mr Alsford was connected to the Baker Street address. He said that three police officers had gone to that address and then described what happened as follows:

> They subsequently conducted a search pursuant to section 18(2) of the Misuse of Drugs Act 1975 and located, in the garage at the address, a sophisticated hydroponic cannabis set-up. The internal walls had been lined, extractor fans installed with fluorescent lighting ballasts, heat lamps and light shades. A water pumping system with chemicals and fertilisers was also located.
>
> Fifty snap-lock bags each containing one ounce of cannabis plant material were located along with 49 healthy cannabis plants.
>
> [Mr Alsford] was spoken to at 116 Baker Street by Detective Kelvin YEADON. [Mr Alsford] gave his address as 1/21 Pannell Avenue, his occupation as self-employed electrician …, and his cell phone number as … . [Mr Alsford] admitted to setting up the cannabis growing operation and selling it for $250.00 per ounce, only to respectable friends who are adults.
>
> [Mr Alsford] was charged with Cultivation of Cannabis and Possession of Cannabis for Supply. Both charges were subsequently dismissed in the Christchurch District Court on 14 September 2010 due to the search being deemed unlawful.

[79] In his decision ruling the information obtained from the 2010 search inadmissible, Judge MacAskill provides a fuller account of what occurred after the receipt of the anonymous tip-off:[104]

> [4] … [Detective Sergeant Fabish] drove past the Baker Street address with Senior Constables Miller and Payne. He noted a garage at the rear of the property and that a van was parked in front of the newer garage at the front of the property. It appeared to him that someone was at home. He decided to adopt a direct approach and to go to the door and confront the

[104] *Alsford* admissibility judgment (DC), above n 4.

> occupier with the information provided by the anonymous informant. After a diversion for lunch, about 30 minutes after the initial drive-by, the officers returned to the property.
>
> [5] There was no reply from the front door. DS Fabish still thought it likely that someone was home. The three officers walked down the southern side of the property. A high gate barred their way. It was topped by nails. It was bolted from the other side. The bolt could not be reached. One of the officers climbed over the gate in order to unbolt it from the other side. The officers then approached the back door. There was no response to DS Fabish's knock.
>
> [6] While he was at the back door, DS Fabish noticed a large plywood sheet covering the side of the rear garage. It had holes which he thought might be ventilation holes. The three officers approached the garage. DS Fabish could hear the hum of what he thought was a fan inside the garage. He could smell cannabis when standing beside the garage.
>
> [7] DS Fabish then decided to execute a search without warrant pursuant to section 18(2) of the Misuse of Drugs Act 1975. He gained entry to the garage by forcing the door. When he looked inside the door he could see lights and cannabis plants. He asked the constables to remain at the address while he returned to the New Brighton police station to prepare an application for a search warrant.
>
> [8] Before he could complete the application, he received a phone call from SC Payne who advised that the defendant had arrived home. DS Fabish then returned to Baker Street and spoke to the defendant. He explained that he had visited the address to enquire about the alleged cultivation of cannabis and had invoked section 18(2) to conduct a search without warrant. He was preparing an application for a search warrant when the defendant arrived home. The defendant consented to the continuation of the search and to the seizure of the cannabis equipment rather than to require the police to proceed with the application for a search warrant.

The Judge described the conduct of the police as involving a "blatant trespass",[105] a "serious intrusion" on the defendant's right to privacy and to be free from unreasonable search and seizure[106] and a "blatant disregard of the defendant's rights".[107]

[80] As can be seen, the account given in the production order application is somewhat anodyne by comparison to the circumstances as described by Judge MacAskill.

---

105 At [12].
106 At [15](a).
107 At [15](b).

[81] At this point, it is important to reiterate that Mr Alsford received a remedy for the infringement of his rights as a result of the illegal search of his property in 2010 by means of the exclusion of evidence obtained as a consequence of it, which meant that the prosecution against him could not proceed. This case is, therefore, not like the usual case where the illegally obtained evidence is obtained in the course of an investigation leading to a current prosecution and there is an issue as to what remedy, if any, there should be for the infringement in the context of that prosecution. Most of the authorities fall into this latter category, and are accordingly of limited assistance.

[82] An exception is *R v Saggers*.[108] There the police officer applying for a search warrant referred to information obtained in a warrantless search several years earlier, not realising that the search had subsequently been ruled to be unlawful. In the circumstances, it was unnecessary for the Court of Appeal to reach a final view on the point, but the Court did say that there was no "blanket rule rendering inadmissible evidence discovered following an illegal or unreasonable search".[109] The Court went on to say:[110]

> … we would certainly discourage police from using information previously ruled inadmissible in search warrant applications. If police were to include such material, they would need to provide sufficient material (including the decision ruling the information inadmissible) so that the issuing officer was able to form a properly considered view as to whether the information should be taken into account on the search warrant application. This is likely to lead to so much extra work on the police's part that, in our opinion, their working rule should be: if information has previously been ruled inadmissible, don't include it.

[83] As can be seen, the Court of Appeal in *Saggers* indicated that if the police wished to rely on information that has previously been ruled inadmissible in seeking a search warrant they should provide enough detail of the background to enable the issuing officer to consider whether it could properly be relied upon, including a copy of the decision ruling the search unlawful. However, as Judge Neave noted,[111] this approach creates a problem. Most search warrant applications are determined by registrars or deputy registrars of the District Court who are not well placed to

---

108 *R v Saggers* [2009] NZCA 164.
109 At [36].
110 At [38].
111 *Alsford* (DC), above n 5, at [27](c) and [28].

consider the balance of interests involved in the decision whether or not the police should be permitted to rely on inadmissible information; but it will not always be practicable to place applications raising this issue before judges.

[84] To avoid this problem, it is necessary to have either a blanket rule prohibiting any use by the police of information previously ruled inadmissible or some mechanism other than the application for a production order or warrant that will enable an assessment to be made as to the consequences of the use of inadmissible information. The Crown argued that the appropriate course is that:

(a) the police be permitted to utilise information previously ruled inadmissible in an application for a production order or search warrant;

(b) if the subsequent search produced material which the Crown wished to use as evidence in a prosecution, the court could consider in the context of that prosecution how the use of the inadmissible information in support of the particular application should be addressed, by means of a s 30 analysis in relation to the material obtained; and

(c) this would enable a response to the use of the inadmissible information which is proportionate given all the circumstances.

[85] It is well accepted that the police may refer to material that would not be admissible as evidence at trial to support a reasonable belief sufficient to justify the issue of a search warrant.[112] However, the authorities deal with information that was inadmissible because it was, for example, hearsay or provided by unknown or unnamed informants. The present case is different, because the inadmissibility arose from breaches by the police of Mr Alsford's protected rights in an earlier investigation. The argument is that having been ruled inadmissible on account of

---

[112] See for example, *Auckland Medical Aid Trust v Taylor* [1975] 1 NZLR 728 (CA) at 735 per McCarthy P (hearsay); *Rural Timber Ltd v Hughes* [1989] 3 NZLR 178 (CA) at 183 (hearsay); and *R v Sanders* [1994] 3 NZLR 450 (CA) at 460 and 462 per Fisher J.

police misconduct, the information should not be able to be relied on by the police in a subsequent investigation leading to criminal proceedings.

[86] We consider that a blanket prohibition on the use by the police of information that has been ruled inadmissible in an earlier proceeding is both unjustified and unrealistic. It is unjustified for four reasons.

[87] First, in many cases (as in this), the defendant will already have obtained a remedy for the infringement of his or her rights. It is not axiomatic that a further remedy is required in every instance. (Equally, of course, is it not axiomatic that a further response is never required.)[113]

[88] Second, a blanket rule would effectively require the police either to destroy or to quarantine and ignore information that has been ruled inadmissible. But the police have a legitimate intelligence-gathering function, and obtain information from a wide variety of sources of varying reliability and importance. In some situations, the intelligence derived wholly or partly from inadmissible information may prove to be vital in enabling the police to resolve subsequent serious offending.[114] It is not at all clear from a policy perspective that the police should be required, as a matter of course, to avoid any reliance on information that has been ruled to be inadmissible no matter how reliable and important it may be.

[89] Third, a blanket rule would take no account of the particular role of inadmissible information on the later occasion when it is used. In the present case, for example, the police received an anonymous tip-off in 2012. That tip-off might have been malicious or genuine. Enquiries enabled the police to confirm the accuracy of some of the information provided, but the corroborative material did not link Mr Alsford to drug offending. The information from the 2010 search did provide a link, however, and so provided substantial support for the informant's allegations. It seems to us important that an approach be taken to the issue of

---

113 As was said in *Marwood*, above n 1, the fact that there has been a remedy is relevant to the proportionality analysis contemplated by s 30, albeit that it is not determinative: at [50]–[52] per William Young J for himself, Glazebrook, Arnold and O'Regan JJ.

114 It is, of course, possible that inadmissible information may *exculpate* a potential suspect in relation to subsequent suspected offending.

subsequent police reliance on inadmissible information that takes account of the different uses to which such information may be put.

[90] Finally, a blanket rule would not adequately recognise the nature of the process that leads to inadmissibility rulings. Section 30(2) requires a judge determining the admissibility of impugned evidence to decide:

(a) whether, on the balance of probabilities, the evidence was improperly obtained; and

(b) whether the exclusion of the evidence is proportionate to the impropriety.

The proportionality assessment is carried out by means of "a balancing process that gives appropriate weight to the impropriety and takes proper account of the need for an effective and credible system of justice".[115] Section 30(3) sets out various factors to which the judge may have regard for the purposes of the balancing process.

