TARGETED VISUAL SURVEILLANCE IN NEW ZEALAND: AN ANALYSIS AND CRITIQUE OF THE SEARCH AND SURVEILLANCE BILL

SAMUEL P. BESWICK*

Introduction

Surveillance law in New Zealand will soon undergo considerable reform. The Search and Surveillance Bill ("the Bill") will be the first piece of legislation in New Zealand to address state surveillance activities comprehensively.[1] Based on an extensive Law Commission Report,[2] it aims to resolve the problems apparent in the present state of the law, which has been described as a "mess", rife with inconsistencies, incoherence, and uncertainty.[3] Though currently there are laws that govern audio interception techniques[4] and tracking devices,[5] there is virtually no statutory regulation of visual surveillance.[6] Nor does New Zealand have a warrant regime to authorise visual

* BCom/LLB(Hons), University of Auckland. High Court Judges' Clerk. I wish to acknowledge and thank Associate Professor Scott Optican for his guidance and suggestions in writing this article, which is an abridged version of a supervised dissertation.

[1] Search and Surveillance Bill 2009 45-1 ["SSB"]. On 24 May 2010, the Justice and Electoral Committee announced that the current Bill was likely to be redrafted in response to substantial criticisms raised in Select Committee submissions. The Committee, which has been considering the Bill since August 2009, intends to release an interim report to facilitate a process of further consultation with submitters: Justice and Electoral Committee "Search and Surveillance Bill" (press release, 24 May 2010); Tracy Watkins "'Chilling' Surveillance Bill Sent Back for Rewrite" *Stuff* (New Zealand, 25 May 2010). This article aims to raise relevant points for consideration in that regard. See also Barry Wilson and Ian McIntosh "Big Brother to Get More Rights" *The New Zealand Herald* (New Zealand, 20 November 2009).

[2] Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) ["LCR"].

[3] Sir Geoffrey Palmer, quoted in Amy Mansfield "Law Commission Report Damning of Outdated Search and Surveillance Laws" *NZ Lawyer* (New Zealand, 17 August 2007).

[4] See Crimes Act 1961, Part 11A; Misuse of Drugs Amendment Act 1978, ss 14 and 15A.

[5] See Summary Proceedings Act 1957, ss 200A–200P.

[6] LCR, above n 2, at 316–317. Cf Summary Offences Act 1981, s 30 (prohibits peeping and peering); Crimes Act 1961, s 216H (prohibits covert intimate filming).

surveillance activities.[7]

As a consequence, covert state-directed visual surveillance has tended to be regulated only by s 21 of the New Zealand Bill of Rights Act ("NZBORA"), which protects "the right to be secure against unreasonable search or seizure". Though in theory s 21 provides security to individuals from unreasonable state surveillance, alone it is insufficient to regulate this complex field of law. Jurisprudence around s 21 has produced little guidance as to what surveillance activities trigger a reasonable expectation of privacy (and thereby amount to a search), nor the implications of such a finding.[8] In fact to date, no non-trespassory electronic visual surveillance activity by the state has been found to be an unreasonable search by a New Zealand court.

This article presents a broad overview and analysis of the surveillance scheme created by the Bill. For illustrative purposes, this article critiques the Bill predominantly in terms of visual surveillance devices,[9] though much of the discussion is equally applicable to other forms of surveillance. Part II outlines the scope of the Bill's surveillance warrant regime, in particular, the conditions that attach to visual surveillance of premises. Part III discusses further aspects of the warrant regime created by the Bill, while the exceptions to those provisions are discussed in Part IV. Part V then considers the consequences of the independent oversight provisions created by a reporting requirement. As well as explaining the proposed new surveillance regime, this article offers suggestions throughout where reform of the Bill may be appropriate.

A. Scope of Surveillance Regime

Clause 42 of the Bill outlines four activities for which a surveillance

---

[7] See *R v Fraser* [1997] 2 NZLR 442 (CA) at 452; *R v Bailey* HC Auckland CRI-2007-085-7842, 7 October 2009, Winkelmann J at [98]. Note that the appeal of *R v Bailey* was heard on 8 and 9 June 2010: *R v Hunt* CA809/2009, William Young P, Glazebrook, and Ellen France JJ.

[8] See 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; see also *R v Fraser*, above n 7; *R v Gardiner* (1997) 15 CRNZ 131 (CA).

[9] Eg photo and video cameras, thermal imaging devices, aerial surveillance devices, and satellites.

warrant is required:[10]

> (a) use of an interception device to intercept a private communication:
> (b) use of a tracking device:
> (c) observation of private activity in private premises, and any recording of that observation, by means of a visual surveillance device:
> (d) observation of private activity in the curtilage of private premises, and any recording of that observation, if any part of the observation or recording is by means of a visual surveillance device, and the duration of the observation, for the purposes of a single investigation, or a connected series of investigations, exceeds—
> (i) 3 hours in any 24 hour period; or
> (ii) 8 hours in total.

The Bill has steered away from involving itself in the complications of s 21 NZBORA jurisprudence by not defining its scope solely in terms of a reasonable expectation of privacy or a gradation of privacy rights.[11] Instead, the scope of the Bill is clear: it covers certain places and some actions. In terms of surveillance, it applies in three circumstances: interception of private communications;[12] attaching a device to track the movement of a person or thing;[13] and surveilling private activities in or around private premises.[14] These actions will trigger the cl 42 warrant requirement; activities that fall outside of this scope will not.

1. Surveilling Private Premises

A warrant must be obtained when using a visual surveillance device to

---

[10] Note cl 43(1) contains six specific exceptions to cl 42.

[11] Cf *R v Williams* [2007] 3 NZLR 207 (CA) at 241–242; Criminal Code RSC 1985 c C-46 (Can), s 487.01(4).

[12] Replacing Crimes Act 1961, Part 11A, and Misuse of Drugs Amendment Act 1978, ss 14 and 15A.

[13] Replacing Summary Proceedings Act 1957, ss 200A–200P.

[14] Note that the Bill also contains a narrow residual warrant regime: SSB, cls 57–67. See LCR, above n 2, at 345–347; Human Rights Commission, below n 40, at 9–10; HRF & ACCL, below n 40, at [44].

observe "private activity in private premises".[15] Hence, if the police install a video camera to record continuously through a suspected drug dealer's dining room window over a period of months, or place hidden cameras in a private dwellinghouse, that activity will be in breach of the Bill unless a warrant is obtained.[16] Yet not all cases will be so clear cut. The applicability of the cl 42 warrant requirement will depend on what exactly constitutes a 'private premises' and what amounts to 'private activity'.

