Closed-Circuit Television in New Zealand

SIOBHAN CERVIN*

I INTRODUCTION

The explosive growth of closed-circuit television ("CCTV") surveillance that has been experienced throughout the world in recent years cannot be exaggerated. Individuals are increasingly subjected to surveillance in town centres, city streets, public car parks, shopping precincts, banks, transport services, workplaces, and a variety of other public and private spaces.[1] In New Zealand, local authorities and the police have been quick to proclaim the value of CCTV surveillance technology in reducing the incidence of crime and other anti-social behaviour, and in improving public perceptions of safety. However, warnings by the United Kingdom Information Commissioner that the United Kingdom is "sleepwalking into a surveillance society" have now reached New Zealand.[2] The Information Commissioner's concerns are echoed by La Forest J in the Supreme Court of Canada, who warns that the very efficacy of surveillance technologies — if left unregulated — threatens to annihilate reasonable expectations of privacy.[3] This article assesses whether the current legal framework governing state CCTV surveillance in New Zealand adequately protects citizens and society from the harmful effects of CCTV surveillance. It responds to the New Zealand Law Commission's recent call for submissions on whether or not CCTV surveillance should be regulated.[4]

Part II examines the significance of the discussion of state CCTV surveillance. In doing so, the remarkable advances in CCTV technology, and the international growth of state CCTV surveillance as a law enforcement tool, are charted. The significance of the issues raised by CCTV surveillance is discussed by reference to the surveillance literature and the predominant objectives and purposes for which surveillance is implemented. The article proceeds, in Part III, to consider the current

---

* BA/LLB(Hons), Solicitor, Simpson Grierson. The author would like to thank Assoc. Prof. Scott Optican of the University of Auckland Faculty of Law for his support and feedback. The author would also like to extend her gratitude to Maurice and Anne-Marie Cervin, whose encouragement has been invaluable.

1 Petersen, *Understanding Surveillance Technologies: Spy Devices, Privacy, History and Applications* (2 ed, 2007) 541.

2 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, 2008) 25 ["*Privacy: Concepts and Issues*"]; see also House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State* (HL 18–I, 2009) 5.

3 *R v Duarte* [1990] 1 SCR 30 [24] per La Forest J.

4 Palmer, "Release of Law Commission's Issue Paper on Invasion of Privacy" (Media Release, 6 March 2009) <http://www.lawcom.govt.nz/UploadFiles/Publications/Publication_129_428_Press%20Release%20060309/html/Publication_129_428_Press%20Release%20060309.html> (at 14 July 2009).

legal framework governing state CCTV surveillance in New Zealand. In particular, the Privacy Act 1993, the police policy on CCTV in public places ("Police Policy"),[5] and the New Zealand Bill of Rights Act 1990 ("NZBORA") are examined.

The inability of the current legal framework to address the concerns of state CCTV surveillance adequately is built upon in Part IV, which discusses the need for regulation. In particular, the article examines the popular assumptions that CCTV surveillance is effective in reducing the incidence of crime and increasing public perceptions of safety. It is contended that the available evidence debunks such common assumptions, raising concerns regarding the justification and proportionality of implementing state CCTV surveillance. Accordingly, Part V calls for a comprehensive legislative framework governing the implementation, continuation, and operation of state CCTV surveillance in New Zealand. Several proposals are advanced, drawing upon international experience.

II SIGNIFICANCE OF CCTV SURVEILLANCE

Importance of Discussion

In many ways, the perception of state CCTV surveillance epitomizes the debate surrounding the rise of a surveillance state: "[w]hilst its use and further development is accepted without question and welcomed in some quarters, to others it symbolizes the worst excesses of a surveillance society."[6]

For many, state CCTV surveillance represents a significant threat to the tenets of a free democratic society. Excessive and irrelevant surveillance of the public sphere is perceived as diminishing the privacy of individuals and undermining their personal autonomy, dignity, and ability to develop and flourish.[7] Moreover, increased self-consciousness increases inhibition, chilling freedom of expression and association.[8] It has been argued that pervasive surveillance of an individual in public will reveal more information than traditional searches of that individual's personal belongings.[9]

---

5 New Zealand Police Commissioner, *Policy on Crime Prevention Cameras (CCTV) in Public Places* (2003) <http://www.police.govt.nz/resources/2003/cctv/index.html> (at 14 July 2009).

6 House of Commons Home Affairs Committee, *A Surveillance Society* (HC 58–I, 2008) 63.

7 Ibid 38; New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 38, 43, 138; Austin, "Privacy and the Question of Technology" (2003) 22 Law & Phil 119, 144; Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego L Rev 745, 765 ["Nothing to Hide"].

8 Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity" (2004) 82 Tex L Rev 1349, 1410.

9 Ibid 1359.

Further, an individual may suffer distress, embarrassment, and humiliation as a result of the disclosure of CCTV recordings.[10] Individual harm arises irrespective of whether the CCTV recordings are inadvertently or intentionally disclosed to the wider public or unauthorized persons.[11] The potential for CCTV surveillance to be abused also gives rise to concern. CCTV surveillance may be operated in a discriminatory manner, targeting those sections of society that are considered undesirable.[12] Such discrimination leads to the potential that individuals may be excluded from the public sphere. In light of the concerns identified, the relatively nonchalant reception of state CCTV surveillance by the public is surprising.[13] As the government of British Columbia recognized, the public may come to regret the introduction of mass CCTV surveillance over time:[14]

> There is a very real risk that within a few short years British Columbians could find themselves subjected to pervasive, routine and random surveillance of their ordinary, lawful public activities.... In and of itself, each system might be lawful and reasonable, but the synergy of all systems operating together is something the public is likely to regret.

Consequently, the time to address the harmful implications emanating from state CCTV surveillance is now.

The Terminology and Technology

The term 'closed-circuit television' has evolved from its original meaning, based on the distinction between private and broadcast television, to encompass all forms of visual surveillance systems. The terminology applies irrespective of the technological specifications of the particular system.[15] The phrase 'CCTV surveillance' is thus commonly understood to refer simply to the continuous or periodic visual monitoring or recording of the general public.[16] Although CCTV surveillance is extensively implemented throughout the private sector, this article is confined to an analysis of CCTV surveillance employed by the state.

---

10 Gallagher, "CCTV and Human Rights: The Fish and the Bicycle? An Examination of *Peck v United Kingdom* (2003) 36 EHRR 41" (2004) 2 Surveillance & Society 270, 275–276; Austin, supra note 7, 147.

11 House of Commons Home Affairs Committee, supra note 6, 32.

12 Ibid 38.

13 Blitz, supra note 8, 1375; Goold, *CCTV and Policing: Public Area Surveillance and Police Practices in Britain* (2004) 20–21.

14 Office of the Information and Privacy Commissioner for British Columbia, *Public Surveillance System Privacy Guidelines* (Government of British Columbia, 2001) <http://www.oipcbc.org/advice/VID-SURV(2006).pdf> (at 14 July 2009) 1 ["*Guidelines*"]; Petersen, supra note 1, 541–542.

15 New Zealand Law Commission, *Privacy: Concepts and Issues,* supra note 2, 140; Goold, supra note 13, 12.

16 Ministry of Service Alberta, *Freedom of Information and Protection of Privacy: Guide to Using Surveillance Cameras in Public Areas* (Government of Alberta, 2004) <http://foip.gov.ab.ca/resources/publications/SurveillanceGuide.cfm> (at 14 July 2009) 1–2 ["*Guide to Using Surveillance*"].

Visual surveillance devices used by CCTV surveillance systems have come a long way from the grainy black and white pictures of times past.[17] Continuous improvements have seen visual surveillance cameras equipped with high-definition colour, date and time software, indefinite storage, and zoom, tilt, and pan capabilities that may be controlled by automatic pilot or operated remotely.[18] These substantial improvements enhance natural eyesight, allowing a person to see further, more clearly, in greater detail, and in difficult conditions.[19]

The capabilities of CCTV surveillance devices continue to develop apace. New generations of CCTV cameras are capable of monitoring "suspicious behaviour", announcing orders to people, and sounding alarms.[20] The technology to lip-read, see through clothing for concealed objects, identify and track persons through crowds, and judge an individual's temperament is being developed.[21]

New Zealand police are embracing these technological developments. Facial recognition software has already been purchased and will allow faces captured by CCTV cameras to be checked against a database holding approximately 800,000 images of convicted offenders.[22] The police have also signalled their intention to upgrade their technology, developing a wireless broadband network that can be controlled remotely.[23]

Current Use

The exponential growth of CCTV surveillance internationally is impressive. Over 26 million surveillance cameras have been introduced worldwide within a few decades.[24] The United Kingdom, described as having the most watched citizenry, has led the world in state CCTV surveillance, with the number of cameras estimated to be increasing at a rate of 500 per week.[25]

17 For an extensive discussion of the evolution of video surveillance and its many applications throughout society, see Petersen, supra note 1.

18 Gill and Spriggs, *Assessing the Impact of CCTV* (Home Office RS292, 2005) xii, 2; Petersen, supra note 1, 484; New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 136, 140; Blitz, supra note 8, 1353; Pomerance, "Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the 'Inviolate Personality'" (2005) 9 Can Crim L Rev 273.

19 An East London shopping centre has installed facial recognition technology, which, when linked to a database of local offenders, sounds an alarm when a match is detected. The technology is expected to be piloted in airports and border checkpoints in the near future. Petersen, supra note 1, 469; Blitz, supra note 8, 1352.