[91] In cases where it has been held that evidence has been improperly obtained, a number of disparate factors go into the balancing process, with the result that particular features are likely to assume greater or lesser importance in different contexts. Accordingly, a decision that particular improperly obtained evidence is inadmissible in one context will not necessarily mean that the same evidence should be ruled inadmissible in a different context. The contextual nature of admissibility analysis means that it is not appropriate, at the level of principle, to treat evidence that has been ruled inadmissible in one context as being necessarily inadmissible in all other contexts. For example, if improperly obtained evidence is ruled inadmissible in the context of a prosecution for a minor offence but turns out to be relevant to a more serious offence that comes to light later, the balancing process will not necessarily be the same in respect of the second offence as it was in relation to the first. As the Court of Appeal said in *Clark v R*, the s 30 analysis is

---

115 Evidence Act, s 30(2)(b).

"proceeding-specific",[116] a point illustrated by *Hamed*, where there were different outcomes depending on the nature of the charges.[117]

[92] In the present case, of course, the issue before the Court is not the admissibility of the information illegally obtained in 2010 but the admissibility of the evidence obtained as a result of the production order and search warrants, the applications for which relied to a greater or lesser extent on the illegally obtained information. The proceeding-specific nature of the balancing process means that in most cases it will be inappropriate to consider whether the police may properly rely upon the illegally obtained information at the time a production order or warrant is issued. That consideration is better undertaken later in the process, in the context of an extant prosecution (if one is instituted). We consider that this provides a more realistic context for the assessment of all relevant factors. That said, we accept that there may be cases where the inadmissible information is obtained in such extreme circumstances that reliance on it for any purpose would obviously be abhorrent (as where the information was obtained by torture or threats of violence, for example). But absent this type of extreme situation, the assessment is best made in the context of a s 30 analysis of whether the material obtained as a result of the process at issue (whether a production order or a warrant) should be admitted in any subsequent prosecution.[118]

[93] It follows that we do not agree with the Court of Appeal's suggestion in *R v Saggers* that where the police rely in a search warrant application on information that has previously been ruled inadmissible, they should attach a copy of the judgment containing the inadmissibility ruling.[119] We think that is unrealistic. Rather, the police should identify the fact that they are relying on information that has previously been ruled inadmissible and should briefly indicate why the information was held to have been improperly obtained. The issuing officer will not

---

116 *Clark v R* [2013] NZCA 143, (2013) 26 CRNZ 214 at [22]. In that case, the Court of Appeal held that evidence which had been ruled inadmissible in one trial could be led in a later unrelated trial as propensity evidence. The fact that the defendant had earlier received a remedy for the breach of his rights was relevant in the s 30 analysis but was not conclusive.

117 *Hamed*, above n 42.

118 There is, of course, no room for a s 30 analysis when deciding whether to allow information previously declared inadmissible to be used in an application for a warrant in a later investigation because the inadmissible information is not being offered in a "proceeding" as defined in s 4 of the Evidence Act, there being no proceeding yet on foot.

119 *Saggers*, above n 108.

be expected to consider the merits of the police reliance on the inadmissible information other than in the extreme situations referred to above.[120] Nor do we necessarily agree with the observation in *R v Saggers* that it is preferable that the police not rely on information that has previously been ruled inadmissible where they have a sufficient basis to obtain a warrant without reliance on it. If the police have in fact relied to any significant extent on information that has previously been ruled inadmissible in the course of their investigation, they should disclose that in the application even where they consider that they can justify the issue of a warrant or other process without it.

[94] Turning to this case, the first question is whether the text information obtained by way of the production order was improperly obtained as a result of the use in the application of the information obtained in 2010 and ruled inadmissible. This depends on whether the text information was obtained "unfairly" in terms of s 30(5)(c). In that context, it is relevant to consider how the information that had been ruled inadmissible was used by police. The charges presently faced by Mr Alsford resulted from an anonymous tip-off. The police were able to verify many of the details given by the informant by way of further enquiries. The particular value of the inadmissible information was that it supported the informant's account by establishing a clear link between Mr Alsford and cannabis growing. Rather than being a trigger for the investigation in 2012, the inadmissible information served a secondary corroborative function in relation to legitimately obtained information, albeit that the function was an important one.

[95] While the breach of Mr Alsford's rights in 2010 was serious, involving a trespass onto his property, we do not see the inadmissible information as having been obtained in such egregious circumstances that it could not be used by the police for any purpose, as would be the case where information was obtained by torture or threats of violence, for example. Rather, we see the information as falling within the category of general intelligence which the police are entitled to collate over time and to rely on if necessary. Of course, if there was any indication that the police were consciously or systematically breaching rights in order to obtain what might be described as general intelligence, our analysis would be quite different.

---

[120] Above at [92].

[96] Accordingly, we conclude that the text information was not unfairly obtained as a result of the use by the police of the 2010 information in the application for the production order. This applies also to the evidence obtained as a result of the execution of the search warrants, especially given that the 2010 information played a very limited role in those applications – it was mentioned in passing.

[97] Had we reached the conclusion that the text information was improperly obtained, and that because of the reliance on the text information in the search warrant applications, the information obtained from those warrants was unfairly obtained, we would have found that it should be admitted under the s 30 balancing process. In addition to the inadmissible information being corroborative in nature, we note that the police did disclose in the production order application that the 2010 evidence was inadmissible. Further, as we understand it, the Crown is not attempting to rely on the information that was unlawfully obtained in 2010 as evidence in the present prosecution.[121] Moreover, the evidence obtained by the police as a result of the production order and the search warrants strongly incriminates Mr Alsford. As was the case in 2010, it indicates that he ran a significant cannabis growing operation. That said, this is not the most serious form of drug offending – it is at most moderately significant. Finally, while the breach of his rights in 2010 was serious, Mr Alsford has received a remedy for the breach in that the 2010 prosecution did not proceed. This analysis tends to favour admissibility.

[98] As against that, however, we would have to be satisfied that allowing the police to rely on the 2010 information as they did would not undermine the credibility of the criminal justice system by corroding public confidence in it. As we have said, in some cases, the misconduct that produced the inadmissible information will be so egregious that permitting the police to rely on the information subsequently will be corrosive of the administration of justice in the long term, in that it may suggest that the justice system is prepared to condone serious misconduct on the part of the police (or other state agencies). In addition, there is the risk that

---

[121] If the Crown did seek to rely on the illegally obtained information at trial as, say, propensity evidence, that would raise additional considerations requiring further analysis under s 30 and it may well be that the evidence would not be admitted for that purpose.

allowing the police to rely on the information may suggest that "individual rights count for little".[122] However, in the circumstances of this case, we do not consider that any such risk arises. Permitting the police to use the inadmissible information in the way that they did in this case would not undermine public confidence in the criminal justice system, nor would it undervalue Mr Alsford's rights when assessed against the background of the factors identified above.

[99] In the result, then, we consider that the evidence obtained as a result of the execution of the search warrants is admissible despite the reliance on the inadmissible information in the production order application.

Conclusion

[100] We summarise our views on the use of information which a court has ruled to be inadmissible in earlier proceedings as follows:

(a) If the police have relied to any significant extent on information previously ruled inadmissible in an investigation, they should identify that when applying for a search warrant or similar process even if they consider that they have sufficient material to justify the issuance of a warrant without it.

(b) The police should not rely on inadmissible information that falls into the extreme category noted above.[123]

(c) Where the police rely on inadmissible information in a warrant or similar application, the application should identify the information and briefly indicate the reason(s) that led to the finding of inadmissibility. It is not necessary that a copy of the judgment containing the inadmissibility ruling be attached as the issuing officer will not be expected to consider the merits of the police reliance on

---

122 See *R v Grant* 2009 SCC 32, [2009] 2 SCR 353 at [71] per McLachlin CJ and Charron J, delivering the judgment of themselves, LeBel, Fish and Abella JJ.

123 Above at [92].

the inadmissible information other than in the extreme situations referred to above.

(d) If there is a subsequent prosecution based on evidentiary material obtained wholly or partly as a result of reliance on inadmissible information, the fact that inadmissible information was relied upon should be assessed in the context of an analysis of the evidentiary material sought to be used in the prosecution under s 30 of the Evidence Act.

[101] Finally, for the sake of completeness, we note that it was suggested in argument that the electricity consumption data did not advance matters for the purposes of the production order application as it simply showed uniform electricity consumption across the year at both properties, albeit at a lower than normal level in relation to one of them. However, we consider that, when combined with the other information set out in the application, including in particular the 2010 information, the electricity usage data did contribute to a reasonable suspicion that a cannabis growing operation was occurring. Uniform usage across the year, summer and winter, is not the usual pattern of usage.[124] That and the abnormally low usage supported a reasonable belief that the meter had been bypassed to facilitate a cannabis growing operation.

Decision

[102] For the reasons given, we allow the appeal. The evidence obtained from the searches conducted on 19 December 2012 is admissible at trial. For fair trial reasons, we make an order prohibiting publication of the judgment or any part of the proceedings (including the result) in the news media or on the internet or other publicly available database until final disposition of the trial. Publication in a law report or law digest is permitted, however.

---

[124] We agree with the observation of French J that "[h]aving regard to Christchurch's climate, the absence of any seasonal fluctuation in the readings was significant": see *Alsford* (CA), above n 6, at [89].

ELIAS CJ

[103] The appeal concerns a challenge to evidence the Crown proposes to give at the trial of Gregory John Alsford on charges relating to cannabis cultivation. The evidence was obtained when the police executed search warrants in December 2012 at two houses part-owned by Mr Alsford, at Pannell Avenue and Baker Street in Christchurch.[125] The evidence was ruled inadmissible in the District Court by Judge Neave, in application of s 30 of the Evidence Act 2006.[126] His decision was upheld in a majority decision in the Court of Appeal.[127] The Crown appeals to this Court.

Background to the appeal and summary of approach

[104] The challenge to the evidence obtained on execution of the search warrants arose out of the reliance placed in the search warrant applications on material which had been improperly obtained by the police. Two principal bases of impropriety were put forward.

[105] The first was the inclusion in the applications for search warrants and an earlier application for a production order of information obtained two years previously on unlawful search in breach of s 21 of the New Zealand Bill of Rights Act 1990.[128] Evidence arising out of the unlawful search in 2010 had been excluded at the trial of Mr Alsford for the offending then disclosed, with the result that charges against him were dismissed.[129] The same information obtained in the 2010 search was used by the police in the present investigation first to obtain a production order from Mr Alsford's telephone provider and then, together with the apparently incriminating text messages obtained under the production order, to support the 2012

---

125 A third property was also searched, but the evidence obtained from that search is not at issue in the appeal.

126 *R v Alsford* [2015] NZDC 3489.

127 *R v Alsford* [2015] NZCA 628 (Ellen France P, French and Winkelmann JJ). The decision was by majority, with French J dissenting.