(a) Private Premises

The Bill seeks to clarify the scope of the term 'private premises' by defining it both positively ("a private dwellinghouse, a marae, and any other premises that are not within the definition of non-private premises") and negatively (a non-private premises being "premises, or part of a premises, to which members of the public are frequently permitted to have access, and includes any part of a hospital, bus station, railway station, airport, or shop").[17] The Law Commission Report used the term 'building' as opposed to 'premises'. The Commission considered that private buildings include "private residences, offices and commercial premises to which no member of the public would normally have access"; non-private buildings shared the definition adopted by the Bill.[18]

Clearly private houses fall within the scope of the Bill. But by adopting a different term and definition than that recommended by the Commission, the position in relation to private offices and commercial premises is less certain. On a plain meaning interpretation of the Bill, private premises should include private offices and commercial premises. This accords with overseas authority[19] and is consistent with

---

[15] SSB, cl 42(c). A visual surveillance device is defined broadly in the Bill to cover practically all devices that enhance the human eye (aside from spectacles or contact lenses) or are capable of visual recording: cl 3.

[16] Cf *R v Gardiner*, above n 8, where the Court of Appeal held that non-trespassory targeted video surveillance did not amount to an unreasonable search under s 21.

[17] SSB, cl 3.

[18] LCR, above n 2, at 329.

[19] See Kathleen Lomas "Bad Physics and Bad Law: A Review of the Constitutionality of Thermal Imagery Surveillance after *United States v Elkins*" (2000) 34 USFL Rev 799 at 806, 820, 825.

the Court of Appeal's statements in *R v Williams*, which recognise a reasonable expectation of privacy in relation to commercial premises.[20] Additionally, the narrow definition of premises, focussing on privacy in the traditional house, may result in non-house dwellings (such as mobile homes and caravans) receiving lesser (or no) protection of the Bill, even when they are situated on private land.[21] By contrast, in Australia premises can include vehicles.[22] Generally the courts are averse to warrantless searches and are hence likely to adopt a wide interpretation of premises;[23] nevertheless a more encompassing legislative definition would resolve this uncertainty directly.

(b) Private Activity

Clauses 42(c) and (d) incorporate the Law Commission's recommendation, and the generally held judicial view, that privacy is the value that surveillance legislation and the NZBORA aim to protect.[24] 'Private' in this sense means that there is an expectation that others are not watching (rather than that the subject matter of the activity is necessarily private).[25] Nevertheless, reducing cl 42's application only to 'private activity' unnecessarily complicates the otherwise straightforward 'private premises' test. The aim of protecting privacy may be thwarted by a requirement that enforcement officers and warrant issuers turn their minds to whether activity conducted on a premises is likely to be private. It reflects the approach taken in *R v Gardiner*, where the Court of Appeal considered that evidence which indicated the appellants believed they were being surveilled was a factor that reduced their reasonable expectation of privacy.[26] But such a

---

[20] *R v Williams*, above n 11, at 241 (though at a lesser degree to private dwellinghouses).

[21] Note that the Bill does not address the status of vehicles in relation to surveillance, despite the Court in *R v Williams* recognising some reasonable expectation of privacy in vehicles: ibid.

[22] See Surveillance Devices Act 2004 (Cth), s 17(2).

[23] *R v Williams*, above n 11, at 273: "the route of judicial pre-authorisation is preferable".

[24] Ibid; *R v Jefferies* [1994] 1 NZLR 290; LCR, above n 2, at 312–313.

[25] See SSB, cl 3; Kathleen Lomas, above n 19, at 821–822: "mundane activities within the home are just as much none of the government's business as are intimate activities". See also Thomas Clancy "What does the Fourth Amendment Protect: Property, Privacy, or Security?" (1998) 33 Wake Forest L Rev 307.

[26] *R v Gardiner*, above n 8: the defendants, apparently suspecting that their conversations were being taped, instead communicated via a whiteboard, which was then captured by

consideration detracts from the main issue — that surveillance devices enable officers to conduct prolonged, high definition video surveillance of the interior of private dwellinghouses. This is inherently intrusive. If officers need to conduct such surveillance, the question should focus on whether they have the requisite probable cause to obtain a warrant, not whether the occupier did enough to exclude external prying. A preferable approach is to replace the term 'private activity' in cls 42(c) and (d) with simply 'activity', which would create a simple test, requiring a warrant to be obtained for all surveillance of private premises (as it is for traditional searches).

2. Surveilling the Curtilage

Clause 42(d) covers surveillance of "private activity in the curtilage of private premises". The purpose of this clause is to require a warrant to be obtained in situations such as *R v Fraser*, where the police intend to conduct extended surveillance of a suspect's backyard or private property.[27] The Law Commission recommended a "more nuanced approach" to legislating surveillance of activities that occur outside of a private premises.[28] Individuals have a lesser expectation of privacy in activities occurring outside the home, which "are more susceptible of visual observation by a casual observer and enforcement officers"; thus a less strict standard of surveillance of those activities is considered appropriate.[29] In order to enable officers to conduct "fleeting observation",[30] the Bill permits them to surveil the curtilage of a private premises without a warrant, so long as such surveillance does not last longer than 3 hours in a 24-hour period, or 8 hours in total. This allows, for example, a police helicopter equipped with a surveillance device to fly over houses without triggering the warrant requirement.[31] Clauses 42(c) and (d) reflect a more straightforward approach to the gradation of privacy rights than that adopted by the Court of Appeal:

---

the video surveillance.

[27] *R v Fraser*, above n 7.

[28] LCR, above n 2, at 329.

[29] Ibid; cf Krista Boa "Privacy Outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning" (2007) 4 Surveillance & Society 329 at 338–339, discussing the oft misunderstood privacy implications of state-directed surveillance.

[30] LCR, above n 2, at 329.

[31] See eg *R v Peita* (1999) 17 CRNZ 407.

private dwellings have a high expectation of privacy, while less privacy attaches to the exterior curtilage.[32]

(a) Curtilage

'Curtilage' is not defined in the Bill and may become subject to a not insignificant amount of litigation. The Oxford English Dictionary defines it as:[33]

> A small court, yard, garth, or piece of ground attached to a dwelling-house, and forming one enclosure with it, or so regarded by the law; the area attached to and containing a dwelling-house and its out-buildings.

The Law Commission noted that 'curtilage' is used in some legislation but has never been statutorily defined. The Commission's non-exhaustive definition considered that curtilage covers "the immediate surrounds of the buildings, including decks and gardens, whether or not they are fenced or enclosed".[34] Though this provides some guidance, the word contains ambiguities. Attempting to define the immediate surrounds of a building is problematic. For instance, is a glass patio part of a house, so that a surveillance warrant is always required, or akin to a deck, where short-term warrantless surveillance may occur? The issue is complicated further when considering whether different types of premises have a larger curtilage than others (for example, a farm house compared to an apartment).[35]

By not defining curtilage in the Bill, enforcement officers (and citizens) are not given sufficient guidance over when cl 42 might be in issue. This may result in arguments arising at trial as to the admissibility of surveillance evidence captured without a warrant.[36] Such problems have arisen in the United States, where curtilage is defined not just in proximity to a private premises, but also in terms of domestic use

---

[32] Cf *R v Williams*, above n 11, at 241–242, which discusses a complex gradation of privacy rights between and within different places.