20 New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 141.

21 Ibid; Blitz, supra note 8, 1353.

22 Pullar-Strecker, "Police Embrace Face Scans", *Stuff*, Wellington, New Zealand, 1 October 2007 <http://www.stuff.co.nz/technology/34775> (at 14 July 2009); "Learning to Live with Big Brother", *The New Zealand Herald*, Auckland, New Zealand, 1 October 2007; Petersen, supra note 1, 520.

23 Pullar-Strecker, supra note 22.

24 Farmer and Mann, "Surveillance Nation: Part One" (2003) 106 Technol Rev 34, 36 ["Surveillance Nation: Part One"].

25 Goold, supra note 13, 1–2.

The pervasiveness of state CCTV surveillance in the United Kingdom has prompted some to describe CCTV as the country's "fifth utility".[26]

Early CCTV systems were funded through local authorities, police, and commercial interests. However, the late-1990s saw the true honeymoon of CCTV. While in March 1995 over 90 CCTV systems were in operation, by 1998 this had skyrocketed under the Home Office Crime Reduction Programme CCTV Initiative. A central part of the United Kingdom government's law and order campaign, this initiative saw 684 CCTV systems funded at a cost of £170 million.[27] At one point, the Home Office was spending 79 per cent of its budget for crime prevention on the installation and development of CCTV surveillance.[28] Criminologist Clive Norris has estimated that the average Londoner can expect to be captured by over 300 cameras per day.[29] Additionally, the government has openly encouraged businesses in the private sector to install CCTV surveillance.[30]

While the development of state CCTV surveillance in the United Kingdom has been well-documented, the Canadian situation has been largely ignored.[31] The purported success of CCTV surveillance in reducing crime in the United Kingdom was likely to have been instrumental in influencing numerous Canadian cities to implement their own CCTV systems. The first city to introduce CCTV was Sherbrooke, Quebec, in 1991. In 1996, the Ontario city of Sudbury introduced its "Lion's Eye in the Sky" — the first project in Ontario to use CCTV monitoring as a law enforcement tool.[32] Today there are more than 13 reported CCTV systems operating, with many more being proposed.[33]

By one estimate, the United States boasts more than 11 million CCTV surveillance cameras.[34] CCTV surveillance is extensive in New York, with many clandestine private surveillance cameras. A 1998 survey by the New York Civil Liberties Union identified 2,397 visible surveillance cameras

---

26 The first four are gas, electricity, water, and telecommunications. New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 140.

27 For a full list of approved schemes, see United Kingdom Home Office, "Crime Reduction: Mini-sites" (2009) <http://www.crimereduction.homeoffice.gov.uk/mini-sites.htm> (at 14 July 2009); Goold, supra note 13, 18; Blitz, supra note 8, 1352; Gill and Spriggs, supra note 18, 1.

28 Goold, supra note 13, 40.

29 Farmer and Mann, Surveillance Nation: Part One, supra note 24, 35; New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 140.

30 Gallagher, supra note 10, 271–272.

31 Walby, "Open-Street Camera Surveillance and Governance in Canada" (2004) 4 CJCCJ 655, 658 ["Open-Street Camera"].

32 Greater Sudbury Police Service, "Lion's Eye in the Sky" <http://www.police.sudbury.on.ca/lionseye.php> (at 14 July 2009).

33 Cities with CCTV systems include Hamilton, London, Toronto, Windsor, Peterborough, Sturgeon Falls, and Tehssalon, Ontario; Edmonton, Alberta; Antigonish, Nova Scotia; Kelowna, British Columbia; and Montreal and Baie-Comeau, Quebec. Ibid 660.

34 Farmer and Mann, Surveillance Nation: Part One, supra note 24, 36.

at street level in Manhattan.[35] The area from Greenwich Village to Soho had 769 cameras. A count of this area seven years later revealed that the number of cameras had increased to 4,176.[36] In 2006, the New York Police Department ("NYPD") announced the development of a "citywide system of CCTV", which would be funded by a $9 million grant from Federal Homeland Security and up to $81.5 million in federal counter-terrorism funding.[37] Other major United States cities that have implemented CCTV systems include Baltimore, Washington DC, Philadelphia, Los Angeles, Oakland, Tacoma, Seattle, Charleston, and Chicago.[38]

New Zealand local councils are beginning to follow the international trend in implementing CCTV systems in their communities. Most CCTV systems are owned by the local government or business groups but are operated by the police or with police support. The exact number of surveillance cameras in operation remains unknown.[39] Several local councils have CCTV systems in their main streets, including Lower Hutt, Wanganui, Hastings, Napier, and Gisborne.[40] The Auckland City Council operates 49 cameras in the central business district in a joint venture with a business group, Heart of the City, and the police.[41] In 2007, the Waimakariri District Council upgraded its older CCTV system to a wireless one, with higher specification cameras that capture better quality images during both the day and night, and have greater storage capacity. The CCTV system is controlled by local police and monitored by volunteers.[42]

Finally, the Manukau City Council provides the most helpful and illuminative case study in New Zealand. The Council undertook a 16-month in-depth review of its CCTV system, culminating in the development of a CCTV surveillance strategy. It installed its first CCTV system in 2001. By 2006, the Council was responsible for 100 CCTV cameras throughout council premises, 19 public CCTV cameras, and approximately 40 traffic management CCTV cameras, at a cost of approximately $2.1 million.[43]

This nonchalant reception of general video surveillance in the United Kingdom, Canada, the United States, and New Zealand stands in stark contrast to its reception in continental Europe. The French National Committee on Computer Data and Individual Freedom first began to oppose the introduction of state CCTV surveillance as early as 1986. In 1995,

---

35 Siegel, Perry, and Gram, "Who's Watching? Video Surveillance in New York and the Need for Public Oversight" (2006) New York Civil Liberties Union <http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf> (at 14 July 2009) 2; Petersen, supra note 1, 543.

36 Siegel, Perry, and Gram, supra note 35, 2.

37 Ibid.

38 Klein, "Police Go Live Monitoring DC Crime Cameras", *The Washington Post*, Washington DC, United States, 11 February 2008 <http://www.washingtonpost.com/wp-dyn/content/article/2008/02/10/AR2008021002726.html> (at 14 July 2009); Blitz, supra note 8, 1352.

39 New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 140.

40 Ibid.

41 Ibid.

42 "Technology Keeps Cameras Rolling in Rangiora", *New Zealand Local Government*, Auckland, New Zealand, May 2007 <http://www.risc.co.nz/docs/technology.pdf> (at 14 July 2009) 18.

43 Manukau City Council, *Closed Circuit Television Camera (CCTV) Strategy* (2006) 7.

the French Government enacted legislation governing the introduction and control of CCTV, the practical effect of which was to severely restrict its growth.[44] In Germany, the Federal Constitutional Court prohibited state CCTV surveillance in 1983 when it recognized the "right of informational self-determination" based on Article II of the German Constitution.[45] Today, the German position remains relatively unchanged, with opposition to CCTV remaining strong: one Chief Superintendent of Leipzig has stated that "we do not want an English situation".[46] In Sweden, police must obtain authorization to install a CCTV system.[47] The different reaction CCTV surveillance has received in continental Europe indicates that the technology has not been universally embraced as a reasonable, admirable, and benign law enforcement tool.

Fear of a Surveillance State

The unprecedented growth in visual surveillance has been accompanied by an equally impressive growth in the surveillance literature declaring "the death, destruction and utter end of privacy in our society and an emerging, if somewhat disturbing, transparency".[48] Throughout the surveillance literature, privacy advocates relentlessly employ the evocative imagery of George Orwell's prophetic *1984*, Jeremy Bentham's and Michel Foucault's ubiquitous 'panopticon', and Anthony Giddens' description of the totalitarian state.[49] The imagery serves to illustrate the persistent and disturbing theme that state surveillance is out of control, and society is in constant danger of degenerating into an authoritarian or totalitarian state.[50] Privacy International, a privacy advocacy organization, succinctly captures this prevailing concern:[51]

> There is a grave risk that the CCTV industry is out of control. Fuelled by fear of crime, the systems take on a life of their own, defying quantification and quashing public debate. In a very short time, the systems have challenged some fundamental tenets of justice, and created the threat of a surveillance society. Other more traditional approaches to law enforcement and social justice are being undermined without due process.

---

44 Goold, supra note 13, 21–22.

45 Ibid 22–23.

46 Gras, "The Legal Regulation of CCTV in Europe" (2004) 2 Surveillance & Society 216, 222.

47 Ibid 223.

48 Austin, supra note 7, 120.

49 Ibid 139–140; Walby, Open-Street Camera, supra note 31, 657, 660; Petersen, supra note 1, 470; Blitz, supra note 8, 1350; Goold, supra note 13, 5–7.

50 New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 25; Goold, supra note 13, 5–7; Austin, supra note 7, 120.

51 Privacy International, "Privacy International Statement on CCTV" (Media Release, 15 October 1996) <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61926> (at 14 July 2009).

As Goold emphasizes, however, the analogies drawn highlight an assumption that surveillance is inherently related to authoritarianism and totalitarianism.[52] Yet the reality is very different to the picture painted by privacy advocates, as only a small minority of CCTV systems currently possess advanced capabilities.[53] Rather, privacy advocates are concerned with possible future advances in CCTV surveillance. When examining the position in New Zealand, it is necessary to distinguish the capabilities of current CCTV systems, or proposals for new or expanded ones, from the possible developments that might be implemented in the future.