128 Following an anonymous tip-off, three police officers had gone to the Baker Street house. When no one answered their knock, one of the police officers climbed over a high gate and unbolted it from inside, giving access to the property. The officers then conducted a warrantless search of the property and discovered evidence of cannabis cultivation.

129 The evidence obtained in the 2010 search was held by Judge MacAskill to have been obtained in "blatant" breach of law: *Police v Alsford* DC Christchurch CRI-2010-009-6053, 17 September 2010 at [12].

warrant application by providing some substantiation for the anonymous tip-off which had led to the investigation.[130] Without the inclusion of the information about the 2010 cannabis growing operation and without the incriminating text messages (themselves obtained through reliance in the production order application on information obtained in the 2010 unlawful search), there was insufficient information provided in the warrant application to justify the grant of the 2012 warrants.[131]

[106] The second basis of impropriety put forward to justify exclusion of the evidence obtained under the 2012 search warrants was the use in the search warrant and production order applications of information obtained informally by the police from Mr Alsford's electricity service providers as to the consumption of electricity at the two premises. This information had been put forward in support of the applications as indicating a pattern of low and even consumption of electricity. That was said to be consistent with anonymous information provided to the police that the occupier of the premises was bypassing the electricity meter to supply the high intensity lights used in the cannabis cultivation.

[107] Electricity consumption records are personal information within the definition adopted in s 2 of the Privacy Act 1993. Personal information may not be disclosed by an agency holding it unless the disclosure falls within one of the exceptions to the stated principle of non-disclosure.[132] It was argued in the Courts below that the electricity consumption information was obtained by the police from Mr Alsford's electricity suppliers in breach of the provisions of the Privacy Act because none of the exceptions (and in particular the exception contained in paragraph (e)(i) of principle 11 which relates to disclosure necessary to avoid prejudice to the maintenance of law) applied. It was argued that the police should have sought a production order for the electricity records instead of obtaining them

---

130 The application for the production order set out the information obtained from the 2010 search in detail, whereas the search warrant applications recorded that Mr Alsford had previously "been charged with having a substantial indoor cannabis grow" at the Baker Street address.

131 Judge Neave held that the information obtained in the 2010 unlawful search was improperly included and that without it neither the production order nor the search warrants could have been granted: *R v Alsford* [2015] NZDC 3489 at [71]–[72]. This was upheld by the majority of the Court of Appeal: *R v Alsford* [2015] NZCA 628 at [76] per Ellen France P and at [94] per Winkelmann J (agreeing with Ellen France P).

132 The information privacy principles are found in s 6 of the Privacy Act 1993.

informally from the providers. As a result, it was said that the production order by which the text messages were obtained, and therefore the text messages themselves, were improperly obtained for breach of the Privacy Act as well as because of the inclusion of material obtained by the unlawful 2010 search.

[108] In the District Court and Court of Appeal the evidence obtained on execution of the search warrants was excluded under s 30 of the Evidence Act because it was held that the use of the 2010 unlawful search was improper and, without it, the warrants were not justified. The exclusion of the evidence obtained was accepted in the District Court and Court of Appeal to be proportionate to the impropriety.

[109] In the District Court, Judge Neave took the view that the impropriety in the use of the 2010 search material might have been overcome if the police had followed a suggestion made in the Court of Appeal in *R v Saggers.*[133] In *Saggers* it was suggested that applications for search warrants which rely on information previously ruled inadmissible in other proceedings should include "sufficient material (including the decision ruling the information inadmissible) so that the issuing officer is able to form a properly considered view as to whether the information should be taken into account on the search warrant application".[134] Although the applications had indicated that the evidence obtained under the 2010 search had been "deemed unlawful", Judge Neave thought that to be insufficient compliance with the *Saggers* direction to put the previous determination on admissibility before the issuing officer.[135]

[110] In the Court of Appeal, the majority did not rely on failure to comply with the *Saggers* direction and Winkelmann J indicated doubt about its practicality.[136] (French J, in dissent, took the view that, though *Saggers* had not been complied with, enough information had been provided to the issuing officer that the omission did

---

133 *R v Saggers* [2009] NZCA 164.

134 The Court considered such use was to be discouraged and thought that the suggestion of inclusion of the information to enable the issuing officer to form a "properly considered view as to whether the information should be taken into account on the search warrant application" would operate to discourage its inclusion by leading to much "extra work" for the police: at [38].

135 *R v Alsford* [2015] NZDC 3489 at [70].

136 Winkelmann J considered that the approach taken in *Saggers* would have to be reconciled with s 30 of the Evidence Act 2006 and the pre-existing common law: *R v Alsford* [2015] NZCA 628 at [97]. She was sceptical of the practicality of the issuing officer, often a registry officer rather than a judge, being asked to undertake the assessment suggested.

not make "any difference to the outcome".[137]) Ellen France P, for herself and Winkelmann J, held that the 2010 breach had amounted to "blatant abuse" of process. The information was "tainted" by the abuse and its inclusion in the applications for the production order and search warrant was improper.[138] In applying the balancing required by s 30 of the Evidence Act, Ellen France P agreed with the analysis in the District Court.[139] She did not accept that the Crown submission that the previous breach had been remedied by the earlier exclusion was sound, because "the circumstances of that breach must be relevant to the nature of the impropriety".[140] It was not a question of punishing the police but "rather, reflecting the importance of the right infringed and the seriousness of the infringement". Ellen France P considered that the Judge was right to conclude exclusion was a proportionate response to the impropriety.

[111] Neither the District Court nor the Court of Appeal found it necessary to determine whether the electricity records had been obtained in breach of the Privacy Act.[141] They considered that the information obtained from the electricity providers was insufficiently linked to the criminal offending in issue to be material on the questions of validity of the search warrants and production order.[142]

[112] In what follows I explain why I agree with the decision in the Court of Appeal and would dismiss the appeal. I consider the Court of Appeal was right not to adopt the approach taken in the District Court in application of *Saggers.* The question of admissibility must be determined as one of admissibility in the present proceedings. It does not turn on whether the officer who granted the search warrant or production order was provided with sufficient information about the impropriety entailed in collection of the information used in the application, but rather whether the improperly obtained material tainted the new evidence obtained through its further use requiring exclusion of the new evidence in the present case. In this approach, I am in substantial agreement with the other members of this Court

---

137 At [91].
138 At [70].
139 At [81].
140 At [82].
141 *R v Alsford* [2015] NZDC 3489 at [52]–[54]; and *R v Alsford* [2015] NZCA 628 at [57].
142 *R v Alsford* [2015] NZDC 3489 at [56]–[65]; and *R v Alsford* [2015] NZCA 628 at [46].

(although I would not treat disclosure of impropriety to the issuer as relevant to the s 30 assessment, as is suggested at [97]).

[113] I depart from the other members of the Court however in being of the view that the Court of Appeal majority decision was right to hold that the use in the warrant and production order applications of the information obtained in the unlawful 2010 search was improper.[143] If it had not been included, there was no basis on which the search warrants could lawfully have been granted. I agree, too, with the reasons given by the Court of Appeal for holding that the exclusion of the evidence obtained under the search warrants was the correct response.[144]

[114] I agree with the Court of Appeal that the information about the electricity consumption obtained from the electricity providers informally was immaterial to the question of admissibility of evidence.[145] It is therefore unnecessary for me to resolve the question whether the information was obtained in breach of the Privacy Act. The question of the lawfulness of the police conduct in obtaining the information was however further developed on appeal, in response to the issues identified in the leave judgment which included "whether the electricity consumption records were improperly obtained from the service provider".[146] The Privacy Commissioner has intervened on the point. The matter is one that arises on the view taken by the other members of the Court that the electricity consumption data contributed to the basis for the reasonable suspicion of criminal offending justifying the production and search warrants, albeit in combination with the other information (and in particular the 2010 unlawfully-obtained information, which they consider was properly relied on).[147]

[115] Because the point is addressed by the other members of the Court, I indicate why I would hold that the electricity consumption records were unlawfully obtained, in breach of the Privacy Act. This matter is one of some complexity and difficulty. It is also of considerable practical importance in the investigation of criminal

---

143 *R v Alsford* [2015] NZCA 628 at [70]–[75] per Ellen France P.
144 At [79]–[82].
145 At [46] and [57].
146 *R v Alsford* [2016] NZSC 21.
147 See above at [101][110].

offending. It is unfortunate that it has been considered in a context in which we have not had the benefit of reasons in the Courts below. Even on the view taken by the other members of the Court (in which the electricity records buttress the 2010 information),[148] it is something of a make-weight in considering the propriety of use of the 2010 information, the principal matter on which the appeal turns.

[116] The issues in the appeal are at the intersection of three important Acts: the Privacy Act, the Evidence Act and the Search and Surveillance Act 2012. In what follows I explain why I consider the meaning and application of the Privacy Act now falls to be determined in the context of the two later Acts, particularly the Search and Surveillance Act which itself has the purpose of achieving better balance between the Privacy Act and police investigation of crime.[149]

[117] The Search and Surveillance Act provides for compulsory production of information under production orders and compulsory powers of search under search warrants, both on an issuing officer being satisfied that there are reasonable grounds to suspect that an offence has taken place and to believe that material evidence will be obtained.[150] The Act covers not only compulsory production orders and search warrants but also regulates "consent" searches.[151] It is not necessary for such consent searches to be undertaken on the basis of the reasonable belief necessary to obtain production orders or search warrants. But regulation of consent searches suggests some caution about voluntary disclosure of information or material on request. Because of the change in the legislative background, I consider that cases decided on the application of the Privacy Act before enactment of the two later statutes have to be treated with some care. The wider legislative scheme which now provides the context for application of the Privacy Act is why I would not follow the decisions of the Court of Appeal in *R v Thompson*,[152] *R v Harris*[153] and *R v Cox*,[154]

---

148 Above at [101].
149 Search and Surveillance Act 2012, s 5.
150 Sections 6 and 72.
151 Sections 91–96.
152 *R v Thompson* [2001] 1 NZLR 129 (CA).
153 *R v Harris* [2000] 2 NZLR 524 (CA).
154 *R v Cox* (2004) 21 CRNZ 1 (CA).

cases referred to by the majority in this Court[155] and relied upon by French J in her dissent in the Court of Appeal.[156]