[33] 'Curtilage' in JA Simpson and ESC Weiner (eds) *Oxford English Dictionary* (2nd ed, Clarendon Press, Oxford, 1989) at 160.

[34] LCR, above n 2, at 329.

[35] See *R v Williams*, above n 11, at 241–242.

[36] Under the Evidence Act 2006, s 30.

(which requires consideration of whether the area is used and enjoyed "as an adjunct to the domestic economy of the family").[37] To avoid these issues, the legislature should define curtilage in the Bill. This could be done by adopting the Law Commission's definition with a more extensive non-exhaustive list to provide guidance to judges, warrant issuers, and enforcement officers. Though this might not prevent arguments along the fringe, it would go some way toward bringing certainty to cl 42(d).

(b) A Warrant Preference Rule?

The '3 hours in a 24-hour period, or 8 hours in total' leeway was included on the recommendation of the Law Commission so as not to curtail ordinary police practice.[38] It aims to safeguard individuals' privacy rights without stifling legitimate law enforcement interests in acquiring evidence of criminality. The chief concern with the provision is that, although it allows passing unobtrusive surveillance not to be blocked by the warrant procedure, it also gives officers an opportunity to surveil targets for up to eight hours without a warrant. Furthermore, the Bill does not define what 'in total' means: it does not specify the point at which it 'resets' allowing for surveillance for another eight hour period.

Given the general purpose of the surveillance device regime — to regulate targeted surveillance — it may be desirable to include a warrant preference rule into cl 42(d).[39] This could retain the current leeway, with the exception that, when targeting a particular person or property in circumstances where it is not impracticable to obtain a surveillance warrant, a warrant should be sought. The purpose of the rule would be to distinguish between indirect or fleeting observations of a private dwelling (which should not demand a warrant), and short term targeted surveillance (where the argument for a warrant may be stronger). This is in line with the Law Commission's recommendations, and would temper some of the critics' concerns that the Bill greatly expands police

---

[37] *Care v United States* 231 F 2d 22 at 25 (10th Cir), cert denied 351 US 932 (1956). See Anthony Amsterdam "Perspectives on the Fourth Amendment" (1974) 58 Minn L Rev 349 at 370.

[38] LCR, above n 2, at 329–330.

[39] Ibid, at 331.

power to spy on citizens.[40]

(c) Beyond the Curtilage

By defining the scope of the Bill in terms of proximity to private premises the legislature has limited its application considerably. A number of areas where one might otherwise hold a reasonable expectation of privacy are not covered, such as private land masses. In *R v Bailey*, for instance, the police installed surveillance cameras in a privately-owned forest in Urewera to capture evidence of alleged terrorist training activity.[41] The surveillance was purportedly authorised by warrants obtained under s 198 of the Summary Proceedings Act 1957. In the High Court, however, Winkelmann J held that the s 198 warrant provision did not apply to electronic surveillance (and the search was, in part, unreasonable under s 21 of the NZBORA).[42] Peculiarly, the new warrant regime is equally inapplicable to like cases — in *Bailey* the police were surveilling activity in a private forest, not near a premises. Hence, their actions would still be outside of the Bill's jurisdiction. This undermines the Bill's objective to provide coherent and effective law enforcement powers:[43] uncertainty around state surveillance of private property remains because the Bill's warrant regime does not properly address it.

In the United States there is no reasonable expectation of privacy in 'open fields' beyond the curtilage.[44] The United States Supreme Court has held that open fields do not present the same privacy issues as

---

[40] See Human Rights Foundation of New Zealand and Auckland Council for Civil Liberties Inc "Joint Submission to the Justice and Electoral Committee on the Search and Surveillance Bill 2009" ["HRF & ACCL"]; Human Rights Commission "Submission to the Justice and Electoral Committee on the Search and Surveillance Bill 2009".

[41] *R v Bailey*, above n 7.

[42] Ibid, at [98]–[101], [165]: the general search warrant provision in s 198 of the Summary Proceedings Act 1957 does not extend to the authorisation of electronic surveillance, because (a) it is directed to searches for "things" and (b) it requires a warrant to be executed in person.

[43] SSB (explanatory note) at 1.

[44] The open fields doctrine: *Hester v United States* 265 US 57 (1924) at 59; see Richard Wilkins "Defining the 'Reasonable Expectation of Privacy': An Emerging Tripartite Analysis" (1987) 40 V and L Rev 1077 at 1097–1100; Ric Simmons "Technology-Enhanced Surveillance by Law Enforcement Officials" (2005) 60 NYU Ann Surv Am L 711 at 714–716.

private residences, and there is no overriding public interest in protecting activities which occur in such places. The Court specifically rejected the proposition that Fourth Amendment considerations beyond the curtilage should be determined by the individual circumstances of each case, reasoning that this would result in a "highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions."[45] Law enforcement would be frustrated if officers had to turn their minds to complicated privacy issues before every search of an open field, in turn running the risk that the constitutional right would be "arbitrarily and inequitably enforced".[46]

Notwithstanding these concerns, the open fields doctrine has been criticised as an outdated law unsuited for modern society, which allows officers to avoid the requirements of a warrant, the Fourth Amendment (*idem quod* s 21 NZBORA), and probable cause.[47] The Court of Appeal has rejected the open fields doctrine. Whereas in the United States the specific circumstances are irrelevant when considering private property beyond the curtilage, the Court of Appeal in *R v Williams* expressly accepted that "outward signs of an increased (subjective) expectation of privacy (such as signs, barricades or security) … should be taken into account" when assessing a reasonable expectation of privacy.[48] The Court in *R v Peita* suggested that situations could arise where aerial surveillance of private land would implicate s 21, although "each case must be considered on its own facts".[49] The open fields approach was also rejected in *R v Bailey*, where Winkelmann J analysed separately the different areas of the privately-owned forest targeted by police. She found that a reasonable expectation of privacy did not exist (and so s 21 was not in issue) in relation to surveillance of activities in open view when the respondents exerted no control over who could come onto the land. However, where the respondents had made an effort to exclude the public from entering and observing activities on the land,

---

45 *New York v Belton* 453 US 454 (1981) at 458.

46 *Oliver v United States* 466 US 170 (1984) at 182.

47 See Larry Mays and Ronald Pincomb "The Fourth Amendment and Aerial Surveillance: Searching for Guidelines" (1984) 1 Just Q 17 at 20–21.

48 *R v Williams*, above n 11, at 241–242.

49 *R v Peita*, above n 31, at [13].

their expectation of privacy was found to be objectively reasonable.[50] Hence, the warrantless surveillance of that activity by the state was unreasonable under s 21 of the NZBORA (despite there being no applicable warrant regime).