The hyperbole characterizing the surveillance literature may be challenged in two further respects. First, Orwell's 'Big Brother' description did not envisage a key feature of modern surveillance — the extent to which private organizations have embraced CCTV. In fact, the private sector is generally ahead of the state in exploiting CCTV surveillance.[54] In the United States, for example, nearly US$100 billion is spent annually on surveillance equipment devices, with a purported 50 per cent of sales attributable to private commercial organizations.[55] Interestingly, many private CCTV systems are not installed in areas suffering a high incidence of crime. On the contrary, CCTV is prevalent in well-to-do areas, such as up-market shopping strips, entertainment centres, and down-town commercial areas. Business entrepreneurs promote CCTV surveillance not only in the belief that it prevents crime and protects customers, but perhaps also because it provides the opportunity to socially engineer the environment through the eviction of undesirable people.[56]

Consequently, rather than being watched by one 'Big Brother', it is more accurate to say that society is being watched by hundreds of "little brothers".[57] The prevalence of private CCTV surveillance is significant in challenging assumptions that CCTV surveillance reflects a power struggle between citizens and an over-zealous state.

The trend for private CCTV surveillance systems implemented by business entrepreneurs has arrived in New Zealand. In 2007, the Newmarket Business Association installed 14 CCTV cameras in Newmarket, an up-market Auckland shopping precinct, at a cost of $70,000 per annum to ratepayers. In response to media speculation that Newmarket must be

52 Goold, supra note 13, 5.

53 Ibid 8.

54 Ibid 2.

55 Nieto, *Public Video Surveillance: Is it an Effective Crime Prevention Tool?* (California Research Bureau, 1997) 12; see also Farmer and Mann, "Surveillance Nation: Part Two" (2003) 106 Technol Rev 46, 48.

56 For a discussion of the impact of private surveillance upon urban space, and the relationship between private surveillance and the police, see Wakefield, "The Public Surveillance Functions of Private Security" (2004) 2 Surveillance & Society 529, 530; see also Bickel, Brinkley, and White, "Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?" (2003) 33 Stetson L Rev 299, 314.

57 Walby, Open-Street Camera, supra note 31, 662; Petersen, supra note 1, 470.

suffering from a crime wave to justify the installation, Cameron Brewer, the manager of the Newmarket Business Association, remarked:[58]

> No no not at all. The police in the past 12 months have told me one thing we don't have in Newmarket is violent crime. Rarely do we have flare-ups after dark and we don't have any problems with our liquor licences.

Reminiscent of promotions in the United Kingdom, details surrounding the operation of the Newmarket system were noticeably absent,[59] the emphasis instead being on the technical specifications of the system. While it was disclosed that the CCTV system would be kept in the local police station, it remains unclear who retains ultimate responsibility: the police, the security company, the council, or the Newmarket Business Association. In May 2009, the Newmarket Business Association and the local police reported a 22 per cent reduction in thefts in Newmarket during the previous 12 months, attributing some of this success to the new CCTV system.[60]

Secondly, agitation for implementing state CCTV surveillance has frequently come from businesses and citizens themselves. Again, to the extent that businesses and citizens campaign for and support the introduction of CCTV systems, the reigning metaphor holding 'Big Brother' responsible is undermined. The United Kingdom Information Commissioner recently advised the House of Commons Affairs Select Committee that "the population likes cameras and cannot get enough of them".[61] In the past, concerned citizens have mobilized around a common grievance campaign for the implementation of a CCTV system, under a belief that it will solve a perceived crime epidemic. In London, Ontario, for example, 16 surveillance cameras were introduced following a successful campaign by the citizens' initiative, Friends Against Senseless Endings.[62] Significantly, the campaign promoted CCTV surveillance before the police did, and informed the development of the Police Policy.

Justifications and Policies

Surveillance cameras are promoted as an effective and valuable resource that is indispensable to law enforcement. The prevailing belief that CCTV surveillance will deter and prevent crime is premised on the assumption that offenders will realize that the benefits of offending are outweighed by

58 Brewer, cited in Rudman, "Big Brother Appearing in Act on Broadway", *The New Zealand Herald*, Auckland, New Zealand, 28 November 2007 <http://www.nzherald.co.nz/government/news/article.cfm?c_id=49&objectid=10478746> (at 14 July 2009).

59 Brewer asserted that "only those that have something to hide will have something to fear": ibid.

60 "CCTV Keeps Down Crime in Newmarket", *The New Zealand Herald*, Auckland, New Zealand, 24 May 2009 <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10574288> (at 14 July 2009).

61 House of Commons Home Affairs Committee, supra note 6.

62 Friends Against Senseless Endings was mobilized following the violent murder of a young man, which was widely reported by the media. Walby, Open-Street Camera, supra note 31, 673.

the risk of being caught and punished.[63] As a result, CCTV surveillance is expected to reduce the incidence of crime and anti-social behaviour.

In New Zealand, the police have stated that the objective of CCTV surveillance is "to reduce the incidence of crime and disorder, so members of the community feel safe when visiting the public areas covered by the cameras".[64] Similarly, local councils have introduced CCTV surveillance with a goal of preventing or reducing crime and other anti-social behaviour, and of improving public perceptions of safety within town centres.[65]

CCTV surveillance is presumed to reduce the fear of crime as it allows members of the general public to frequent public spaces safely. As a result, natural surveillance of the area increases, which further deters potential offenders. Further, CCTV surveillance is considered to be a mechanism that reminds the public to be security conscious, and to take appropriate steps to keep safe. It is frequently cited as a means of improving police response times, thereby increasing public safety, and reducing costs through the efficient allocation of police resources.[66] CCTV surveillance is also attributed with reducing costs by facilitating the investigation and identification of offenders, and obtaining convictions through speedier prosecutions.[67] For some, when compared with the above purposes, concerns in the surveillance literature appear pessimistic, overdramatic, and unrealistic. The objectives of CCTV surveillance are perceived as utterly reasonable, admirable, and benign.[68] But are they?

III THE CURRENT LEGAL FRAMEWORK

This Part explores the ways in which state CCTV surveillance has been regulated in New Zealand and overseas. The discussion begins by outlining the applicable regulatory framework in New Zealand and assessing its strengths and weaknesses.

The Current Legal Framework in New Zealand

New Zealand has no comprehensive legislation prohibiting or authorizing CCTV surveillance. There is a lacuna in the law. Local authorities, the police, and private organizations have an absolute discretion to introduce

63 Armitage, *To CCTV or Not to CCTV? A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime* (Nacro, 2002) <http://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf> (at 14 July 2009) 2.

64 New Zealand Police Commissioner, supra note 5.

65 Manukau City Council, supra note 43, 15.

66 This is, of course, dependent upon the CCTV system being monitored live.

67 See Walby, Open-Street Camera, supra note 31; Petersen, supra note 1, 520; Nieto, supra note 55, 1; Gill and Spriggs, supra note 18, 1–7; Goold, supra note 13, 3.

68 Gallagher, supra note 10, 271–272.

and maintain CCTV surveillance systems. However, as the Manukau strategy identifies, CCTV systems must be operated in a manner consistent with the Privacy Act 1993.[69]

The police are subject to further regulation under the Police Policy, which was developed in association with the Office of the Privacy Commissioner.[70] It provides that the police may support and work in conjunction with local authorities and other groups wanting to install CCTV systems in public places for the purposes of crime prevention.[71] The Police Policy governs all proposals for new CCTV systems and the expansion of existing systems.

1 Strengths of the Current Legal Framework

The Police Policy represents a positive contribution to the regulation of state CCTV surveillance. It provides a set of rules that apply the principles of the Privacy Act to the operation of CCTV surveillance. As a result, emphasis is placed upon prescriptive rules surrounding the storage, retention, and use of the surveillance footage. For example, surveillance must be clearly labelled, access to the monitors and archived surveillance footage must be restricted to authorized persons only, and the purposes for which surveillance may be used are restricted to inquiries for an investigation or prosecution, training purposes, or research.[72]

The Police Policy also addresses, to a limited extent, some of the wider implications of state CCTV surveillance. First, there is a retention period of two months, after which the records must be completely and securely destroyed. This obligation is significant as it addresses concerns that state CCTV surveillance may chill the public sphere, by ensuring that the public are not exposed to a permanent risk of surveillance footage reappearing years later.[73]

Secondly, the public must be consulted prior to the installation of a new CCTV system, or the expansion of an existing one. The Privacy Commissioner must also be notified of this consultation process. The obligation to consult with the public is important as it provides citizens the opportunity to contribute to the decision of implementation. Moreover, the Police Policy requires that prominent and clear signs be installed at the perimeter of the target area to notify the public of the presence of CCTV surveillance.

Thirdly, the Police Policy addresses concerns regarding the arbitrary, continuous, and targeted surveillance of individuals. Crucially, the positioning of the camera must be justified by reference to statistics

69 Manukau City Council, supra note 43, 10.

70 The Police Policy was last updated in November 2003: ibid Appendix 1, 2.

71 New Zealand Police Commissioner, supra note 5.

72 Ibid 2–5.

73 Blitz, supra note 8, 1411.

concerning specific crimes, such as car theft, assault, or drugs.[74] Continuous 24-hour monitoring is also prohibited, with operational hours restricted to times where it can be shown that there is a higher likelihood of offences being committed and detected by the camera.[75] These requirements reflect the need for cameras to be justified as necessary and proportionate in the circumstances.