[118] The majority in the Court of Appeal did not come to any final conclusion on a submission that the requests to the electricity companies for information about consumption and the subsequent disclosure of the information by the providers were unlawful. That was both because Judge Neave had not made findings on the point and because they considered it was possible to resolve the appeal without determining it.[157] Ellen France P (with whom Winkelmann J agreed) indicated reservations however about the Crown's reliance on the view taken in *Thompson*[158] that the information fell within the exception in principle 11(e)(i) of the Privacy Act as disclosure "to avoid prejudice to the maintenance of the law".[159] She considered that it was not clear that *Thompson* remained good law following enactment of the Search and Surveillance Act, given its purpose in balancing the needs of investigation of offences with the rights affirmed in the New Zealand Bill of Rights Act and the Privacy Act and given the specific authority given to obtain production of information, "which indicates that route should be used". In addition, Ellen France P questioned whether the information provided to Genesis Energy (one of the providers), which was not specific as to the offence under investigation, was "sufficient to invoke the relevant privacy principle".[160]

[119] In my view, the police are able to access personal information protected by the Privacy Act only when acting under statutory powers (such as those found in the Search and Surveillance Act) or in circumstances falling within the exceptions to the information privacy principles. I do not accept that the request by the police to the electricity providers came within the exception contained in principle 11(e)(i) of s 6 of the Privacy Act for "non-compliance … necessary … to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention,

---

155 See above at [23]–[26] and [51]–[52].
156 *R v Alsford* [2015] NZCA 628 at [90].
157 *R v Alsford* [2015] NZCA 628 at [57] per Ellen France P, with whom Winkelmann J agreed.
158 *R v Thompson* [2001] 1 NZLR 129 (CA) at [54].
159 *R v Alsford* [2015] NZCA 628 at [54].
160 At [56].

detection, investigation, prosecution, and punishment of offences".[161] In this conclusion I differ from the other members of the Court.

[120] For the reasons developed in what follows, I agree with the reservations expressed by Ellen France P and consider that the exception in principle 11(e)(i) (for disclosure necessary to avoid prejudice to the administration of justice) has not been made out. I am unable to agree with the view of the majority that advice that the personal information sought is relevant to a police inquiry into specific offending is sufficient to bring the request for non-compliant disclosure within the exception for non-compliance "necessary to avoid prejudice to the maintenance of the law" (including in "the prevention, detection, investigation, prosecution, and punishment of offences"). Against the powers of compulsory disclosure in the Search and Surveillance Act, no basis is disclosed as to why non-compliant informal disclosure was "necessary" in this case to avoid prejudice to the investigation.

[121] The electricity records were therefore obtained unlawfully, in breach of the Privacy Act. I do not agree with the view taken by the other members of this Court that s 11(2) of the Privacy Act precludes evidence collected in breach of the information privacy principles being unlawfully obtained in terms of s 30 of the Evidence Act.[162]

[122] Since I take the view that the evidence obtained through the search warrants was unlawfully obtained, I consider that s 30 of the Evidence Act was engaged. In application of s 30(2)(b), I agree with the lower Courts that exclusion of the evidence is proportionate to the impropriety involved in its collection.

[123] Because of the view taken by the other members of the Court that impropriety in the obtaining of evidence cannot be established by breach of the privacy principles but must be addressed under s 21 of the New Zealand Bill of Rights Act[163] (an analysis I do not adopt), it is necessary for me to express reservations about the restriction of "search" under s 21 to conduct which invades a "reasonable expectation of privacy". If I had found it necessary to decide the matter

---

161 See below at [136] and following.
162 See below at [161]–[174]; and compare above at [37]–[40] and [47].
163 See above at [47].

under s 21 of the New Zealand Bill of Rights Act, I am provisionally of the view that the request by the police to the electricity providers constituted unreasonable search and seizure when considered in the context of the Privacy Act's prohibition on the disclosure and collection of personal information and the context provided by the scheme of the Search and Surveillance Act.

Use of the material obtained in the 2010 search meant the evidence was "improperly obtained"

[124] Judge MacAskill held that the evidence excluded in the 2010 proceeding was obtained through "blatant trespass" and was a "serious intrusion" and in "blatant disregard of the defendant's rights".[164] I agree with that characterisation of what happened and that it amounted to an abuse of process, as Ellen France P considered it to be.[165] It was a deliberate and flagrant trespass entailing intrusion into a domestic property with no lawful authority. It was rightly treated as a breach of s 21 of the New Zealand Bill of Rights Act.

[125] I do not agree with suggestions made in argument that the breach of rights was "vindicated" by the exclusion of evidence obtained in the 2010 prosecution. The correct characterisation is not that exclusion of the evidence was "vindication" or remedy for the undoubted breach of fundamental rights, but that the evidence obtained as a result of such breach was excluded on the basis that such exclusion was not disproportionate to the impropriety. The question in the present appeal is whether the evidence obtained under the search warrants and production orders which were justified by the same material obtained in breach of s 21 of the New Zealand Bill of Rights Act is evidence that is improperly obtained and ought to be excluded.[166] In *Marwood v Commissioner of Police* the majority considered that the fact that evidence had previously been excluded was relevant in considering its admissibility in a subsequent case.[167] In my concurring opinion I took the view that the question of admissibility in subsequent proceedings should be considered on its

---

164 *Police v Alsford* DC Christchurch CRI-2010-009-6053, 17 September 2010 at [12] and [15].

165 *R v Alsford* [2015] NZCA 628 at [70].

166 For discussion on the tainting of evidence by prior law enforcement misconduct, see *R v Shaheed* [2002] 2 NZLR 377 (CA) at [6]–[14] per Elias CJ, at [157]–[163] per Blanchard J (delivering the reasons of Richardson P, Blanchard and Tipping JJ), at [174]–[181] per Gault J, at [193] and [195]–[198] per McGrath J and at [204]–[206] per Anderson J.

167 *Marwood v Commissioner of Police* [2016] NZSC 139 at [50]–[51].

merits, without any preconception derived from the outcome in the earlier proceedings, whether it was to admit or exclude evidence.[168] I remain of that view. While in this case the other members of the Court do not treat earlier exclusion of evidence as more than a relevant consideration in assessing exclusion of evidence in subsequent proceedings, I do not agree with them that the s 30(2)(b) balancing process should take into account that Mr Alsford "received a remedy" in the earlier proceedings.[169]

[126] The information obtained in the unlawful entry in 2010 remains information which was improperly obtained in what the lower Courts have accepted was a flagrant and deliberate breach of rights. I agree with the Court of Appeal that its use to obtain the production order which obtained the incriminating text messages and the search warrant which obtained the evidence of cultivation was itself improper. I consider that the use in this way of information obtained in serious breach of rights was wrong. It was deliberate use in judicial process of information known to have been unlawfully obtained in flagrant breach of rights. No circumstance to justify the use of such tainted information has been put forward. I consider that the Court of Appeal was right to hold that its exclusion was proportionate to the impropriety.

[127] I agree with Judge Neave and the majority in the Court of Appeal that there was insufficient justification for the production order and the search warrants if the information obtained in the earlier unlawful search in 2010 is put to one side. As the District Court and the Court of Appeal were agreed, the anonymous tip-off "on its own, would not have justified any form of search warrant".[170] In addition to its other inadequacies, I agree with Judge Neave that the currency of the information and the accuracy of the source were questionable.

[128] In the Court of Appeal, Ellen France P (for herself and Winkelmann J) agreed that Judge Neave had been correct to take the view that the information obtained through the anonymous tip-off, even after further police enquiries established that the person in issue was the respondent (by linking him to the address), was

---

168 At [67].
169 Compare above at [97].
170 *R v Alsford* [2015] NZDC 3489 at [65].

insufficient on its own to establish a basis for the production order.[171] Although the Judge had made some factual errors in considering the significance of the information about electricity consumption, Ellen France P considered that the Judge had been right to take the view that "not a lot" could be taken from the figures.[172] The consumption was accepted by the police witness to be "not far below" the national average and there was in any event no clarity about how many people were living at each address and therefore whether the assumption (based on a three bedroom home in which five people were living) was accurate. I agree with these conclusions.

[129] I do not agree that the information obtained in 2010 was mentioned only "in passing" in the search warrant applications and "played a very limited role".[173] The mobile phone data obtained through the production warrant may have been sufficient to found a search warrant application, but as Ellen France P pointed out "that information only came to hand because of the production order" which could not have been granted on the material provided without the 2010 information.[174] I consider the warrants were defective and the evidence obtained during their execution was improperly obtained.[175] I would dismiss the appeal and exclude the evidence obtained.

[130] These are the reasons on which I would dispose of the appeal. As has been explained, however, because of the different view taken by the other members of the Court and because I have serious reservations about their approach, it is necessary for me to deal with the question of breach of the Privacy Act principles and s 30 of

---

171 In dissent in the Court of Appeal, French J was prepared to treat the anonymous information that started the inquiry as providing some support for the warrants because it was "independent" of the illegally obtained 2010 evidence: *R v Alsford* [2015] NZCA 628 at [87]. I do not think however that answers the point unless the anonymous information was credible enough to support the applications. I agree with the majority in the Court of Appeal that it was not. French J (at [89]) was also prepared to give more weight to the electricity evidence as providing "further support for the credibility" of the informant information (an approach echoed by the majority in this Court above at [99]). But in my view the majority in the Court of Appeal was right to treat the meaning of the electricity consumption information as too uncertain to provide any support for the applications.

172 *R v Alsford* [2015] NZCA 628 at [46].

173 Above at [96].

174 *R v Alsford* [2015] NZCA 628 at [76].

175 Section 107 of the Search and Surveillance Act provides that a search warrant is "invalid" if the information contained in the application does not satisfy the conditions for lawful issue of a warrant.

the Evidence Act. The need to review the legislation means that it is, unfortunately, not possible to be brief.

The Privacy Act 1993

[131] The Privacy Act regulates the collection and disclosure of personal information about individuals. It applies to all personal information, defined in s 2 to mean all "information about an identifiable individual".

[132] The breadth of the definition means that personal information includes information in which the individual can have no reasonable expectation of complete privacy. It may be publicly available, or it may be information the individual has disclosed or shared or knows will come into the hands of others. Customer information held by retailers and service providers with whom the individual deals falls into this last category. The fact that such information is captured and retained by the retailer or service provider is generally understood. It does not however lose the character of personal information under the statute and it is subject to protection under the Privacy Act against unauthorised disclosure.