Because the Courts recognise a reasonable expectation of privacy beyond the curtilage, the legislature must keep apace by proscribing a warrant regime which addresses state surveillance activities beyond the curtilage. Thus cl 42(d) should be extended at least to cover all surveillance of private land, regardless of its proximity to buildings. Just as police must obtain a warrant to conduct a physical search of private property, so they should have to get a warrant to conduct extensive electronic surveillance of such property. (The cl 42(d) leeway would continue to permit fleeting surveillance, however.) This would bring certainty both to police and the public regarding the circumstances in which the state can target citizens through surveillance. It would also enhance the legitimacy of police surveillance actions by requiring all non-public property surveillance to be subjected to the Bill's provisions, thereby better safeguarding the privacy rights of individuals.

B. Warrant Regime

1. Warrant Application Requirements

A common criticism of the present warrant system is a general lack of specificity in warrant applications.[51] It is unsatisfactory for state officers to exert intrusive powers on the basis of a warrant that is overly wide or lacking in specificity. Rather, a warrant application (and warrant) must be "as specific as the circumstances allow" to enable the Judge to determine the persuasiveness of the evidence gathered.[52] Accordingly, cl 45(1) requires that the following particulars be included in an officer's application for a surveillance warrant:

(a) the name of the applicant:

---

[50] *R v Bailey*, above n 7, at [156]–[165].

[51] LCR, above n 2, at 208–210; *R v Williams*, above n 11, at 261, 273; SSB (explanatory note) at 1–2.

[52] *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780 (CA) at [41].

(b) the provision authorising the making of an application for a search warrant in respect of the suspected offence:
(c) the grounds on which the application is made:
(d) the suspected offence in relation to which the surveillance device warrant is sought:
(e) the type of surveillance device to be used:
(f) the name, address, or other description of the person, place, vehicle, or other thing that is the object of the proposed surveillance:
(g) a description of the evidential material believed to be able to be obtained by use of the surveillance device:
(h) the period for which the warrant is sought.

It can be difficult to ascertain specificity in surveillance warrant applications. In some circumstances, it may be appropriate to surveil activities though the identity of a specific target person, place, or object may not be known to police (for example, when tracing drug traffickers).[53] For this reason, cl 45(2) contains an exception to cls 45(1)(f) and (g): where the target person, place, or object cannot be identified in the warrant application, the officer must instead "state the circumstances in which the surveillance is proposed to be undertaken in enough detail to identify the parameters of, and objectives to be achieved by, the proposed use of the surveillance device". Clause 45(2) follows the approach adopted in Australia, by seeking to permit surveillance where full information is not available, while ensuring that warrants are not sought merely to aid fishing expeditions into suspected illegal activity.[54] Nevertheless, without adequate restraint cl 45(2) borders on a 'general warrant' — it could be used to sanction surveillance of an unspecified target and object. What the courts require from, and how strictly they interpret, "enough detail" will determine the extent to which the provision contains scope for abuse.

Additionally, the disclosure requirements in cls 45(3) and (4) aim to prevent abuse of surveillance powers by requiring applicants to disclose

---

[53] LCR, above n 2, at 334.

[54] See Surveillance Devices Act 2004 (Cth), s 17(1)(b)(viii); Surveillance Devices Act 1999 (Vic), ss 19(1)(c), 19(2)(c); Surveillance Devices Act 1998 (WA), ss 13(8)(b)–(d).

the details of any previous (within three months) warrant applications and the result of those applications. This is intended to deter officers from unreasonably hounding suspects through surveillance, or reapplying via alternative avenues for warrants that have previously been unsuccessful.

2. Conditions for Issuing

(a) Scope

Traditional attitudes toward targeted surveillance are that it should be highly restricted, only to be used when essential. Hence, under the current interception and tracking device warrant regimes, an officer generally must exhaust alternative strategies before undertaking surveillance of alleged illegal activity.[55] The Law Commission and the drafters of the Bill rejected this approach, recommending that surveillance warrants should be available in the same circumstances as search warrants.[56] That is, a warrant should generally be available for offences punishable by imprisonment, and should generally not be available for infringement offences or for offences that are prescribed by regulation.[57] Hence, cl 46 allows a surveillance warrant to be obtained in relation to any "offence" that "has been committed, or is being committed, or will be committed". This significantly expands the scope of surveillance warrants in New Zealand.[58]

There have been a number of criticisms that the Bill's scope is too wide in allowing surveillance for any type of offence.[59] Surveillance is inherently intrusive: it infringes upon personal privacy, liberty, and

---

[55] Crimes Act 1961, s 312C(1)(c); Summary Proceedings Act 1957, s 200B(2)(c).

[56] LCR, above n 2, at 331–332; the Law Commission focused on the similarities between surveillance and a traditional search, and concluded that "the former are not intrinsically more intrusive than the latter".

[57] Ibid, at 90–92.

[58] Warrants are valid for up to 60 days (SSB, cl 50(1)(c)), and permit enforcement officers to use reasonable force to enter specified premises, areas, vehicles, and things to install, maintain, or remove a surveillance device (SSB, cl 50(3)(g)).

[59] See HRF & ACCL, above n 40; Human Rights Commission, above n 40; Chief Justice of New Zealand "Submission to the Justice and Electoral Committee on the Search and Surveillance Bill 2009".

security regardless of whether it is conducted pursuant to a warrant.[60] There is genuine concern that a broad approach to surveillance applications will result in the use of targeted surveillance which is out of all proportion to the alleged offending.[61] Two approaches have been raised to placate these concerns. The first, submitted by the Chief Justice, is to amend cl 46 so that surveillance warrants are available only for specified offences.[62] This would effectively create a 'floor' to prevent surveillance being used on low-level offences. It is the approach currently adopted for interception warrants and in the Australian federal jurisdiction.[63]

A second approach would be to require a warrant issuer to turn their mind to the intrusiveness of surveillance and balance that against the need of enforcement officers to gather evidence efficiently. This is the approach applied in Victoria, where a judge in considering a warrant application must have regard to:[64]

> (a) the nature and gravity of the alleged offence in respect of which the warrant is sought; and
> (b) the extent to which the privacy of any person is likely to be affected; and
> (c) alternative means of obtaining the evidence or information sought to be obtained; and
> (d) the evidentiary value of any evidence sought to be obtained; and
> (e) any previous warrant sought or issued under this Division in connection with the same offence.

---

[60] Bell Gully "Submission to the Justice and Electoral Committee on the Search and Surveillance Bill 2009" at 4–5.

[61] See eg "Council 'Spied on Woman 21 Times'" *BBC News* (United Kingdom, 5 November 2009); "The Anti-Terror Law Used on Litterbugs" *BBC News* (United Kingdom, 17 April 2009).