Further, unless there is a reasonable suspicion that an offence is taking place, cameras are prohibited from tracking or zooming in on any person, monitoring the entrance of a building, or viewing through a building's windows (unless it is part of a wide angle, long shot, or pan). These prohibitions reflect the purpose of surveillance: "[c]rime prevention cameras are not used to maintain surveillance on individuals or groups — they are to prevent and detect criminal offences in identified high crime areas."[76]

2 *Weaknesses of the Current Legal Framework*

The current legal framework governing state CCTV surveillance is weak and ineffective. The framework employs codes of conduct and industry guidelines, rather than legislative provisions. The principal concern is that 'soft-regulation' effectively relies on the co-operation and goodwill of the relevant organizations.[77] As a regulatory regime, it provides insufficient safeguards and raises concerns regarding justification, accountability, and transparency.

In particular, the narrow focus on the management and security of personal information fails to appreciate and capture the wider implications and concerns arising from state CCTV surveillance:[78] namely, that excessive, irrelevant, or unnecessary surveillance may undermine a person's autonomy and dignity, and ultimately the nature of the public sphere. The Privacy Act deals merely with the consequences of interfering with privacy.[79] It does not address the preliminary and more important issue of whether the state should be permitted to implement CCTV surveillance in the first place. Further, the enforcement and investigation of the obligations under the Privacy Act are primarily dependent upon individual complaints made by the public to the Privacy Commissioner.[80] Compliance with the privacy legislation is thus perceived merely as an organizational or business cost, rather than a moral, social, or legal obligation.[81]

---

74 New Zealand Police Commissioner, supra note 5.

75 Ibid 1–2.

76 Ibid 1.

77 Ball et al, *A Report on the Surveillance Society* (Surveillance Studies Network, 2006) <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf> (at 14 July 2009) 83.

78 Gras, supra note 46, 217.

79 Ball et al, supra note 77, 77.

80 Norris and Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* (1999) 228; Gras, supra note 46, 218.

81 Lyon, *Surveillance Studies: An Overview* (2007) 176.

Despite going further than the Privacy Act, the Police Policy suffers from several fundamental weaknesses. Perhaps the most obvious shortcoming is its restrictive application. It applies only to the police, and is therefore not binding upon other state organizations, such as local councils. Consequently, there is no uniform guide that governs all forms of state CCTV surveillance.

While the Police Policy provides several mechanisms of accountability, the independence and enforcement of these are questionable. For example, the police are subject to periodic internal audits that examine operating standards and security, and a further annual review to examine the location, operation, effectiveness, and continuing necessity for the cameras. The review recognizes that CCTV surveillance requires ongoing justification, and contemplates that cameras should be removed where they are deemed no longer necessary.

The main criticism of the above review mechanisms is that they are too vague. It is debatable as to whether a police officer performing a review has the necessary experience and qualifications to undertake the complex task of assessing a system's effectiveness. The appropriateness of a member of the police assessing the continuing necessity of a CCTV system is also questionable. Audits should be encouraged to identify any non-compliance and areas in need of improvement. The Police Policy does not elaborate on the details of such audits. Questions left unanswered include who assesses the audits, where accountability rests, and what the consequences are for non-compliance.

The Privacy Commissioner has a right under the Police Policy to review the need for, and use of, any police crime prevention camera operation.[82] Police are required to disclose to the Privacy Commissioner a proposal outlining the justification for implementing a CCTV system, or the expansion of an existing one. Following installation, the police must disclose copies of the operating policies, the public notices issued, and periodic evaluation reports.[83] The role of the Privacy Commissioner is essential to independent accountability of the police. However, it remains unclear what power the Privacy Commissioner may exert. The obligations of disclosure are arguably no more onerous than merely keeping the Commissioner informed. Yet as Norris and Armstrong note, "[i]n the absence of effective democratic oversight and accountability we are in effect hostages to our faith that those operating and running such systems will do so in an enlightened way."[84]

The Police Policy fails to provide an adequate framework for regulating state CCTV surveillance. It is designed to ensure compliance

82 The Privacy Commissioners of Alberta and British Columbia possess a similar power. See Ministry of Service Alberta, supra note 16, 3–4; Ministry of Labour and Citizens' Services, *Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies* (Government of British Columbia, 2004) <http://www.lcs.gov.bc.ca/privacyaccess/main/video_security.htm> (at 14 July 2009).

83 New Zealand Police Commissioner, supra note 5; Manukau City Council, supra note 43, Appendix 1, 1–2.

84 Norris and Armstrong, supra note 80, 229.

with the narrow concerns protected under the Privacy Act. Where the Police Policy does address further issues regarding justification, accountability, and enforcement, it fails to go far enough.

Legal Frameworks Overseas

1 United Kingdom

The use of privacy protection legislation, supplemented by codes of practice to govern state CCTV surveillance, is also used overseas. In the United Kingdom, the state is authorized to implement and maintain CCTV surveillance systems without any approval process. This power is implied under a number of statutes, including the Local Government Act 1972, the Criminal Justice and Public Order Act 1994, and the Data Protection Act 1998.[85] In fact, the need to obtain planning permission to install CCTV surveillance was deliberately abolished in 1995.[86]

Like the New Zealand Privacy Act 1993, the Data Protection Act 1998 imposes obligations on the collection, use, and retention of personal information. Following a review and public consultation in August 2007, the Information Commissioner released the Code of Practice 2008 ("the Code"). The primary purpose of the Code is to establish standards that comply with the eight legally enforceable Data Protection Act principles, and to ensure that CCTV surveillance is used for limited purposes that are compatible with individual rights.[87] The Code itself remains unenforceable, and is therefore best described as merely a recommendation on good practice.

The Code goes further than the Data Protection Act by setting out a series of questions designed to assist in the decision of whether or not to implement a CCTV system. Local authorities are encouraged to assess whether a system is necessary and proportionate in the circumstances, and if so, what the parameters of its operation should be.[88] The Code requires that systems be reviewed regularly so as to establish the continued justification of the system, preferably when notification is renewed annually.[89]

In February 2009, the House of Lords Select Committee on the Constitution released a report,[90] which highlighted that the rising pervasiveness of surveillance in the United Kingdom creates the risk of undermining the traditional relationship between citizens and the state,

85 *Peck v United Kingdom* (2003) 36 EHRR 41, [2003] ECHR 44647/98 [35]–[36], [46]; Bickel, Brinkley, and White, supra note 56, 359; Goold, supra note 13, 96–97.

86 See Town and Country Planning (General Permitted Development) Order 1995 (UK), sch 2, part 33; Gras, supra note 46, 216.

87 Thomas, "CCTV Code of Practice: Revised Edition 2008" (2008) Information Commissioner's Office <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf> (at 14 July 2009).

88 Ibid 6.

89 Ibid 8.

90 House of Lords Select Committee on the Constitution, supra note 2.

and the right to privacy. The House of Lords concluded that regulation of state CCTV surveillance in the United Kingdom is necessary.[91] This development, while significant, has come at a late stage. During the United Kingdom's CCTV honeymoon period (when the overwhelming majority of CCTV surveillance systems were introduced), there was no regulation governing the circumstances in which CCTV systems could be installed.

2 *Canada*

Contrary to the United Kingdom, the development of CCTV surveillance in Canada has taken place within a regulatory framework of both federal and provincial privacy legislation.[92] As a result, an extensive array of resources is available in Canada, which provides guidance on developing a CCTV system that is lawful, justifiable, and has regard for privacy interests.

Approximately 150 federal government agencies are subject to the Privacy Act RSC 1985, which imposes safeguards on the collection, use, and disclosure of personal information. The Office of the Privacy Commissioner has also issued guidelines on the use of CCTV systems in public places.[93] This regime is replicated in every territory and province, all of which have implemented similar privacy protection laws and guidelines.[94] The various Canadian guidelines require the development of a comprehensive written policy governing the use of state CCTV surveillance systems. Moreover, the guidelines provide detailed advice concerning issues relevant to the Police Policy. To illustrate, Alberta and British Columbia specifically prescribe the means by which visual surveillance records should be destroyed.[95] Like New Zealand, the prescriptive nature of the guidelines may be attributed to the emphasis on the management of personal information protected through the respective privacy protection laws.

Significantly, Canada has not restricted itself to the protection and management of personal information. Instead, it has placed a greater

---

91 Ibid 52.

92 Walby, "Little England? The Rise of Open-Street Closed Circuit Television Surveillance in Canada" (2006) 4 Surveillance & Society 29, 30.

93 Office of the Privacy Commissioner of Canada, *Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (Government of Canada, 2006) <http://www.privcom.gc.ca/information/guide/vs_060301_e.asp> (at 14 July 2009).

94 In Alberta, for example, state CCTV surveillance must comply with the Freedom of Information and Protection of Privacy Act 2000 (AB), supplemented by the *Guide to Using Surveillance*: Ministry of Service Alberta, supra note 16, 2. Similarly, in British Columbia, CCTV surveillance must comply with the Freedom of Information and Protection of Privacy Act 1996 (BC) and guidelines: Ministry of Labour and Citizens' Services, supra note 82. Finally, the Government of Ontario's guidelines build on both the guidelines offered by Alberta and British Columbia: Cavoukian, *Guidelines for Using Video Surveillance Cameras in Public Places* (Information and Privacy Commissioner of Ontario, 2001) <http://www.ipc.on.ca/images/Resources/video-e.pdf> (at 14 July 2009) 1.

95 Namely, by burning, shredding, or magnetically erasing the record: Ministry of Service Alberta, supra note 16, 5; Ministry of Labour and Citizens' Services, supra note 82, para 9.

emphasis on the interference of state CCTV surveillance with the privacy of individuals, and its implications for society as a whole:[96]

> Video surveillance of public places nonetheless presents a challenge to privacy, to freedom of movement and freedom of association, all rights we take for granted in Canada. This is especially true when the surveillance is conducted by police or other law enforcement authorities.