[133] As the Privacy Commissioner pointed out in his helpful submissions as intervener, the concept of a "reasonable expectation of privacy" is not part of the scheme of the Privacy Act. The Act applies to all types of personal information, whether or not it is sensitive or intimate, and whether or not it is information in which the individual has a "reasonable expectation of privacy". The nature of the interest and what protection it is reasonable to expect for it in the particular context may be significant when considering matters of enforcement under Part 8 of the Act or in the balance required by s 30 of the Evidence Act when determining questions of admission of improperly obtained evidence. But the statutory protection of personal information establishes what may be lawfully obtained or disclosed.

[134] Today, electronic capture and storage of such information and the ease with which it can be shared may greatly extend what is reasonably to be expected in the original sharing of information. Such extended disclosure is potentially destructive of the values of human dignity and autonomy protected by the concept of privacy. Since the concept of privacy is contextual, information which may not appear to be

personal or intrusive in the context in which it is supplied or obtained may well be so in another context. Such considerations are behind the protections on collection and disclosure of personal information under the Privacy Act. Behind the legislation lies international recognition, found in instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, that privacy is a human right.[176]

[135] Privacy interests are protected under the Privacy Act through "information privacy principles", which are stated in s 6.[177] Section 7 of the Privacy Act provides "savings" for other enactments which authorise disclosure or collection or restriction upon the availability of personal information. In particular, s 7(1) provides that nothing in principles 6 or 11 "derogates from any provision that is contained in any enactment and that authorises or requires personal information to be made available" and s 7(4) provides that an action is not a breach of the other principles if it is "authorised or required by or under law". One such source of statutory authority for disclosure is to be found in the Search and Surveillance Act, which provides for search under warrant and supply of information under production order.

[136] In addition to the savings for other enactments, principles 2, 3, 9 and 11 of the Privacy Act are subject to the exceptions contained in the principles themselves.

---

176 *Universal Declaration of Human Rights* GA Res 217A, A/Res/217 (1948), art 12; and International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976), art 17.

177 Principle 1 prevents the collection of personal information by an agency unless it is for a lawful purpose connected with the function of the agency. Principle 2 establishes that personal information may be collected only directly from the individual concerned. Principle 3 requires agencies collecting personal information directly from the individual to ensure that the individual is aware of the collection, the purposes for which it is collected, and the intended recipients of the information. If the collection of the information is authorised or required by or under law the individual must be advised of the law under which it is provided and whether supply of the information by the individual is voluntary or mandatory. Principle 4 prohibits collection of personal information by means that are "unlawful", "unfair" or that "intrude to an unreasonable extent upon the personal affairs of the individual concerned". Principle 5 requires an agency holding personal information to ensure the information is protected by reasonable security standards from loss or disclosure. Principle 6 gives the individual access to the personal information held by an agency concerning the individual and principle 7 gives the individual the right to obtain correction of information which is inaccurate. Principle 8 requires an agency to check the accuracy of the information before it is used. Under principle 9 an agency may not keep information for longer than is required for its lawful purposes. Principle 10 prevents an agency holding personal information for one purpose using it for another. Principle 11 limits the disclosure that can be made of information held by an agency. Finally, principle 12 prevents an agency assigning a "unique identifier" to an individual except under specified conditions. Most of the principles are expressed to be subject to specific exceptions. The exceptions to the principles at issue are discussed below.

They include the exception in principle 11(e)(i), relied upon here, where the agency holding the personal information "believes, on reasonable grounds," that "non-compliance is necessary … to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences".

[137] The scheme and terms of the Privacy Act do not therefore prevent the disclosure under lawful authority of personal information to law enforcement agencies. Such disclosure may be authorised under the provisions of the Search and Surveillance Act or may be disclosed or obtained without breach of the Privacy Act if within the exceptions, including the exception to prevent prejudice to the maintenance of law (including in the detection and investigation of offences). As is described further in what follows, I am of the view that the context provided by the Act does not suggest that the exception to prevent prejudice to the maintenance of law is a hurdle passed if the police simply request disclosure of personal information on the basis that it is relevant to an investigation.[178]

[138] Central to the scheme of protection under the Privacy Act are principles 1, 2 and 6. Principle 1 permits the collection of personal information by an agency only for lawful purpose associated with its function and only if the collection of the information is "necessary" for that purpose. Principle 2 requires personal information to be collected only from the individual unless a number of exceptions apply. Principle 6 confers on the individual concerned an entitlement to confirmation of the information held about him by the agency and to have access to the information and to require correction of errors in it. These principles indicate that informed consent by the individual affected is an important element in the collection and disclosure of personal information.

[139] Principle 11 prevents an agency holding personal information from disclosing it to any person, body or agency unless the agency holding the information "believes, on reasonable grounds," a number of matters comprising distinct exceptions to the general principle. As already indicated, the present appeal concerns the application of the exception contained in principle 11(e)(i) which permits "non-compliance" to

[178] See below at [159].

avoid prejudice "to the maintenance of law" (including in "the prevention, detection, investigation, prosecution, and punishment of offences"). The scope of that exception needs to be considered in the context of the other exceptions to the general principle of non-disclosure. It is to be noted that where the threshold for principle 11(e)(i) is made out release of the information is justified but is not compelled.

[140] Principle 11 and its exceptions, dealing with disclosure, are mirrored by principle 2 which prevents the collection of personal information except directly from the individual concerned, with a number of exceptions to that general principle. They include reasonable belief that the collection of personal information has been "authorised" by the individual or that it is "publicly available". There is a specific exception where "non-compliance is necessary":

> (i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
>
> (ii) for the enforcement of a law imposing a pecuniary penalty; or
>
> (iii) for the protection of the public revenue; or
>
> (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); …

Again, the references to authorisation and belief that the information is publicly available indicate that a policy of the legislation is transparency to the person affected of the collection of personal information. And again the general principle of non-collection of personal information about individuals is subject to specific legislation and to an exception "to avoid prejudice to the maintenance of the law by any public sector agency", in a provision that mirrors the exception for disclosure under principle 11(e)(i).

[141] What is "necessary" to avoid prejudice to the maintenance of the law is a contextual assessment. The context includes that provided by the Privacy Act more generally and general legislation, including the legislative regime for compulsory disclosure or collection of information which ousts privacy values under the savings

provision in s 7 of the Privacy Act. The savings meet legislative priorities such as facilitating law enforcement. Compulsory powers under other enactments, such as the Search and Surveillance Act, have their own built-in safeguards.[179]

[142] In construing the exception in principle 11(e) where disclosure is "necessary" to "avoid prejudice" to the maintenance of law, including in the detection and investigation of offences, the exception provided in principle 11(f) is of relevance. It permits disclosure when necessary "to prevent or lessen a serious threat … to public health or public safety; or … the life or health of the individual concerned or another individual." A "serious threat" is defined in s 2 as:

> … a threat that an agency reasonably believes to be a serious threat having regard to all of the following:
>
> (a) the likelihood of the threat being realised; and
>
> (b) the severity of the consequences if the threat is realised; and
>
> (c) the time at which the threat may be realised.

[143] In the context of the exception in 11(f) (which entails severity and likelihood of a serious threat), I do not think there is any occasion to read down the requirements of exception (e)(i). The scheme of the exceptions to the principles does not suggest that the test of what constitutes necessary avoidance of prejudice to the maintenance of law is "a relatively low one".[180] What is necessary is that the requesting authority indicates why disclosure under the exception, as opposed to disclosure under a production order or search warrant, is "necessary … to avoid prejudice". Some circumstances of urgency would be the obvious example if the purpose is to avoid "prejudice" to an investigation or prosecution. The circumstance that an agency need not accede to a request (because the exception is not a power to compel) supports the view that the exception cannot be invoked whenever the police ask for information to help with an ongoing investigation, because in those

---

179 A judicial officer granting a production order or search warrant must form the view that there are reasonable grounds to suspect that an offence has been committed and to believe that production or search will obtain evidential material in respect of the offence that is in the possession of the person from whom production is sought or in the place to be searched: Search and Surveillance Act, ss 6 and 72.

180 Compare above at [34].

circumstances whether the information is provided will depend on the attitude taken by the holding agency.

[144] An evident policy in the legislation is that individuals should know if personal information about them is being collected and have the opportunity to control its use and obtain correction if it is inaccurate. Secret collection and unauthorised use of personal information undermines these policies and is permitted only where there is good reason. In cases under Part 8 of the Act,[181] the defendant has the onus of proving that his conduct falls within an exception.

[145] The Privacy Commissioner, in his submissions to the Court, pointed out that principle 11(e)(i) is not an empowering provision for law enforcement agency requests for disclosure of information. It does not excuse the law enforcement agency from complying with its obligations as a requesting agency.

[146] The information privacy principles enacted in s 6 apply both to the collection of personal information by the police and to disclosure of such information to the police. Principle 4 deals with the collection of information. It prevents the collection of personal information by an agency:

> (a) by unlawful means; or
>
> (b) by means that, in the circumstances of the case,—
>
> (i) are unfair; or
>
> (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

[147] On the scheme of the Act, I consider that if the police request information from a third party in circumstances which are in breach of principle 11 (perhaps because insufficient information is provided to enable the disclosing agency to form a reasonable belief that the disclosure is permitted), the police would themselves be in breach of principle 4 because the collection would be "unfair". If the agency acts inconsistently with principle 4 by collecting information "unfairly", it is in my view obtaining evidence in breach of an enactment for the purposes of s 30 of the

---

[181] See below at [166].

Evidence Act. In this view, I differ from the narrower interpretation of principle 4 adopted by the other members of this Court at [44]–[45].

The Search and Surveillance Act 2012

[148] In considering the consequential impropriety entailed in the obtaining of personal information in breach of principle 11, the scheme of the Search and Surveillance Act powers bear on the necessity of the disclosure under principle 11(e)(i) and whether exclusion is proportionate to the impropriety under s 30 of the Evidence Act.