[62] Chief Justice of New Zealand, above n 59, at [15].

[63] Crimes Act 1961, ss 312B(1), 312CA(1), 312CC(1) (participation in organised crime, serious violent offending, and terrorism); Misuse of Drugs Amendment Act 1978, ss 14 and 15A (drug dealing). See also Surveillance Devices Act 2004 (Cth), s 6 (offences punishable by 3 years imprisonment or more).

[64] Surveillance Devices Act 1999 (Vic), s 17(2); see also Crime and Misconduct Act 2001 (Qld), s 123.

Similarly, the current tracking device regime requires the judge to consider the public interest in issuing a warrant, taking into account the above factors.[65] This approach effectively requires the judge to undergo a balancing exercise which assesses whether an individual's privacy rights can be justifiably interfered with by the state in the circumstances. Such an assessment reflects the Court of Appeal's concerns in *R v McGinty*, that a "clear and strong case has to be made out for the grant of a warrant to intercept private communications. Patently it is a step never to be lightly authorised in the New Zealand society."[66] Though introducing a 'floor' or an assessment of factors may conflict with the legislature's goal of an all-encompassing surveillance regime, such considerations should not be lightly disregarded given the invasiveness of targeted state surveillance. Neither the Law Commission nor the legislature have given a reasoned explanation as to why suspected minor offences warrant the full invasive powers of state surveillance. Efficiency in gathering evidence should not automatically trump an individual's right to be free from unreasonable state intrusion.

(b) Threshold

The current threshold that must be met to exercise search or surveillance powers differs depending on the particular laws, some requiring 'reasonable grounds to believe' and others the lesser 'reasonable grounds to suspect'.[67] After considering the different standards and contexts within which the thresholds apply in New Zealand, the Law Commission recommended that 'reasonable grounds to believe' be the prerequisite for the exercise of law enforcement powers, "a threshold that should be departed from only in *exceptional* cases".[68]

It is interesting, then, that the drafters of cl 46 chose to define the conditions for issuing surveillance warrants by reference to two limbs:

---

[65] Summary Proceedings Act 1957, s 200B; see Alex Conte "Crime and Terror: New Zealand's Criminal Law Reform Since 9/11" (2005) 21 NZULR 635 at 657.

[66] *R v McGinty* [1983] NZLR 524 (CA) at 528.

[67] LCR, above n 2, at 56–59.

[68] Ibid, at 21 (emphasis added).

(a) Where there are reasonable grounds *to suspect* that an offence punishable by imprisonment[69] has been committed, or is being committed, or will be committed; and
(b) Where there are reasonable grounds *to believe* that a surveillance warrant will obtain information that is evidential material in respect of the offence.

Clause 46 employs a lower standard than that recommended by the Law Commission, requiring that officers need only have a reasonable suspicion (rather than belief) of an offence. Though both approaches demand an objective assessment, reasonable grounds to believe employs "a much higher test" than the suspicion test.[70] Suspicion requires a degree of likelihood, while belief requires a "view that the state of affairs in question actually exists."[71] Hence, evidence of a one-off cannabis sale may give officers a reasonable suspicion that a suspect has drug paraphernalia at his house, but that alone will not meet the reasonable belief threshold when applying for a warrant two months later.[72] The cl 46 bi-partite test was criticised in a number of Select Committee submissions, which argued that the intrusiveness of surveillance powers requires that the higher threshold should apply.[73] The concern is that the suspicion test reduces the threshold to an unacceptably low level. Also, there is no evidence to suggest that the belief test operates inadequately.

3. Issuing Judges

In relation to search warrants, the Bill creates a new regime of issuing officers, which includes judges, justices of the peace, community magistrates, court registrars, and deputy registrars.[74] Clause 48 applies a stricter approach — only High Court or District Court judges may

---

[69] SSB, cl 6; or an offence where an enactment authorises a warrant.

[70] *R v Karalus* (2005) 21 CRNZ 728 (CA) at [27].

[71] *R v Sanders* [1994] 3 NZLR 450 (CA) at 461.

[72] *R v Karalus*, above n 70, at [28].

[73] Human Rights Commission, above n 40, at 7; HRF & ACCL, above n 40, at [74].

[74] SSB, cl 3.

issue surveillance warrants. Though the Law Commission supported, in principle, an all-encompassing approach, it recognised that the current surveillance regime requires a High Court judge to issue interception warrants (and a District Court judge may issue tracking device warrants), and there is genuine public concern about the expansion of surveillance powers. Therefore, on balance, the Commission recommended a stricter standard than for search warrants, requiring judges alone to issue surveillance warrants. This approach is consistent with Australian regimes, where all state jurisdictions restrict issuers to judges[75] or Supreme Court judges.[76] The Chief Justice advised a higher standard still, submitting to the Select Committee that the intricacies of determining invasion of privacy issues and the need for confidentiality dictate that surveillance warrants should be issuable by High Court Judges only.[77] Though it may not be practical to so limit the number of issuers, the submission highlights the need for judges to assess warrant applications critically to safeguard individual freedoms in the *ex parte* process.

4. The Plain View Rule

In relation to the execution of a warrant, cl 51(3) introduces the plain view evidence rule into the surveillance scheme: windfall evidence,[78] or evidential material in relation to one offence, that is inadvertently obtained during the lawful surveillance of a different offence, in respect of which a surveillance warrant could have been issued,[79] is not inadmissible in criminal proceedings by reason only that it was obtained in the course of surveilling a different offence.[80] In other words, evidence of illegality caught in plain view of a lawful surveillance device is not inadmissible merely because the officer did not have a warrant to

---

[75] Surveillance Devices Act 1998 (WA), s 12; Surveillance Devices Act 2007 (NSW), s 17(2); Surveillance Devices Act 2007 (NT), s 19(2); see also Criminal Code RSC 1985 c C-46 (Can), s 487.01(1).

[76] Crime and Misconduct Act 2001 (Qld), s 121(2); Surveillance Devices Act 1999 (Vic), s 14; Listening and Surveillance Devices Act 1972 (SA), s 6(1); Police Powers (Surveillance Devices) Act 2006 (Tas), s 9(2).

[77] Chief Justice of New Zealand, above n 59, at [23].

[78] "Search and Surveillance Bill 2009" No 1696 (22 July 2009) *Bills Digest* at 2.

[79] Meaning that the offence would meet the cl 46 requirements (not that the officer necessarily had the requisite probable cause for a warrant).

[80] SSB, cl 51(2)–(3).

capture that evidence.