In recognition of this concern, Canada has imposed a mandatory obligation on state agents to undertake a privacy impact assessment ("PIA"), which must be supplied to the Privacy Commissioner prior to implementation. A PIA assesses the impact that the proposed surveillance will have on the privacy rights of individuals, and how such effects could be mitigated.[97] In particular, a PIA provides that state CCTV surveillance must only be employed where conventional methods of law enforcement are substantially less effective, and the benefits of surveillance substantially outweigh the reduction in privacy.[98] The surveillance must be justified through reference to verifiable and specific crime statistics, safety concerns, or other compelling evidence. Yet ultimately, the decision-making power to introduce CCTV surveillance remains with the local authority or police.

The mechanisms of accountability are in many respects similar to New Zealand. Local authorities are required to conduct internal audits, and the respective provincial and territory Information and Privacy Commissioners are also empowered to conduct audits — although the role of the Commissioner is more appropriately described as one of guidance, rather than accountability and enforcement.[99] Despite this, the Canadian framework provides a wealth of information, and clearly represents the most comprehensive regulatory framework of CCTV surveillance. It is an illustration of the current best practices with regard to state CCTV surveillance.

3 United States

Some states and cities in the United States have attempted to regulate the use of CCTV surveillance. Washington DC has imposed an obligation on the police to conduct audits that examine compliance with the

96 Office of the Privacy Commissioner of Canada, supra note 93. Similarly, British Columbia firmly asserts the individual's right to privacy in public spaces: Ministry of Labour and Citizens' Services, supra note 82, para 1. Under Alberta's guide, privacy is conceived as the right to be left alone, which must be balanced against the perceived benefits of CCTV: Ministry of Service Alberta, supra note 16, 1.

97 Ministry of Service Alberta, supra note 16, 2–3. See also House of Lords Select Committee on the Constitution, supra note 2, 70.

98 Ministry of Service Alberta, supra note 16, 2–3; Ministry of Labour and Citizens' Services, supra note 82, para 11; Office of the Privacy Commissioner of Canada, supra note 93.

99 Ministry of Service Alberta, supra note 16, 6; Ministry of Labour and Citizens' Services, supra note 82, para 14; Office of the Privacy Commissioner of Canada, supra note 93, 9.

established policies and procedures.[100] In the absence of comprehensive legislation, however, private organizations have taken to issuing their own guidelines. For example, the New York Civil Liberties Union has developed guidelines (based on the Canadian system), which both the Security Industry Association and the International Association of Chiefs of Police support.[101]

The current legal frameworks governing state CCTV surveillance in New Zealand, the United Kingdom, Canada, and the United States are premised on privacy protection legislation, supplemented through codes of practice. Yet privacy protection legislation fails to provide an effective and meaningful regulatory framework. In particular, it does not address the preliminary decision of whether CCTV surveillance should be introduced at all. In this respect, New Zealand could learn from the Canadian PIA, which effectively requires state CCTV surveillance to be justified as a necessary and proportionate law enforcement measure.

The New Zealand Bill of Rights Act 1990

A final avenue potentially available to govern CCTV surveillance is provided by section 21 of the NZBORA:

> **21 Unreasonable search and seizure**
>
> Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property or correspondence or otherwise.

The purpose of search and seizure law is to regulate the state's powers to intrude into the lives of its citizens.[102] The ability of state CCTV surveillance to intrude on the daily lives of individuals thus makes recourse to section 21 appealing. In particular, application of the NZBORA will provide valuable judicial oversight and guidance as to the lawful and reasonable use of CCTV surveillance. The New Zealand Law Commission has recognized that recourse to the NZBORA may be particularly helpful in circumstances where additional technological enhancements are used by CCTV systems.[103]

However, the courts have yet to determine whether CCTV surveillance may constitute a "search" within the meaning of section 21, a prerequisite to invoking the right.[104] It is clear that the traditional common law concept of

100 Siegel, Perry, and Gram, supra note 35, 13.

101 Ibid. Similarly, the American Bar Association has developed its own standards for the use of CCTV surveillance: Bickel, Brinkley, and White, supra note 56, 322.

102 Optican, "Search and Seizure" in Huscroft and Rishworth (eds), *Rights and Freedoms: The New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993* (1995) 297–298.

103 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, 2009) 223–224 ["*Invasion of Privacy*"].

104 Ibid 9, 223.

a "search" — premised on the strict requirements of a physical trespass — is inept at dealing with public CCTV surveillance.[105] The Court of Appeal has indicated an expansion of the definition of "search" to encompass any state activity that impinges upon a "reasonable expectation of privacy".[106] The reasonable expectation of privacy concept is essentially an analytical tool designed to reconcile privacy and law enforcement interests.[107]

On the continuum of privacy expectations, it is trite to state that an expectation of privacy in a public place is the most attenuated. Privacy must be diminished in public — interference is a necessary incidence of venturing beyond one's door.[108] Although an individual cannot expect absolute freedom from police observation, it is reasonable to expect that he or she will not be subject to constant surveillance throughout the public sphere.[109] The New Zealand Law Commission has recognized that people in public places do not give up all expectations of privacy, particularly if they are caught in a vulnerable situation not of their own making.[110]

A commonly held belief is that the capturing of intimate or sensitive information is likely to be the exception rather than the rule when dealing with CCTV surveillance.[111] This gives rise to the most prevalent justification for CCTV surveillance:[112]

> [A]ll law-abiding citizens should have nothing to hide. Only if people desire to conceal unlawful activity should they be concerned, but ... people engaged in illegal conduct have no legitimate claim to maintaining privacy of such activities.

The 'nothing to hide' argument attempts to balance the extent to which privacy interests are implicated by CCTV surveillance, and the legitimate objectives of law enforcement.[113] Privacy here may be seen as a cloak

---

105 Wilkins, "Defining the 'Reasonable Expectation of Privacy': An Emerging Tripartite Analysis" (1987) 40 Vand L Rev 1077, 1084; Fontana, *The Law of Search and Seizure in Canada* (6 ed, 2005) 567; Optican, supra note 102, 300.

106 *R v Jefferies* [1994] 1 NZLR 290, 302 (CA). The phrase "reasonable expectation of privacy" was first elucidated in the landmark United States Supreme Court decision of *Katz v United States* 389 US 347, 361 (1967), which recognized that search and seizure law protects "people, not places". This was affirmed by the Supreme Court of Canada in *Hunter v Southam* (1988) 45 CCC (3d) 244 (SCC). The New Zealand Court of Appeal, however, has expressed some ambivalence, and has declined to state a definitive view on whether non-trespassory visual surveillance may constitute a search pursuant to s 21 of the NZBORA. New Zealand Law Commission, *Search and Surveillance Powers* (NZLC R55, 2007) 316, 320 ["*Search and Surveillance Powers*"].

107 See Cape, "Search and Surveillance Powers" [2008] NZLJ 75.

108 See New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 209; *R v Jefferies*, supra note 106, 305 per Richardson J; *R v Grayson and Taylor* [1997] 1 NZLR 399, 407 (CA); Wilkins, supra note 105, 1112.

109 For example, a woman writing in a diary under a tree would be offended if a stranger crept up and read over her shoulder. The ability for CCTV to zoom in and surreptitiously record her writing raises a similar concern. Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50 UTLJ 305, 327, 329.

110 New Zealand Law Commission, *Invasion of Privacy*, supra note 103, 8.

111 Austin, supra note 7, 129; Solove, Nothing to Hide, supra note 7, 746–747, 752.

112 Solove, Nothing to Hide, supra note 7, 751; Regan, "Privacy Legislation in the United States: A Debate about Ideas and Interests" (1996) 62 Int'l Rev Admin Sci 465, 472.

113 Solove, Nothing to Hide, supra note 7, 747, 753.

that permits an individual to commit fraud or deception by concealing information from persons who have a legitimate interest in it.[114] Under this approach, privacy interests appear doomed to be defeated.[115]

Yet this argument succeeds only to the extent that it confines the debate to a narrow conception of privacy. First, it fails to acknowledge that state CCTV surveillance does pose a risk that intimate or sensitive information will be captured.[116] Secondly, the argument does not recognize that privacy has a social function necessary for human flourishing and self-development, and is justifiable in itself.[117] In particular, it fails to appreciate the long-term implications of CCTV surveillance on the nature of a free and democratic society. The intrusiveness of CCTV surveillance is not necessarily revealed in any particular situation but may be more accurately described as an environmental harm that builds up over time.[118]

A focus on the actual expectations of privacy held by society is problematic. In the United Kingdom, Canada, and the United States, CCTV was introduced prior to thorough policy discussions, intellectual debate, and in some cases, any public consultation. There is concern that by the time the courts define "reasonable expectation of privacy", the impact of technology in society may have already changed public perceptions of privacy:[119] "if one leaves it too late to find an answer, the nature of the very problem will have changed".[120] Adopting a normative interpretation of reasonable expectation of privacy avoids the uncertainty and difficulties produced by the public's changing attitudes towards privacy.[121]

La Forest J has endorsed the normative analysis of reasonable expectation of privacy. In April 2002, La Forest J issued an opinion that examined the legal and constitutional implications of state CCTV surveillance in Canada, and concluded that it contravened section 8 of the Canadian Charter of Rights and Freedoms 1982.[122] The normative analysis examines whether CCTV surveillance is acceptable in the absence of any limitations whatsoever on the state.[123] In doing so, it examines the "standards of privacy that persons can expect to enjoy in a free and democratic society".[124]

---

114 New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 46; Regan, supra note 112, 471–472.

115 Solove, Nothing to Hide, supra note 7, 747.

116 Ibid 750; McBride, "State Surveillance — The Slippery Slope?" [1997] PLPR 41.

117 Solove, Nothing to Hide, supra note 7, 765; New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 38, 43; Austin, supra note 7, 144.