[149] The Search and Surveillance Act was enacted to provide better balance between rights of privacy and the public interest in the detection and prosecution of crime. It regulates "consent searches" and authorises search warrants and production orders by which information can be obtained by compulsion. The purposes of the Search and Surveillance Act are set out in s 5. They indicate that it is concerned to facilitate the investigation and prosecution of offences "in a manner that is consistent with human rights". In that connection it "recognises the importance of the rights and entitlements affirmed" in both the New Zealand Bill of Rights Act and the Privacy Act. This cross-referencing to the policies of other Acts is legislative recognition of the wider legislative context for interpretation and application of each.

[150] The policy and scheme of the Search and Surveillance Act calls into question the continued validity of the reasoning in decisions such as that of the Court of Appeal in *Thompson*[182] and *Cox.*[183] The Search and Surveillance Act was enacted to strike a better balance between the interests of law-enforcement and the human rights and privacy interests recognised under the New Zealand Bill of Rights and the Privacy Act. That new balance requires reassessment of earlier assumptions about the lawfulness of "voluntary" disclosure of personal information to the police (and loose statements about civic responsibilities to provide such information). It bears on the "necessity" of non-compliance with the principle of non-disclosure or non-collection "to avoid prejudice to the maintenance of the law".

---

182 *R v Thompson* [2001] 1 NZLR 129 (CA).
183 *R v Cox* (2004) 21 CRNZ 1 (CA).

[151] In *Thompson* the Court of Appeal considered that a request by the police for disclosure of personal information from an electricity company for the purposes of the investigation of offending came within exception (e)(i) of principle 11.[184] There was no consideration in that case of whether the disclosure of information was "necessary" within the meaning of the exception. As the earlier discussion in *R v Wong-Tung* indicates,[185] there was some doubt about whether such "intangible" information could be the subject of a search warrant, which may have had some bearing on assessment of necessity. But, whatever the position then, the Search and Surveillance Act now sets up a scheme of consent searches, production orders and search warrants which provide the modern context against which the "necessity" of non-compliance with principle 11 of the Privacy Act must be considered.

[152] Production orders were introduced as an alternative to search warrants.[186] Enforcement officers may apply for production orders under s 71 of the Search and Surveillance Act instead of applying for search warrants if the conditions specified in s 72 are made out. They require reasonable grounds to suspect the commission of an offence and reasonable grounds to believe that the documents sought will be evidence and are in the possession of the person against whom the order is sought. The issuing officer must be satisfied that the conditions specified in s 72 are made out.

[153] Search warrants may be sought from an issuing officer by application made under s 98. Search warrants require reasonable grounds to suspect the commission of an offence punishable by imprisonment and reasonable grounds to believe that the place to be searched will contain evidential material.[187]

[154] Production orders were introduced as a more efficient and less intrusive means of obtaining documents than by search where there is no reason to expect lack

---

184 *R v Thompson* [2001] 1 NZLR 129 (CA) at [54].
185 *R v Wong-Tung* (1995) 13 CRNZ 422 (CA); see below at n 198.
186 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.24].
187 Search and Surveillance Act, s 6.

of cooperation.[188] The Law Commission suggested that it would be a process suited in particular to obtaining business records, utility use data and telephone records.[189]

[155] Of significance in the present appeal are the provisions made in the Act for "consent searches". They are contained in ss 91–96. These provisions make it clear that search may be undertaken with consent (of the person to be searched or in control of the premises or thing to be searched) even if the enforcement officer does not have the reasonable belief or suspicion necessary for a production warrant or search warrant. The subpart of the Act dealing with "consent searches" does not confer a power of search. Rather, it regulates the circumstances in which an enforcement officer may ask someone to consent to undergo a search or to permit a search. Although the officer need not have the reasonable belief or suspicion necessary for a search warrant or production order, he must determine that the search is for a purpose authorised by s 92. That is to say, the search must be for one of the following purposes:

> (a) to prevent the commission of an offence:
>
> (b) to protect life or property, or to prevent injury or harm:
>
> (c) to investigate whether an offence has been committed:
>
> (d) any purpose in respect of which the enforcement officer could exercise a power of search conferred by an enactment, if he or she held a particular belief or suspicion specified in the enactment.

[156] Before conducting the search by consent, the enforcement officer must advise the person being asked for consent:[190]

> …
>
> (b) … the reason for the proposed search; and
>
> (c) … that he or she may either consent to the search or refuse to consent to the search.

---

188 See (20 March 2012) 678 NZPD 1115; and (22 March 2012) 678 NZPD 1246. The Minister responsible for the Bill, Hon Judith Collins, explained in the House of Representatives that production orders would be used to procure documents from persons "willing to assist".

189 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [10.25].

190 Search and Surveillance Act, s 93.

[157] If a search by consent is made for a purpose other than one prescribed by s 92 or if it is made without advising the person being searched of the reason for the proposed search and that he or she may refuse consent, then the search is unlawful under s 94(a) and (b). It is also unlawful if "the search is undertaken in reliance on a consent given by a person who does not have authority to give that consent".[191]

[158] The regulation of "consent searches" is indication that the concept of consent to search is not treated by Parliament as something informal. It was seen to require controls and protection. Although the point was not taken, it seems to me that it is well arguable that disclosure otherwise than in accordance with the Privacy Act is "unauthorised", even if consented to by the holding agency, and for that reason is an "unlawful" search in terms of s 94 of the Search and Surveillance Act.

Principle 11(e) in the context of the Search and Surveillance Act

[159] Under s 6 of the Interpretation Act 1999, enactments "apply to circumstances as they arise". Against the background of enactment of the Search and Surveillance Act and s 30 of the Evidence Act, I do not think that the uncritical approach formerly taken to exception (e) of principle 11 is defensible. Assessment of whether disclosure is "necessary" for law enforcement purposes must occur in the context of the disclosure regime provided by the Search and Surveillance Act. Ellen France P, with whom Winkelmann J agreed in the Court of Appeal, considered there was "force" in the submission that, following enactment of the Search and Surveillance Act, "that regime should be utilised for the production of this information".[192] I consider that, at the very least, provision of the personal information cannot be shown to be "necessary" for law enforcement purposes unless there are circumstances, either of urgency or otherwise, which prevent application for a production order or search warrant.

[160] This is not to accept completely the submission of the respondent that the provision of production orders in the Search and Surveillance Act prevents the police obtaining information from third parties except through that compulsory process. It is to say that, where the police seek personal information about an individual from an

---

191 Section 94(c).
192 *R v Alsford* [2015] NZCA 628 at [53].

agency holding the information, the police and the holding agency must come within an exception to the prohibition against disclosure under principle 11 or the information must be sought from or with the consent of the individual or a production order must be obtained on proper grounds.

Breach of the information privacy principles and the Evidence Act 2006

[161] The Privacy Commissioner suggests that the principles, although not directly enforceable in court, are relevant when assessing whether evidence is improperly obtained for the purposes of s 30(5) of the Evidence Act. His submission is that the principles are most appropriately considered under s 30(5)(c), as a possible basis for unfairness depending on the circumstances of the breach.

[162] The Commissioner submits that compliance with the principles may also be taken into account in deciding whether there was a reasonable expectation of privacy in relation to personal information which might make disclosure for law enforcement purposes unreasonable search, contrary to s 21 of the New Zealand Bill of Rights Act, or in considering whether a production order should have been obtained. He accepts that failure to comply with the principles would not be determinative of breach of s 21, because he accepts that failure to observe the principles does not in itself demonstrate intrusion into a reasonable expectation of privacy.

[163] Section 30(5)(a) includes in the identification of evidence "improperly obtained", evidence obtained "in consequence of a breach of any enactment of rule of law by a person to whom section 3 of the New Zealand Bill of Rights Act 1990 applies".

[164] Breach of a principle enacted under s 6 of the Privacy Act in obtaining and providing personal information might have been thought to be "breach of an enactment" within the meaning of s 30 of the Evidence Act. It is argued for the Crown, however, that since under s 11 of the Privacy Act principles are not enforceable as "legal rights" in the courts, their breach does not amount to "breach of an enactment" such as might justify exclusion of the evidence obtained through the breach under s 30 of the Evidence Act.

[165] Section 11 of the Privacy Act deals with the manner of enforcement of the principles:

> **11 Enforceability of principles**
>
> (1) The entitlements conferred on an individual by subclause (1) of principle 6,[193] in so far as that subclause relates to personal information held by a public sector agency, are legal rights, and are enforceable accordingly in a court of law.
>
> (2) Subject to subsection (1), the information privacy principles do not confer on any person any legal right that is enforceable in a court of law.

[166] The limitation in s 11 sets up investigation and enforcement by the Privacy Commissioner under Part 8 of the Act as the primary means of direct enforcement of the information privacy principles. (An exception provided by s 11(1) is that disclosure of the information a public sector agency holds about an individual can be compelled through court action.[194]) I cannot agree however that the restriction on the manner of enforcement of the prohibitions on disclosure and collection of personal information means that non-compliance with the principles is not breach of the provisions of the Privacy Act. In my view, information obtained as a result of non-compliance which is not within an exception contained in the Privacy Act or is not authorised by another enactment (and saved by s 7) is unlawfully obtained and its admission as evidence may be challenged under s 30 of the Evidence Act.

[167] The scheme of enforcement under Part 8 of the Privacy Act envisages that "adequate remedy" for breach of privacy may be obtained outside the enforcement provisions of the Act.[195] Where the resulting detriment through breach is the obtaining of evidence, it seems to me entirely preferable that any question of redress is assessed in the context of s 30. As the Privacy Commissioner pointed out in his submissions, it would be impractical to require a defendant to pursue a Privacy Act complaint before challenging the admissibility of evidence. As he said, "[t]he

---

193 Principle 6 gives an individual access to the personal information held by an agency.

194 Obtaining access to such information is important in the scheme of protections contained in the Act such as the entitlement to obtain correction provided by principle 7 and limits on the use to which an agency may put personal information about others or hold it on file under principles 8–10.

195 Privacy Act, s 71(1)(g).

statutory process has a uniform track and does not include urgent processing for complaints that have a bearing on other proceedings".

[168] To the extent that the decision of the Court of Appeal in *Wong-Tung* suggests that, by virtue of s 11(2), the privacy principles "[do] not have the force of law", 196 I would not follow it. Enforceability in the courts (as opposed to through the mechanism provided for redress in the statute) does not affect the obligations imposed by law on agencies which collect or disclose personal information.[197] They are statutory obligations the agencies are required to observe. Although their breach may not found a direct cause of action in itself, s 11(2) does not justify or excuse the breach.