The plain view rule effectively allows officers to seize evidence in the absence of a warrant for it.[81] This invites potential for abuse if officers were opportunistically to obtain a warrant in relation to one offence, hoping to uncover some other type of criminality. To quell this risk, United States courts require four conditions to coalesce for plain view evidence to be admissible at trial: (1) a prior justified intrusion into the search area (such as consent, a warrant, or statutory authority); (2) the evidence was in plain view to be seen by those lawfully present; (3) the incriminating nature of the evidence was "immediately apparent"; and (4) the discovery was "inadvertent".[82] Officers cannot undertake fishing expeditions for incriminating evidence outside of the scope of their warrant; but if such evidence is discovered inadvertently and its incriminating nature is obvious, the seizure of that evidence is justified.

New Zealand courts recognise only a "limited" plain view rule (in relation to stolen property),[83] and have not developed a thorough jurisprudence on it. The Bill purports to expand the application of the rule, yet it does not detail the test that will apply to cl 51(3). It is conceivable that the courts will follow the United States approach in *Coolidge v New Hampshire*,[84] though the effect cl 51(3) will have on surveillance cases is not immediately apparent. Presumably, any illegal activity that is inadvertently captured by a lawfully-placed surveillance device will be in plain view.[85] But if police intentionally go beyond the scope of a surveillance warrant to capture other types of illegality, this is less likely to satisfy the requirements of the rule.

---

[81] The plain view rule applies to seizures of evidence, not searches. In the context of surveillance it applies to the electronic capturing of evidence.

[82] *Coolidge v New Hampshire* 403 US 443 (1971) at 466; Howard Wallin "Plain View Revisited" (2002) 22 Pace L Rev 307 at 307–308, 324; cf Don Stuart *Charter Justice in Canadian Criminal Law* (2nd ed, Carswell, Scarborough, 1996) at 248, asserting that 'inadvertence' is not a requirement.

[83] *R v Williams*, above n 11, at 223; *McFarlane v Sharpe* [1972] NZLR 838 (CA) at 844; *R v Power* (1999) 17 CRNZ 662 (CA).

[84] *Coolidge v New Hampshire*, above n 82. This is recommended by the Law Commission: LCR, above n 2, at 82.

[85] For example, police might have a warrant to use a thermal imaging device to search a house for unlawful hydroponic systems, but lawfully capture evidence of domestic violence also.

C. Warrantless Surveillance: Emergency or Urgency

In some situations of emergency or urgency it may not be feasible for an officer to obtain a warrant before undertaking surveillance. Nevertheless, the circumstances may present a need for surveillance. This need must be balanced carefully against the intrusiveness of permitting the state to surveil individuals in the absence of a warrant: "warrantless searches … should not be the norm".[86] There are three pertinent issues in regard to determining the legitimacy of warrantless surveillance: the approval process for permitting surveillance, the timeframe for which it should run, and the offences to which warrantless surveillance should apply.

1. Approval Process

In relation to the approval process, three approaches are available. The first is to permit officers to undertake emergency surveillance subject to retrospective judicial approval. The Law Commission, however, considered that this would be "pointless", as retrospective approval has no practical effect, and disproval would produce unclear consequences.[87] The second option, applied in several Australian jurisdictions, is to permit emergency surveillance subject to an internal authorisation process.[88] Again this is unsatisfactory, as "[i]f there is time to obtain internal approval then there ought to be sufficient time to obtain a telewarrant".[89]

Consequently, the Bill proscribes the third option: to permit an officer to undertake emergency surveillance, "leaving the question of the lawfulness of the warrantless use of the device for determination in later civil or criminal proceedings".[90] Understandably, if there is an

---

[86] *R v Williams*, above n 11, at 272–273.

[87] LCR, above n 2, at 340. Cf Crimes Act 1961, s 312G(9), and Misuse of Drugs Amendment Act 1978, s 19(9): retrospective approval provisions available to a judge to validate emergency use of an interception device.

[88] Surveillance Devices Act 1999 (Vic), s 25; Surveillance Devices Act 2007 (NSW), s 32; Surveillance Devices Act 2004 (Cth), s 28. See Crimes Act 1961, s 312G, and Misuse of Drugs Amendment Act 1978, s 19, which prescribe an "emergency permits" scheme for judges to sanction the use of interception devices.

[89] LCR, above n 2, at 340.

[90] Ibid.

urgent situation, an officer should not be discouraged to act due to an impractical requirement to obtain approval. Nevertheless, it should be recognised that this approach bypasses the (arguably) most important accountability measure on officers, that being prospective independent oversight. In that regard, the need for officers to comply with the strict provisions in the Bill is heightened. If it is later found that the warrantless surveillance was unjustified, this may have repercussions at the reporting stage (which in turn becomes the crucial accountability measure) or when considering the admissibility of evidence at trial.[91]

2. Timeframe for Warrantless Surveillance

Clause 44 specifies certain exceptions to the cl 42 warrant requirement. In specific situations, an officer may use a surveillance device for up to 72 hours without obtaining a warrant, if the officer would be entitled to apply for a warrant but, due to time constraints, it would be "impracticable in the circumstances".[92] After the expiry of the 72 hour time period, evidence obtained pursuant to cl 44 will be obtained illegally unless the surveillance has been sanctioned by a cl 42 warrant. Therefore officers will either have to cease the surveillance or seek a warrant under the cl 45 procedure. Again, it may be desirable to incorporate a warrant preference rule into cl 44, stipulating that warrantless emergency surveillance is permissible in certain circumstances, but where it is not impracticable to obtain a surveillance warrant, a warrant should be sought.[93]

3. Circumstances in which Warrantless Surveillance is Permissible

Those situations to which cl 44 applies are where an officer has reasonable grounds *to suspect* there is offending involving serious harm or danger, or specified drug offending. Specifically, the warrantless surveillance provision applies to offences punishable by a term of at least 14 years imprisonment, to offences where injury to a person or serious damage to property is likely or where there is an emergency that

---

[91] See Evidence Act 2006, s 30.

[92] SSB, cl 44(1)(b). The Law Commission recommended that the maximum period to permit emergency surveillance should be only 48 hours: LCR, above n 2, at 340.

[93] See 'A Warrant Preference Rule' discussion above.

may endanger the life or safety of any person, and to specified offences in relation to possessing arms in dangerous circumstances under the Arms Act 1983 and certain drug offending under the Misuse of Drugs Act 1975.[94] This strict detailing of the offences for which warrantless surveillance is permissible is consistent with an approach to surveillance that balances an individual's right not to be arbitrarily targeted by the state, against the need of law enforcement to act competently in emergencies.

In relation to each of those grounds, cl 44(2) requires also that the enforcement officer have reasonable grounds *to believe* that the use of the surveillance device is necessary to obtain the evidential material or to prevent the suspected offending. This mirrors the cl 46 bi-partite test, requiring reasonable grounds to believe that the warrant will be effective but only reasonable grounds to suspect that there is criminality. It also differs somewhat from the Law Commission's recommendations, which stipulated that the belief threshold should apply to general serious offending and drug offending, and the suspicion threshold to offending involving personal harm or danger and Arms Act offending.[95] In circumstances of a serious emergency, it is more justifiable that the lesser suspicion test apply — the need to act is greater in light of imminent harm. Nevertheless, a lower threshold should not be used as a lax standard to surveil extensively in the absence of sufficient probable cause.