118 Solove, Nothing to Hide, supra note 7, 769.

119 Solove, "Conceptualising Privacy" (2002) 90 CLR 4, 1087, 1142.

120 La Forest, "Opinion — Video Surveillance" (2002) Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp> (at 14 July 2009). See also Gallagher, supra note 10, 273; Boa, "Privacy Outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning" (2007) 4 Surveillance & Society 329, 332.

121 Blitz, supra note 8, 1364; see also Paton-Simpson, supra note 109, 339–340.

122 See La Forest, supra note 120.

123 Blitz, supra note 8, 1422–1423.

124 *R v Wong* (1990) 3 SCR 36, [45]–[46] (SCC) per La Forest J; *R v Duarte*, supra note 3, [11]; Fontana, supra note 105, 568; Boa, supra note 120, 333.

A defining feature of a free society is the transient nature of the public sphere, which affords members of the public a degree of anonymity and freedom. One can be comforted by the fact that information is revealed only fleetingly — strangers do not know our identity and any information is likely to be forgotten.[125] The ability to repeatedly scrutinize recorded surveillance footage, however, materially alters the interference with privacy, which is no longer merely an incidental observation of an individual's movements. It has been argued that the potential for disclosure, months or even years later, to a far greater audience, including family, friends, or work colleagues, "annihilates the very important right to choose the range of our listeners [and watchers]".[126]

Prevalent and unmitigated state surveillance is repeatedly described in the surveillance literature as "suffocating".[127] The loss of privacy undermines an individual's autonomy and ability to develop intimate relationships, and increases self-consciousness.[128] State CCTV surveillance thus poses a threat to freedom of expression and association, fundamental hall-marks of the democratic society in which we live.[129] The New Zealand Law Commission recently acknowledged that excessive surveillance may deter eccentric or spontaneous behaviour, including legitimate protest and political activism.[130]

Recognition of the long-term implications of state CCTV surveillance highlights the societal interest in protecting and maintaining the privacy of individuals. State CCTV surveillance permits the police to observe systematically any potential offenders as well as every law-abiding member of society. Accordingly, the finding that CCTV surveillance does not constitute a "search" is effectively a decision to authorize or expand state power to pry into its citizens' lives: "[b]y removing entire categories of searches from Fourth Amendment [or section 21] scrutiny, the Court eviscerates what is often the only limitation upon law enforcement power."[131] This is true for state CCTV surveillance. The NZBORA is currently the only legal avenue for challenging the legitimacy of a CCTV surveillance system. Requiring state CCTV surveillance to be reasonable pursuant to section 21 will not shield wrongdoers per se, but will preserve a measure of personal privacy for all society, which is necessary in a free democracy.[132]

---

125 Boa, supra note 120, 333; Paton-Simpson, supra note 109, 326–327; Blitz, supra note 8, 1408; New Zealand Law Commission, *Invasion of Privacy*, supra note 103, 202.

126 Blitz, supra note 8, 1411; see also *United States v White* 401 US 745, 790 (1971).

127 Blitz, supra note 8, 1346, 1377; Solove, Nothing to Hide, supra note 7, 762.

128 Blitz, supra note 8, 1424–1425.

129 Ibid 1422–1423; *R v Wong*, supra note 124, [13]; *Commonwealth v Schaeffer* 536 A 2d 354 (Pa 1987) 364, 366.

130 New Zealand Law Commission, *Invasion of Privacy*, supra note 103, 201.

131 Ku, "The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance" (2002) 86 Minn L Rev 1325, 1328–1329.

132 *United States v White*, supra note 126, 790.

IV THE NEED FOR REGULATION

This Part identifies and discusses further reasons that support the need for regulation and, in particular, examines common assumptions regarding the justifications for implementing state CCTV surveillance. These justifications are premised on the objectives for which the surveillance is implemented. Nonetheless, there is a growing body of evidence that suggests that the justification for state CCTV surveillance is not as strong as it first appears.

Justified Intrusion? Examining the Effectiveness of CCTV

For some criminologists, the advent of CCTV surveillance is indicative of a general trend in law enforcement to move away from the traditional punitive and deterrent framework of crime control to "risk-based policing".[133] CCTV surveillance exemplifies risk-based policing: it focuses on the indiscriminate gathering of information on an entire population, rather than targeting and investigating persons of interest during an investigation into an offence.

Risk-based policing marks a significant change in power between the individual and the state. A fundamental feature of a democratic society is "the individual's sense that she will not have to justify her every action and expression to a government official".[134] For La Forest J, arbitrary surveillance of the entire population fails to strike an appropriate balance between the right to be left alone and the legitimate aims of law enforcement. The implementation of mass CCTV surveillance should not be justified by the claim that citizens have nothing to hide but by the presentation of a compelling state interest.[135] It is therefore necessary to examine and assess the principal arguments for and against the use of state CCTV surveillance.

1 Prevalence of Unsubstantiated Assumptions

The perception that CCTV surveillance is an effective tool in decreasing crime and increasing public safety has been predominant since the first systems were introduced. Goold argues that the politicization of criminal justice saw policy increasingly premised on ideology rather than research.[136] Enthusiastic assertions of the benefits of CCTV surveillance — despite the dearth of evidence to substantiate such claims — quickly became an

133 New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 138; Wakefield, supra note 56, 535; Goold, supra note 13, 4.

134 Blitz, supra note 8, 1411.

135 Gallagher, supra note 10, 291.

136 Goold, supra note 13, 29–30.

established pattern for both the Conservative and Labour Parties in the United Kingdom.[137] CCTV surveillance became an attractive policy that assured the public that action on crime was being taken.[138] This is epitomized by the words of the former Home Secretary, Michael Howard:[139]

> CCTV is a wonderful technological supplement to the police.... CCTV spots crimes, identifies law breakers, and helps convict the guilty ... [it] is a real asset to communities: a great deterrent to crime and a huge reassurance to the public.

Further, the media have played a significant role in promoting the virtues of CCTV surveillance:[140]

> The media frequently echoes this trumpeting, approving style of analysis ... the technology is presented as a highly effective tool of both deterrence and detection, with few questions raised about civil liberties implications (or its effectiveness for that matter).

2 *Effectiveness in New Zealand*

The role of politicians and the media in promoting CCTV surveillance is certainly not unique to the United Kingdom. Promotional materials released by local authorities are often silent on the technical capabilities and other features of the CCTV systems, and focus on the purported benefits that the systems will bring to communities.[141] Further, local authorities and the police release intermittent media reports extolling the virtues of CCTV systems, reinforcing common assumptions that CCTV is effective. One illustration is the use of CCTV in the rapid arrest of an offender responsible for a savage attack in Hamilton's central business district in 2008.[142]

However, there are few statistics available in New Zealand indicating the effectiveness of CCTV systems. It appears that the only local council that has conducted a comprehensive research study, or at least made its findings public, is the Manukau City Council. The Council assessed the effectiveness of its CCTV system in public places against the objectives for which it was implemented. To this end, it analyzed public surveys, the number of incidents recorded, the requests for assistance made by CCTV operators, police requests for footage, and local crime statistics. The two principal claims — that CCTV surveillance is effective in reducing crime and increasing public safety perceptions — are discussed below in reference to several reports on CCTV systems.

---

137 Ibid 20, 27.

138 Armitage, supra note 63, 4.

139 Howard, cited in Goold, supra note 13, 25.

140 Gallagher, supra note 10, 272.

141 Goold, supra note 13, 10; Norris and Armstrong, supra note 80, 88.

142 New Zealand Police Waikato, "Serious Attack Hamilton CBD" (Media Release, 17 April 2008) <http://www.scoop.co.nz/stories/AK0804/S00176.htm> (at 14 July 2009).

(a) Crime Statistics

The Manukau Report was unable to assess the impact of its CCTV system on preventing or reducing crime because the available crime statistics related to a greater geographical area than what the CCTV system covered.[143] The report recognized that despite a decline in anti-social behaviour recorded by CCTV cameras, "there is [a] lack of evidence to attribute these decreases to the installation of the CCTV systems alone".[144] This finding reflects the results in one of the earliest authoritative research studies conducted in the United Kingdom. In December 1995, the Home Office issued a study that examined the effectiveness of CCTV systems in the town centres of King's Lynn, Newcastle, and Birmingham.[145] The study concluded that CCTV systems had the greatest impact when first installed, but to be successful they could not be a lone initiative.[146]

Further studies have also suggested that CCTV surveillance is subject to a "life cycle" that reduces any initial impact of CCTV surveillance over time.[147] This phenomenon was identified by the Nacro Report,[148] which systematically reviewed 24 studies that satisfied the minimum research standards recognized by the Home Office. While six systems employed in city centres were found to have had a positive effect, two had a negative effect, and another six had a null or uncertain effect. Further, the impact of CCTV varied depending upon the nature of the offence. The results indicated that CCTV had no impact on violent crimes against the person, such as assault, but did reduce vehicle crime.[149]

More recently, the Home Office released a report, *Assessing the Impact of CCTV*,[150] which confirmed the Nacro Report and the previous Home Office study (and was significantly greater in scope and allocated research time). The report examined the effectiveness of 13 CCTV systems covering town centres, car-parks, residential areas, and hospitals. It assessed crime statistics, the CCTV system's management and operation, public opinion surveys, and other initiatives operating in the areas covered. Its conclusion was blunt:[151]

> All systems aimed to reduce crime, yet this study suggests that CCTV has generally failed to achieve this. Although police-recorded crime has decreased in six out of the 13 systems for which

143 Manukau City Council, supra note 43, Appendix 3, 14.

144 Ibid 10.

145 Brown, *CCTV in Town Centres: Three Case Studies* (Home Office Police Research Group, Crime Detection and Prevention Series Paper 68, 1995).