[169] There have been considerable developments in the years since 1995 (when *Wong-Tung* was decided) both relating to privacy in information and the need for protections and in relation to what constitutes a breach of s 21 of the New Zealand Bill of Rights Act.[198] The major reforms of the Search and Surveillance Act have occurred since. *Wong-Tung* was also decided before s 30 of the Evidence Act was enacted to provide a framework for considering the common law discretion to exclude evidence. Section 30 requires evidence improperly obtained to be excluded unless exclusion is out of proportion to the impropriety.

[170] Where the admission of evidence obtained in breach of principles in the Privacy Act is sought to be excluded as improperly obtained in application of s 30 of the Evidence Act, it is not properly characterised as the "enforcement" of a legal right conferred by the privacy principles, within the meaning of s 11(2) and in

---

196 The statement in *Wong-Tung* was not material to the determination in that case because the Court took the view that there was no breach of principle 4 (the principle there in issue): *R v Wong-Tung* (1995) 13 CRNZ 422 (CA) at 426.

197 The Privacy Commissioner suggested that s 11(2) could be seen as limiting the provision of "civil remedies", but "does not restrict the courts from applying or taking account of the Principles as an expression of privacy standards in criminal proceedings such as an assessment under s 30(5)". As will be apparent, I take the view that a breach of the privacy principles in obtaining evidence is directly within the scope of s 30(5)(a), even if it is also a matter to be taken into account in considering whether the evidence was unfairly obtained.

198 At the time *Wong-Tung* was decided, it was unclear whether something "intangible" (such as the information there obtained by a "telephone analyser", which recorded details about calls) amounted to "search and seizure" for the purposes of s 21 of the New Zealand Bill of Rights Act. See *R v Wong-Tung* (1995) 13 CRNZ 422 (CA) at 426–427; referring to *R v A* [1994] 1 NZLR 429 (CA); and *R v Barlow* (1995) 14 CRNZ 9 (CA).

respect of which the Part 8 procedure is available.[199] The policy of limited direct enforcement does not require non-compliance with s 6 to be ignored in considering admissibility of evidence under s 30 of the Evidence Act.

[171] The Privacy Commissioner's submission that breaches of the information privacy principles should perhaps be considered under the unfairness limb of s 30(5)(c) was put forward on the basis that the law is as stated in *Wong-Tung*. I have explained why I do not think that decision can be maintained following the legislative reforms in the Search and Surveillance Act and the Evidence Act and why I take the view that s 11(2) does not itself constitute justification for breach of a principle. Since I also take the view that interference with privacy arises when evidence is obtained in breach of the principles (in what I would accept is relevant detriment and adverse effect on the individual's interests), I do not agree that it is necessary here to have recourse to s 30(5)(c) rather than s 30(5)(a). In my view, evidence obtained by the police (an agency to which s 3 of the New Zealand Bill of Rights attaches) through breach of the privacy principles is obtained in breach of an enactment. I would accept in addition that it is also unfairly obtained because obtained contrary to the reliance the individual was entitled to place on the Privacy Act, in this case echoed by the contractual undertakings of the utility providers to comply with the Act.[200]

[172] It follows that I am unable to agree with the other members of this Court in their view that breach of the privacy principles is unlikely to be of "independent significance" under s 30 of the Evidence Act 2006, although it "will [possibly] be relevant under s 30".[201] In my view, breach of the privacy principles in obtaining evidence means that the evidence is "improperly obtained" because obtained in breach of an enactment.

---

199 A conclusion reached also by Lang J in *R v Leone* HC Auckland CRI-2007-004-18646, 27 April 2009 at [90].

200 Although contractual terms permitting disclosure to third parties could not be determinative of compliance with the statutory obligation, a contractual representation that personal information will be protected and not disclosed except with the consent of the individual or in accordance with law is itself relevant to whether there was a reasonable expectation that the information would not be disclosed. The terms of the privacy policies adopted by the three utilities whose disclosure was in issue in the present case are set out in the reasons given by Arnold J above at [69]. All indicated the companies would disclose personal information only with the agreement of the individual or in accordance with the legislation.

201 Above at [40].

[173] Although I do not consider it is necessary to rely on the impropriety in the breach of the Privacy Act given the conclusion I reach on the use of the unlawfully obtained 2010 information, I mention for completeness that in another case, and depending on the context, breach of the principles of the Privacy Act may well not justify exclusion of evidence, in application of s 30(2) of the Evidence Act. Some guide to when breach of the privacy principles is such that exclusion of evidence obtained through the breach will be a proportionate response may be found in the enforcement provisions of the Privacy Act. Under s 66, enforceability by the Privacy Commissioner depends on whether there has been interference with privacy which entails not only breach of the privacy principles but loss, detriment or damage to the individual, adverse effect on rights, benefits, privileges or interests of the individual, or has resulted in or may result in significant humiliation, significant loss of dignity or significant injury to the feelings of the individual.

[174] In this scheme, while "significant" effect on feelings is necessary, any non-trivial detriment or adverse effect on rights or interests is treated by the statute as an interference with privacy justifying action by the Commissioner unless there is another adequate remedy. It is unnecessary for the purposes of disposition of this case to be definite. My tentative view however is that evidence improperly obtained through breach of the privacy principles which is not trivial will usually be an interference with privacy for which the appropriate remedy will be exclusion of evidence if it is justified by the balance required by s 30 of the Evidence Act. That seems to be consistent with Part 8 of the Privacy Act.

Compliance with the Privacy Act in obtaining the electricity consumption records

[175] The police requested the records relating to power consumption at Pannell Avenue and Baker Street from the three electricity suppliers, Genesis Energy, Meridian Energy and Contact Energy. Two of the requests referred to the Privacy Act. The request to Meridian was described as an Official Information Act 1982 request.

[176] I do not consider that the form of the request was material. What mattered was whether the basis for invoking the exception in principle 11(e)(i) was properly

made out. The requests were made on the basis of assertions by the police officer making them that:

(a) "intelligence has indicated that cannabis is possibly being grown at these addresses" (the request addressed to Contact Energy in relation to Pannell Avenue);

(b) "[t]o assist Police with an investigation that we are currently undertaking, information is sought in relation to [Pannell Avenue]" (the request to Genesis Energy); and

(c) the police were investigating an allegation of criminal activity and that "intelligence has indicated that cannabis is possibly being grown at [Baker Street]" (the request to Meridian Energy).

[177] Ellen France P queried whether the information provided to Genesis Energy by the police was sufficient to invoke exception (e)(i) to principle 11.[202] The email request said only that the disclosure of personal information was sought "to assist Police with an investigation we are currently undertaking". Although Ellen France P thought this email could be contrasted with the requests to Contact and Meridian Energy, I am not sure that the information provided to these companies was much improvement. It simply recorded that the personal information was required by the police for an investigation at the customer's given address where "intelligence has indicated that cannabis is possibly being grown". On the other hand, I do not think that what was called for was more detail about the intelligence the police had. Such information might well be information the police would properly be reluctant to provide and which the utility companies were not well-placed to assess.

[178] More importantly, there was no explanation of the need for the exception to non-disclosure, in the context of the availability of the judicial process of compulsion. The Search and Surveillance Act and its regulation of consent searches is also the context in which the exception for maintenance of law in principle 11(e)(i) falls to be interpreted and applied today. The requests provided no reason why a

---

202 *R v Alsford* [2015] NZCA 628 at [56].

refusal by the energy companies to disclose the information until they received a production order would have prejudiced the maintenance of law.

[179] Because there is no explanation of the need to provide the information under the exception to avoid prejudice to the maintenance of the law, I do not consider that the organisations who supplied the personal information could reasonably have held the belief that the provision of the information came within the (e)(i) exception to principle 11. I therefore consider that the information was supplied in breach of the legislation. The police actively facilitated the energy companies' breach of their obligations under principle 11. As explained above,[203] I consider that this amounted to collection of personal information by unfair means, a contravention of principle 4.

[180] It has been suggested here that there was insufficient information available to the police to make a successful application for a production order. If so, I think that circumstance demonstrates the wrongness of a broad interpretation of exception (e). It would permit easy evasion of the protections put in place for search under the Search and Surveillance Act wherever personal information is held by a third party. And it would avoid the policy of the Privacy Act in seeking to ensure as far as possible that those whose personal information is held by third parties and can be easily shared (as so much personal information is in the circumstances of today) are protected from undisclosed disclosure of it for purposes other than that for which it was provided unless the information is public or unless their consent is sought.

[181] As indicated, I consider that statements in some of the cases about the freedom of an agency holding personal information to act as a "good corporate citizen" in responding to requests by law enforcement agencies[204] need reassessment in the light of the policies of the Privacy Act and the availability of orders under the Search and Surveillance Act with its policy of balancing law enforcement interests with human rights and rights of privacy.

[182] I do not think it accords with the importance placed by the legislation on privacy interests in personal information for the provision of information to be left to

---

[203] Above at [146]–[147].

[204] See, for example, *R v Cox* (2004) 21 CRNZ 1 (CA) at [66].

the choice of the agencies holding the information. That opens the door to uneven application of the law, as is illustrated in the present case. The telecommunication company required a production order before providing information about the respondent's mobile phone use but the electricity providers passed it over on request. Unless there is some particular reason why obtaining a production order or search warrant is not practicable, I do not see that there is any "necessity" for the information to be provided as an exception to the general principle of non-disclosure save where there is statutory requirement. Such necessity is not shown simply by the request for the provision of the information by a law enforcement agency and its linkage with an investigation.

[183] Such interpretation of exception (e)(i) to principle 11 also means that a reasonable belief that the provision of the personal information is "necessary … to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences" does not require a holding agency to make the sort of assessment required of judicial officers in making compulsory orders under the Search and Surveillance Act. That is not a task they are qualified to perform. Instead, it requires provision to them of reasons why there would be prejudice to the maintenance of law (including in the investigation of crime) if there is compliance with the Act. The reasons may be directed at why it would be prejudicial to the maintenance of law for orders under the Search and Surveillance Act to be sought. If that course is not taken, the effect is that the police will have a blanket exemption from compliance with the Act for the purposes of investigation of crime. I do not think that any such blanket exemption is consistent with the scheme of the scheme of the Search and Surveillance Act and the Privacy Act.