D. Reporting Requirement

This article has already discussed the first of the two key state accountability mechanisms in the Bill, that being a warrant requirement. A mandatory obligation to obtain a warrant before executing targeted surveillance aims to uphold the legitimacy and integrity of police investigatory techniques, by subjecting to judicial scrutiny officers' reasons for conducting surveillance. This is a prospective accountability mechanism. The second independent oversight safeguard involves assessing the legitimacy of officers' conduct in executing a surveillance power after the fact. This is a retrospective accountability mechanism which is effected through a reporting

[94] SSB, cl 44(2).

[95] LCR, above n 2, at 340–341.

requirement.

The Bill attempts to temper fears of abuse of surveillance powers by imposing detailed reporting standards. Within one month of a warrant expiring, or from the last day of any emergency surveillance, the person who carried out the surveillance activities must provide to a judge of the warrant-issuing court a report detailing:[96]

> (a) Whether the surveillance activities resulted in obtaining evidential material, or, in the case of emergency surveillance, whether the cl 44(2) objectives were met;
> (b) The circumstances in which the surveillance device was used; and
> (c) Where relevant, any other information that was stated in the warrant as being required in the report.[97]

The purpose of the reporting requirement is to ensure the accountability of officers who utilise surveillance devices via a retrospective oversight procedure. It is similar to the procedure currently applied to interception warrants.[98] Unfortunately, under the current drafting of the Bill, the reports will potentially have little or no effect. The following discussion outlines three fundamental criticisms of the reporting requirement, and recommends amendments to the Bill.

1. Judge May Order Destruction of Material

Clauses 55 and 56 should cause concern to liberty and privacy advocates for the use of the word 'may' in three crucial circumstances. The first is that a judge *may* give directions as to the destruction or

---

[96] SSB, cls 53 and 54; see also cl 50(1)(d). The New Zealand Police Association submitted that more rigorous reporting requirements will take further police resources away from frontline work and the advancement of cases: New Zealand Police Association "Submission to the Justice and Electoral Committee on the Search and Surveillance Bill 2009" at [26]–[29]. Counter to this argument are concerns that increased state surveillance necessarily requires stricter regulatory oversight.

[97] SSB, cl 50(2) authorises a judge to impose any other reasonable conditions when issuing a warrant.

[98] Crimes Act 1961, s 312P.

retention of material obtained as a result of surveillance.[99] This is the only mention of what should be done with post-surveillance material, and is a topic notably absent from the Law Commission Report.

One of the inherent concerns of surveillance is its ability (and tendency) to capture non-illegal activity, whether classified as private or otherwise. Though one has no reasonable expectation of privacy in illegal activity, the concern is that, in utilising surveillance devices, officers will capture legitimately private activity.[100] Where that activity has no relation to the alleged illegal activity, the state can have no interest in retaining it. Hence it is of concern that the Bill not only contains an implicit presumption against destroying irrelevant, inadvertently captured, potentially private activity, but that destruction of that material is subject to the discretion of the judge receiving the warrant report. The provision also significantly increases judicial influence in monitoring the actions and consequences of law enforcement agencies from an early stage, which, as the Chief Justice asserted, presents an inappropriate expansion of the courts' role.[101]

This approach is at odds with overseas jurisdictions[102] and the current interception device regime, which contains strict provisions directing the destruction of acquired evidence. Under s 312I(1) of the Crimes Act, any person who intercepts a private communication "must, as soon as practicable", destroy any records that are irrelevant to the specific crimes for which interception devices are permitted to be used. Furthermore, relevant records must be "destroyed as soon as it appears that no proceedings, or no further proceedings, will be taken".[103] Clearly the interception device regime was drafted so as to grant police

---

[99] SSB, cls 55(1)(a) and 56(1)(a).

[100] *R v Williams*, above n 11, at 231.

[101] Chief Justice of New Zealand, above n 59, at [21]; see Simon Bronitt and James Stellios "Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects" (2005) 29 Telecomm Pol'y 875 at 882–885.

[102] See mandatory destruction provisions: Regulation of Investigatory Powers Act 2000 (UK), s 15(3); Surveillance Devices Act 2004 (Cth), s 46; Crime and Misconduct Act 2001 (Qld), s 131; Surveillance Devices Act 1998 (WA), s 41; Surveillance Devices Act 1999 (Vic), s 36; Surveillance Devices Act 2007 (NSW), s 41. Cf Surveillance Devices Act 2007 (NT), s 45(5); Listening and Surveillance Devices Act 1972 (SA), s 6C (prescribing a discretion not to destroy evidence).

[103] Crimes Act 1961, s 312J(1).

no greater powers than they need to gather evidence, with the rights of the individual central to the focus. Overseas jurisdictions contain similar provisions. The United Kingdom and most Australian jurisdictions state that the presiding judge or magistrate must order the destruction of evidence that is irrelevant to an investigation or that no longer needs to be retained.[104]

The Bill on the other hand raises serious questions about what will happen to retrieved material after its usefulness in an investigation expires. If material is not destroyed there is a concern that it might be kept in an archive or a surveillance database, an expansion of police authority that is not warranted by the Bill. The legislature should therefore introduce a provision into the Bill similar to the interception device requirement, so that there is a presumption in favour of destroying irrelevant surveillance footage. This would reduce the need for judicial interference, and would strike a better balance between the privacy concerns of individuals and law enforcement requirements, which indicate no obvious need to retain irrelevant footage.

2. Judge May Refer Breaches of Conditions

A second discretion given to the judge upon receiving a report is whether or not to refer breaches of the warrant conditions under cl 46, or non-compliance with cl 44, to the relevant agency's chief executive.[105] It is not apparent why this provision falls to a judge to determine — the Chief Justice considered it to be an "Executive responsibilit[y] not appropriately conferred upon Judges"[106] — nor why referring breaches is discretionary. Where an officer breaches the conditions of a warrant, or the emergency surveillance boundaries, it should be mandatory to report the breach. The extent of the breach, or whether the officer intentionally or innocently committed it, are

---

[104] See Regulation of Investigatory Powers Act 2000 (UK), s 15(3); Surveillance Devices Act 2004 (Cth), s 46; Crime and Misconduct Act 2001 (Qld), s 131; Surveillance Devices Act 1998 (WA), s 41; Surveillance Devices Act 1999 (Vic), s 36; Surveillance Devices Act 2007 (NSW), s 41. Cf Surveillance Devices Act 2007 (NT), s 45(5); Listening and Surveillance Devices Act 1972 (SA), s 6C (prescribing a discretion not to destroy evidence).