146 Ibid; Manukau City Council, supra note 43, Appendix 2, 5; Goold, supra note 13, 42; Norris and Armstrong, supra note 80, 65.

147 Armitage, supra note 63, 4.

148 Ibid.

149 Ibid 3, 5; Gill and Spriggs, supra note 18, 3–4.

150 Gill and Spriggs, supra note 18, 3–4.

151 Ibid 58.

> data were available, in only three cases might this decrease be attributable to CCTV, and in only two areas was there a significant decrease compared with the control.

The report recognized that some CCTV systems appeared to deter property offences (such as car theft), but did not influence impulsive alcohol-related offences, which, following national trends, continue to rise.[152] Again, this supported the 1995 study, which concluded that, contrary to popular belief, CCTV has the greatest effect on property-related offences, but it does not deter personal crimes.

The most successful systems covered a variety of locales, from car-parks to hospitals, and were in areas that had few entrance and exit points.[153] For example, car theft decreased by up to 75 per cent in car-parks with a closed environment and with a limited number of entrances and exits.[154] In contrast, results for CCTV systems situated in town centres and residential areas were much more varied, with crime increasing in some areas and decreasing in others.[155]

Displacement has been a significant concern for state CCTV surveillance since its inception. The Home Office report highlighted that while displacement did occur, it was not common.[156] Only one system exhibited evidence that overall crime had shifted to a neighbouring area. Two systems demonstrated displacement only in relation to one category of offences each, namely, burglary and car theft respectively.[157]

Significantly, the report emphasized that the apparent failure of the CCTV systems to achieve their objectives cannot be remedied by simply increasing the number of cameras. The evidence demonstrated that high-density surveillance did not necessarily produce a corresponding reduction in crime.[158] The report suggested that the apparent "blasé attitude" exhibited by offenders towards CCTV surveillance might subside as CCTV captures more offenders.[159]

The United States experience echoes the conclusions drawn by the United Kingdom reports. While the NYPD claimed that CCTV deterred crime by 36 per cent in its housing projects, the crime statistics had already been falling throughout the 1990s. As a result, experts do not accept that this outcome can be attributed solely to CCTV surveillance, but to a variety of established initiatives.[160] In Times Square, the CCTV system was eventually

152 Ibid vii.
153 Ibid vi–vii.
154 Ibid 59.
155 Ibid vi.
156 Ibid.
157 Ibid vii, 6, 59.
158 Ibid xi.
159 Ibid 5.
160 Siegel, Perry, and Gram, supra note 35, 5.

removed when it was discovered that the system had contributed to only 10 arrests in 22 months.[161]

(b) Perceptions of Safety

The second area assessed by the Manukau City Council concerned the impact of CCTV on public perceptions of safety. It should be acknowledged that measuring public opinion is particularly complex and difficult. The Council found that the introduction of CCTV surveillance, along with its other initiatives, had no impact on the public perception of feeling unsafe, which continues to rise. The majority of respondents did not feel any safer despite knowing that a CCTV system had been installed.[162] Similar results were found in the Home Office report, which indicated that CCTV systems had virtually no impact in alleviating fears for safety. Ironically, individuals who were aware of the CCTV systems were actually more worried than those who remained ignorant.[163]

(c) Police are also under Surveillance

Little attention has been afforded to the impact of CCTV surveillance on police practice and behaviour. A United Kingdom research study found that two thirds of police officers interviewed admitted that CCTV surveillance forced them to be "more careful".[164] The research revealed that police officers were particularly fearful of an increase in complaints, and that their actions would be interpreted out of context.[165] The study raised concerns that CCTV may even undermine police practice because it engenders police reluctance to intervene in violent situations.[166] These findings are important — to be effective, CCTV must not be something feared or avoided by police.[167]

It is clear from the available evidence that CCTV surveillance is not the 'silver bullet' that will solve crime or make people feel safer as expected.[168] The general failure of state CCTV surveillance to achieve its objectives seriously undermines the argument that it is justified as a proportionate response to a particular set of circumstances. Officials in the United Kingdom have finally acknowledged this issue. In June 2008, the House of Commons Home Affairs Committee called for the suspension of all Home Office funding of CCTV surveillance, and the undertaking of new

161 Petersen, supra note 1, 543.

162 Manukau City Council, supra note 43, 4.

163 Gill and Spriggs, supra note 18, 60.

164 Goold, supra note 13, 3, 193–194.

165 Ibid 195–196.

166 Ibid 197.

167 Ibid 201.

168 Manukau City Council, supra note 43, Appendix 3, 4; Siegel, Perry, and Gram, supra note 35, 6; Norris and Armstrong, supra note 80, 65.

initiatives, pending further research into the effectiveness of CCTV.[169] In February 2009, the House of Lords Select Committee on the Constitution recommended that an independent appraisal of CCTV surveillance is necessary.[170]

Adequate Safeguards

CCTV surveillance requires comprehensive legislative control as its very existence and operation exposes individuals to potential harm. It is interesting that the surveillance industry is itself publicly pushing for the regulation of CCTV surveillance to ensure adequate safeguards are in place to protect privacy interests.[171]

Recent research examining the monitoring of CCTV systems with zoom and pan capabilities suggests that visual surveillance may only be as objective as the person operating the camera.[172] In a research study of 148 cameras in 3 major areas in the United Kingdom, criminologists Norris and Armstrong exposed apparent racial bias and discrimination, reminiscent to issues of racial profiling by traffic officers. The homeless, youth, and people of colour were systematically and disproportionately targeted "for no apparent reason":[173]

> The gaze of the cameras does not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant ... [and] singled out by operators as unrespectable.... [R]ather than contributing to social justice through the reduction of victimisation, CCTV may become a tool of injustice through the amplification of differential and discriminatory policing.

The Nacro Review also identified clear discrimination towards males, particularly black males.[174] Norris and Armstrong go even further, questioning the integrity and independence of CCTV operators. In particular, they claim that CCTV operators have, in the past, intentionally avoided filming, or have suppressed footage of, situations that might prove embarrassing to the police.[175]

In the United States, the American Civil Liberties Union has been particularly vocal in highlighting the vulnerability of women under the

169 House of Commons Home Affairs Committee, supra note 6, 69.

170 House of Lords Select Committee on the Constitution, supra note 2, 22. This proposition was supported in Information Commissioner, *Information Commissioner's Response to the House of Lords Select Committee on the Constitution Inquiry into 'Surveillance: Citizens and the State'* (Information Commissioner's Office, 2009) <http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_response_to_hol_constitution_committee.pdf> (at 14 July 2009) 2.

171 Baltman, "Rethinking Surveillance", *The Washington Post*, Washington DC, United States, 11 February 2008.

172 Petersen, supra note 1, 473.

173 Ibid 539; Norris and Armstrong, supra note 80, 201. Similar concerns were expressed in Siegel, Perry, and Gram, supra note 35, 10; Norris and Armstrong, supra note 80, 196–197.

174 Armitage, supra note 63, 4.

175 Goold, supra note 13, 187.

gaze of CCTV cameras. The use of cameras to zoom up skirts and down blouses is an issue on United States campuses.[176] Although no studies have been released, instances have been exposed where CCTV cameras were exploited for similar unethical and voyeuristic purposes.[177] While abuse may not be prevalent, and the evidence is largely anecdotal, the above discussion demonstrates the dangers in proceeding with CCTV surveillance unregulated.

Both inadvertent and intentional disclosure of CCTV images revealing intimate or sensitive events can cause distress, embarrassment, and harm to the individuals involved. In 2004, CCTV footage of the suicide of 22-year-old Paris Lane in the lobby of a building in the Bronx was published on the Internet. Until this incident, the public had been largely unaware that the NYPD monitored 3,100 cameras throughout local African-American communities.[178] Despite public concern that procedures controlling the videotapes were inadequate, the NYPD has remained reluctant to disclose its operating guidelines publicly.[179]

Peck v United Kingdom exemplifies the need for adequate safeguards to protect individuals from the harmful consequences that disclosure of CCTV footage may bring.[180] Peck, who suffered from severe depression, attempted suicide one night in August 1995. A CCTV camera operator observed Peck walking down the street carrying a kitchen knife, and notified the police. The police quickly ascertained that Peck was of no danger except to himself. During a promotional campaign for the CCTV system, however, the local council released a 'success story' entitled "Defused — The Partnership between CCTV and the Police Prevents a Potentially Dangerous Situation", which was accompanied by two photographs of Peck.[181] The press release received extensive media attention, with media reports on local television and the BBC reaching audiences of 350,000 and 9.2 million viewers respectively. In the media publicity, Peck was easily recognizable to those who knew him. As a result of the disclosure, Peck was subjected to jokes, taunts, and abuse, which caused him distress and humiliation.[182]

In *Peck*, the European Court of Human Rights identified a distinction between being observed incidentally and being scrutinized: "[t]he relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation ... and to a degree surpassing that

176 Siegel, Perry, and Gram, supra note 35, 11–12.

177 For example, in 2004 the NYPD undertook blanket visual surveillance of the Republican National Convention. Shortly afterwards, the *Times Newspaper* found that one camera had wandered from the Convention to film a couple in an intimate embrace on their rooftop terrace: ibid 9.