[184] In my view it was incumbent on the police, as the requesting agency, to identify why obtaining a production order or search warrant would prejudice the investigation. If the only available answer is that the police did not have sufficient basis for making an application for production order or search warrant, I cannot think that recourse to the "maintenance of the law" exception in the prohibition on disclosure in principle 11 could be available to avoid the safeguards imposed for compulsory disclosure. The view that the utility companies can choose to disclose

personal information by treating any request by the police to supply it (if linked to investigation of a particular offence) as sufficient to establish prejudice to "maintenance of law", notwithstanding the general prohibition, is in my view inconsistent with the policies behind the regulation of "consent searches" under the Search and Surveillance Act.

[185] The Search and Surveillance Act makes it unlawful to undertake a search with the consent of someone who does not have authority to give it. I am of the view that on a purposive interpretation of the Privacy Act, collecting agencies do not have any authority to disclose personal information except in accordance with its provisions. The "consent" of the individual affected to disclosure envisaged by the scheme of the Privacy Act is otherwise illusory because it is obtained not from the individual affected but from someone who has no personal interest in the personal information.

[186] I have already indicated why I consider a general exception for requests by the police to assist in investigations would also diminish to vanishing point the elements of "necessity" and "prejudice" which are the conditions of the exception to principle 11. As a result, I consider that a law enforcement agency which procures disclosure of personal information by a holding agency in reliance on paragraph (e)(i) of principle 11 when there is no basis for doing so has collected that information "unfairly", in breach of its obligations under principle 4. Such collection is also in breach of an enactment, providing the occasion for application of s 30 of the Evidence Act.

[187] The view taken by the other members of the Court that breach of the privacy principles does not render evidence obtained through the breach unlawfully obtained in terms of s 30(5)(a) of the Evidence Act leads them to identify the "critical question" for the appeal as being whether the information was obtained through unreasonable search or seizure, contrary to s 21 of the New Zealand Bill of Rights Act, and on the basis that it "invades a reasonable expectation of privacy" (the test for breach of s 21 suggested by Blanchard J in *Hamed v R*).[205] The conclusion that

---

[205] See above at [47]–[48]. See also *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [163] and following.

there was no reasonable expectation of privacy in the monthly power usage data is determinative of the appeal in relation to the information obtained from the electricity providers.

[188] I disagree with this approach. I consider it insufficiently recognises the legislative policies contained in the Privacy Act in relation to personal information and the scheme of that Act. They make disclosure and collection of personal information which breaches the principles of the Act unlawful. I consider the correct approach was not to assess whether the individual had any reasonable subjective expectation of privacy in the information, but to assess whether the collection and disclosure of information was in breach of the Privacy Act. Reasonable expectations of privacy may well have been important in any consequential determination by the Privacy Commissioner of remedy under Part 8 or in the balance required in excluding improperly obtained evidence under s 30, but they were not determinative of breach of the Privacy Act. In the case of personal information, disclosure and collection of information had to be justified in terms of the Act. Otherwise such disclosure and collection was unlawful and constituted "improperly obtained" evidence for the purposes of s 30(5)(a).

[189] I consider it is inconsistent with the purpose and scheme of protection in the Privacy Act to treat the personal information in issue here as if "the companies' records", even in a formal sense.[206] The legislation makes it clear that it is personal information for the purposes of the Privacy Act and may not be disclosed by the utility company except in conformity with the Act. Nor indeed may it be used by the company collecting it except in the circumstances set out in principle 10, including where "the purpose for which the information is used is directly related to the purpose in connection with the information was obtained".[207] Any self-interest on the part of the company in detecting possible theft of electricity do not seem to me to bear on the obligations under the legislation.[208]

---

206 Compare above at [23].

207 Principle 10(e). Other exceptions are provided where the information is reasonably believed to be publicly available or that non-compliance is necessary to avoid prejudice to the maintenance of the law (mirroring the provision in principle 11(e)), or where it is necessary to avoid a serious threat (mirroring principle 11(f)).

208 Compare above at [67].

[190] For the reasons already indicated, I consider it is inadequate to conclude that "voluntary" collection and disclosure of personal information to the police is lawful if it complies with s 21 of the New Zealand Bill of Rights Act, as is the effect of the reasons given by the other members of the Court.[209] The conclusion they reach is driven by the approach that "the decisive issue is not whether the power consumption records were obtained consistently with the Privacy Act but whether they were obtained as a result of an unreasonable search, contrary to s 21 of [the New Zealand Bill of Rights Act]".[210]

[191] It is not open to the police to seek from third parties personal information held by them about individuals except in conformity with the provisions of the Privacy Act or after obtaining a production order or search warrant. Disclosure can be obtained with the consent of the individual affected or under the exceptions provided for in the Act. If consent is not forthcoming (or is not sought by the police), then I do not consider that the statutory scheme of the Privacy Act and the Search and Surveillance Act leaves scope for the utility companies to "volunteer" the personal information. If that means that "intelligence gathering" from third parties who hold personal information is inhibited in circumstances where the police have no sufficient belief to justify application for compulsory disclosure under production order or through search warrant, then that I consider is the consequence of the regulation of consent disclosure and the better balance sought to be achieved through the Search and Surveillance Act for privacy. I consider that case-law that predates the Search and Surveillance Act needs to be reassessed in light of that Act.

Section 21 of the New Zealand Bill of Rights Act

[192] Because I take the view that evidence obtained in breach of the Privacy principles is evidence improperly obtained within the meaning of s 30(5) of the Evidence Act, it is unnecessary for me to determine whether it was also improperly obtained because it constituted unreasonable search, in breach of s 21 of the

---

209 Above at [73]–[74].
210 Above at [17].

New Zealand Bill of Rights Act. I differ from other members of the Court who take the view, in application of the approach taken in *Cox*[211] and *R v H*,[212] that the "central" question is whether the evidence was obtained in breach of s 21 of the New Zealand Bill of Rights Act.[213] I consider that the central question for the Court in considering the use of the electricity records was whether disclosure was in breach of the Privacy Act. Whether it was also a breach of s 21 of the New Zealand Bill of Rights Act was not a matter that was critical to the application of s 30(5). Rather, if also a breach of s 21 of the Bill of Rights Act, that circumstance would be material to the proportionality analysis required by s 30(2)(b) of the Evidence Act. That is because breach of a right recognised as fundamental makes it less likely that exclusion will be found to be "disproportionate".

[193] I do not consider that the analysis of the appeal starts and ends with s 21 of the New Zealand Bill of Rights Act. In jurisdictions where there is no equivalent statutory prohibition on collection or disclosure of personal information, broadly defined, lawfulness may turn on matters of degree comparable to the s 21 proscription on "unreasonable search and seizure". But some care needs to be taken in treating case-law from jurisdictions without an equivalent protection for personal information to that contained in s 6 of the Privacy Act as controlling of the circumstances in which evidence is obtained in breach of an enactment. Similarly, New Zealand case-law concerned with the application of s 21 of the New Zealand Bill of Rights Act does not seem to me to address the question whether there has been a breach of s 6 of the Privacy Act. I do not therefore find the decision of the Canadian Supreme Court in *R v Plant*[214] to be as helpful as it is treated in the decision of the other members of the Court.[215] Similarly, I do not accept the view taken by Arnold J for the majority that the Canadian decisions on the equivalent Charter provision to s 21 of the New Zealand Bill of Rights Act provide the correct framework for analysis in the New Zealand context of the effect of breach of the Privacy Act principles.[216]

---

211 *R v Cox* (2004) 21 CRNZ 1 (CA).
212 *R v H* [1994] 2 NZLR 143 (CA).
213 See above at [17] and [28].
214 *R v Plant* [1993] 3 SCR 281.
215 See above at [55]–[57] and [63]–[64].
216 Compare above at [63]–[64].

[194] That is not to say that the use of the material obtained through the search is not breach of s 21 of the New Zealand Bill of Rights Act as well as breach of the Privacy Act. The other members of the Court hold that the obtaining of the respondent's electricity consumption records does not constitute an "unreasonable search" because conduct does not entail "search" unless it invades a "reasonable expectation of privacy".[217] I do not agree that "unreasonable search" is determined by whether it entails encroachment on a "reasonable expectation of privacy". The reasonableness requirement in s 21 attaches to the search or seizure in issue. In any event, while I do not accept that protection of a reasonable expectation of privacy is the only purpose served by s 21 (a matter I adverted to in *Hamed*[218]), the scope of the protection provided by the Privacy Act must bear on what expectation of privacy in personal information it is reasonable for the individual to expect. Relevant too is the scheme of the Search and Surveillance Act, a reform proposed by the Law Commission in part to provide "clear statutory rules" that could be used to "guide" the interpretation and application of "the protean" concept of "reasonable expectations of privacy" in connection with s 21.[219] The Law Commission recommended expansion of the search and seizure measures regulated by "detailed statutory provisions" to "guide the integration of reasonableness under section 21 in a number of contexts and ensure more complete protection of reasonable expectations of privacy".

[195] The provisions of the Search and Surveillance Act based on the Commission's report and referring explicitly to the balance struck between law enforcement and the privacy interests protected both under the New Zealand Bill of Rights Act and the Privacy Act point to congruence which is inconsistent with a narrow interpretation of "search" limited to information in which there is a reasonable expectation of privacy. Such interpretation would exclude much protected personal information. There seems to me to be no reason to constrain the meaning of "search" in this way. The balancing required by s 30 allows further consideration of all the circumstances and assessment of proportionality before evidence is excluded for breach of s 21. But the presumptive position that accords

---

217 Above at [47]–[48]; adopting *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [163] and following per Blanchard J.

218 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [10]–[11].

219 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [2.49].

better with the scheme of the legislation seems to me to allow that the obtaining of personal information in breach of the provisions of the Privacy Act is unreasonable search under s 21.

Conclusion

[196] For the reasons given in paragraphs [104] to [130], I would dismiss the appeal and affirm the decision in the Court of Appeal.

Solicitors:
Crown Law Office, Wellington for Appellant
Kearney & Co, Christchurch for Respondent
Office of the Privacy Commissioner, Wellington for Intervener