[105] SSB, cls 55(1)(b) and 56(1)(b).

[106] Chief Justice of New Zealand, above n 59, at [21].

irrelevant considerations.

Ideally, referring all breaches would serve dual purposes. First, it would facilitate the re-training or disciplining (where necessary) of the officer who committed the breach. Secondly, it would highlight the breach so that steps could be taken to prevent similar breaches in the future. The Law Commission discussed in detail the benefits of reporting:[107]

> Reporting requirements enable the supervision and monitoring of the exercise of enforcement powers. Reporting also enables information on the use of these powers to be collated so that their value, their appropriateness to the particular circumstances in which they are exercised, and the necessity for any changes in substance or procedure can be assessed.

An internal oversight procedure may be more suitable than requiring judges to regulate all breaches. Regardless, the phrases stating that breaches of the Bill *may* be reported should be redrafted to state that they *must* be reported. This is crucial to the transparency of the justice system, perceived legitimacy of police actions, and effectiveness of the Bill. In the absence of such an amendment, it is hoped that judges will approach their discretion not to refer breaches cautiously.

3. Judge May Order Notification

The third and most concerning discretion imparted to the judge is whether or not to order that the subject of the surveillance be notified after the fact.[108] The Law Commission, originally in favour of a notification presumption, changed its stance after "enforcement agencies pointed out that this had the potential to seriously compromise ongoing or future enforcement operations".[109] The Commission identified that it can take months or years for surveillance evidence to trickle down to a prosecution, and prematurely alerting a suspect to the presence of surveillance has the potential to compromise future investigations.

---

[107] LCR, above n 2, at 433.

[108] SSB, cls 55(1)(c) and 56(1)(c).

[109] LCR, above n 2, at 341.

In light of this, the Commission recommended reversing the presumptive approach: notification should be given within seven days after the conclusion of surveillance unless a judge grants postponement or dispensation. Where an officer seeks to suspend notification, the judge should do so unless she is satisfied that there is no risk of prejudice to any ongoing or future investigations. This in itself would be sufficient to block the notification of a number of surveillance targets (in appropriate circumstances). For instance, it would have allowed the police in *R v Bailey* to postpone notification while successive warrants were sought during the lengthy investigation into the Urewera training camps.[110] But the Bill goes considerably further.

Under cls 55(2) and 56(2) of the Bill, a judge *must not* order that a surveillance target be notified of any surveillance unless the judge is satisfied that the public interest in notification outweighs any potential prejudice to:[111]

> (a) any investigation by the law enforcement agency:
> (b) the safety of informants or undercover officers:
> (c) the supply of information to the law enforcement agency:
> (d) any international relationships of the law enforcement agency.

In addition to this requirement, the judge *must not* order notification unless she is satisfied that the warrant should not have been issued, or that there was a serious breach of any of the conditions in the warrant or any applicable statute, or that there was a serious breach of the cl 44 criteria.[112]

The test under the Bill raises the threshold so high that, when applying the opt-out provision, it would be near impossible for anyone to be notified of the fact that they have been the subject of state surveillance. Even if an officer used a surveillance device in a manner that clearly

---

[110] *R v Bailey*, above n 7. Though see criticisms in HRF & ACCL, above n 40, at [19], concerning the potential for police to abuse the opt-out procedure.

[111] SSB, cls 55(3) and 56(3).

[112] SSB, cls 55(2)(b) and 56(2)(b).

breached the law or a person's rights, the person would have no opportunity to be notified of this fact where the public interest did not outweigh "any potential prejudice" to a variety of state interests. Also, a person who was wrongly surveilled in a manner which violated that person's reasonable expectation of privacy would have no prospect of being notified unless the high threshold of illegality were met.

The second limb of the threshold test (requiring illegality) is unnecessary and encroaches too far on individual rights. At the least this limb should be removed from the Bill. In her Select Committee Submission, the Privacy Commissioner advised that "notification after the fact should be a matter of course".[113] Citizens ought to know when their government has been watching them. The Commissioner recommended that the clauses be amended to include a stricter presumption in favour of notification, or alternatively, the imposition of a "standing obligation on the agency or enforcement officer to notify the subjects of surveillance device warrants that the surveillance has occurred".[114] The Law Commission also recommended that judges be able to give directions as to the person or people to be notified — a recommendation that was not incorporated into the Bill.[115] The legislature should take note of these concerns. Surveillance is intended to be undetectable; without an adequate notification requirement, subjects of surveillance will usually have no way of ever knowing when the state has been targeting them. Such a position runs counter to the principles of a free democracy, and unduly favours law enforcement interests above privacy rights and legitimate disclosure considerations.

Conclusion

Notwithstanding the Select Committee's acceptance that the current drafting of the Bill requires substantial improvement,[116] a

---

[113] Privacy Commissioner "Submission to the Justice and Electoral Committee on the Search and Surveillance Bill 2009"; see New York Criminal Procedure Law, § 700.50.3: notification within a "reasonable time" or no later than 90 days; Canadian Criminal Code, s 487.01(5.1): notification within a "reasonable time".

[114] Privacy Commissioner, above n 113, at 3: a mere letter would be sufficient notification.

[115] LCR, above n 2, at 343.

[116] Justice and Electoral Committee, above n 1.

comprehensive surveillance regime is necessary for New Zealand. From a system where targeted visual surveillance receives almost no statutory regulation, the Bill extends a wide surveillance warrant regime which applies to any offence punishable by imprisonment. The new warrant regime will facilitate the use of surveillance devices in police investigations by clarifying the circumstances in which surveillance is permissible. Nevertheless, the Bill contains some ambiguities, particularly in regard to surveillance beyond the curtilage and the 'private activity' condition. Clarification of these issues would better determine the scope of the warrant requirement; as a corollary it would indicate those circumstances in which warrantless surveillance is not prohibited by the Bill.

The circumstances in which warrantless emergency surveillance is permissible are rightly narrow. Warrantless surveillance should be preferably avoided and permitted only when necessary. If surveillance is conducted without a warrant in circumstances where a warrant ought to have been sought it is likely to constitute both a violation of the Bill and a breach of s 21 of the NZBORA.[117] Such breaches will have a direct impact on the admissibility of evidence at trial.[118] Theoretically, breaches will also result in consequences at the reporting stage, although this article has canvassed the inadequacies of those provisions. Reform of the reporting provisions — introducing a presumption in favour of destruction of irrelevant material, reporting of breaches, and notification after the fact — is appropriate. While the Bill in its present form fails to reconcile adequately legitimate law enforcement interests and human rights values, it is hoped that a redrafted Search and Surveillance Bill will strike a more satisfactory balance.

---

[117] *R v Williams*, above n 11, at 221–222, 271; *R v Laugalis* (1993) 10 CRNZ 350 (CA) at 355–356.

[118] See Evidence Act 2006, s 30.