178 Ibid 11.

179 Ibid 4, 5.

180 *Peck v United Kingdom*, supra note 85, [10]. For an overview of the case and its subsequent impact in the United Kingdom, see Gallagher, supra note 10, 274; Emmerson, Ashworth, and MacDonald, *Human Rights and Criminal Justice* (2007) 302.

181 *Peck v United Kingdom*, supra note 85, [13].

182 Gallagher, supra note 10, 275–276.

which the applicant could possibly have foreseen".[183] Consequently, the European Court of Human Rights, in a landmark decision, held that the disclosure of the CCTV surveillance footage to the media constituted an unjustified interference with the right to privacy under Article 8 of the European Convention on Human Rights.[184]

For many commentators, the horse has long since bolted and state CCTV surveillance is here to stay.[185] CCTV technology is expected to continue to increase in scale, variety, capability, and ultimately, in intrusiveness:[186]

> The police are often abetted in obtaining unnecessary, ineffective, and dangerous powers by the reflexive belief among many citizens that restrictions on liberty do not affect them, or more dangerously, that such restrictions are insubstantial and worth the sacrifice.

As a more sophisticated blanket of surveillance is extended over society, it becomes increasingly difficult to maintain a laissez-faire attitude to its regulation.

V PROPOSALS

The current legal framework is woefully inadequate in regulating state CCTV surveillance; recourse to the NZBORA is fraught with uncertainty. This Part brings together the discussion so far and outlines some proposals to path the way forward.

The Responsibility of Parliament

The current regulatory framework, dependent on the Privacy Act 1993, is narrow in its conception of the harms attributable to state CCTV surveillance. The measure of protection is limited to the interference of state CCTV surveillance, with the focus primarily on the management of surveillance footage. Even when supplemented by the Police Policy, this framework reflects a soft form of regulation that fails to provide adequate oversight and accountability for the decision to implement, continue, or expand a state CCTV system.

The NZBORA does not provide a satisfactory legal framework within which state CCTV surveillance can be governed. The ability to provide

183 *Peck v United Kingdom*, supra note 85, [62]–[63].

184 Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221, art 8 (entered into force 3 September 1953) ["European Convention on Human Rights"].

185 Petersen, supra note 1, 510; Farmer and Mann, Surveillance Nation: Part One, supra note 24, 43; Norris and Armstrong, supra note 80, 205.

186 La Forest, supra note 120, [5].

guidance on the reasonable use of state CCTV surveillance is dependent upon cases being brought. In the meantime, citizens are left uncertain about the extent of their rights against interference from the state.[187] The situation is no easier on local councils and the police. Ex post facto judicial guidance poses a risk that the courts will find particular surveillance to be an "unreasonable search" after substantial investment in the technology has already been made.[188] In this respect, the House of Lords acknowledged that "the right to privacy alone cannot provide an adequate basis for the protection of individuals against over-zealous surveillance".[189]

The responsibility to provide an effective regulatory framework for state CCTV belongs with parliament. In developing a legislative framework to govern state CCTV surveillance, parliament has the greatest access to resources and is politically accountable for its decisions.[190] La Forest J, in examining state CCTV surveillance, recognized the crucial role of parliament:[191]

> [G]eneral video surveillance is not solely or even primarily a legal question, at least not in the sense that it is to be resolved exclusively by the courts.... [I]t raises broad socio-political issues, the resolution of which will help to define the proper relationship between the individual and the State in coming decades.

There is a potential for prevalent CCTV surveillance to breed a climate of fear and suspicion, reflecting a breakdown of trust between the state and its citizens. As mentioned above, the House of Lords Select Committee on the Constitution has recommended that CCTV surveillance be regulated in the United Kingdom.[192] The House of Commons Home Affairs Committee recently affirmed the need for balance:[193]

> Privacy plays an important role in the social contract between citizen and State: to enjoy a private life is to act on the assumption that the State trusts the citizen to behave in a law-abiding and responsible way. Engaging in more surveillance undermines this assumption and erodes trust between citizen and State.

In demanding greater transparency and accountability, a comprehensive legislative framework will assure the public that CCTV surveillance is

187 New Zealand Law Commission, *Search and Surveillance Powers*, supra note 106, 321.

188 Ibid.

189 House of Lords Select Committee on the Constitution, supra note 2, 33.

190 Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 J Crim L & Criminology 477, 501.

191 La Forest, supra note 120, [2].

192 House of Lords Select Committee on the Constitution, supra note 2, 52.

193 House of Commons Home Affairs Committee, supra note 6, 9, 38. The importance of trust between citizens and the state is considered in depth by the House of Lords Select Committee on the Constitution, supra note 2, 27–28.

developing within legally defined parameters and safeguards, thereby promoting a relationship of trust.[194] Most significantly, the preliminary decision to implement a state CCTV system will be addressed. A comprehensive legislative regime will help inform the reasonableness standard under section 21 of the NZBORA and will ensure a more complete protection of reasonable expectation of privacy.[195] The courts will retain their role in assessing the reasonableness of CCTV systems and enforcing the legislative framework.

Proposals

1 Authorization

The most significant proposal that this article advances is that the ultimate decision-making power to implement a new CCTV system, or to allow the continuation or expansion of an existing system, must rest with a specialized independent body. Central to attaining authorization for the implementation, continuation, or expansion of a CCTV system, is the need to demonstrate that the surveillance is justified in the circumstances. Where it is determined that the surveillance is not justified, authorization should be declined, and in the case of an existing system, an order for its dismantling made.

In Canada, the use of CCTV surveillance is considered an exceptional step that is justified only where alternative law enforcement measures are not feasible or are significantly less effective, and the benefits of surveillance substantially outweigh the negative interference with privacy.[196] This approach recognizes that the predominant belief that CCTV surveillance provides a simple, effective 'silver bullet' to law enforcement issues is largely unfounded. La Forest J highlights that while the police naturally seek out tools that they believe will be helpful, they neglect to consider the risks:[197]

> [Police] often under-estimate the dangers these tools may pose to other basic societal values. That is why executive control must be carefully exercised, and why we should look with suspicion at demands for additional intrusions on individual liberty.

The Manukau City Council has accepted that the assumption that CCTV surveillance offers the best solution to crime is difficult to sustain when assessing the effectiveness of CCTV systems and alternative options.[198]

---

194 Siegel, Perry, and Gram, supra note 35, 12.

195 New Zealand Law Commission, *Search and Surveillance Powers*, supra note 106, 43.

196 Ministry of Service Alberta, supra note 16, 2–3; Ministry of Labour and Citizens' Services, supra note 82, para 11; Office of the Privacy Commissioner of Canada, supra note 93; Cavoukian, supra note 94, 10.

197 La Forest, supra note 120, [3].

198 Manukau City Council, supra note 43, 9.

Similarly, the United Kingdom House of Commons Home Affairs Committee recently concluded its surveillance report:[199]

> The Home Office should ensure that any extension to the use of camera surveillance is justified by evidence of its effectiveness for its intended purpose, and that its function and operation is understood by the public.

New Zealand should adopt a cautious approach when assessing the justification for CCTV surveillance. In particular, CCTV surveillance should only be authorized where it is both necessary and proportional to the issue it seeks to address.[200] To assist in assessing the justification of a system, it is recommended that the Canadian requirement to undertake a PIA be adopted. A PIA must:[201]

a) Justify the implementation of surveillance, with regard to crime statistics, public safety concerns, and other compelling reasons;
b) Carefully assess the actual or potential implications for privacy; and
c) Propose ways to achieve the objectives without interfering with privacy any more than is absolutely necessary.

Part of the PIA analysis is already provided for in the Police Policy, which provides that cameras must only be installed in areas with a higher incidence of crime, justified by reference to statistics concerning specific categories of offences. A PIA will enhance the effectiveness of CCTV systems by guiding their development further. The CCTV studies demonstrate that the development of a realistic CCTV strategy is crucial to the assessment and success of a system.[202] Both of the United Kingdom reports[203] were critical of the failure to prescribe clear objectives and to take account of local factors such as established crime prevention measures:[204]

> Many projects did not have clear objectives. Partly this reflected an uncritical view that CCTV was 'a good thing' and that specific objectives were unnecessary. It also typified a lack of understanding

199 House of Commons Home Affairs Committee, supra note 6, 69. In February 2009, the House of Lords recommended that the Data Protection Act 1998 (UK) be amended to make it mandatory for a PIA to be produced for every new CCTV system, and for the Information Commissioner to have a role in scrutinizing and approving these PIAs: House of Lords Select Committee on the Constitution, supra note 2, 76.

200 A similar standard exists in Germany, where the constitutional principles of *Verhältnismäßigkeit* (proportionality) and *Erforderlichkeit* (necessity) require that the state justify the implementation and continuation of CCTV surveillance. Gras, supra note 46, 222.

201 Ministry of Service Alberta, supra note 16, 2–3; Office of the Privacy Commissioner of Canada, supra note 93; Ministry of Labour and Citizens' Services, supra note 82, para 11.

202 Manukau City Council, supra note 43, 16.

203 Brown, supra note 145; Gill and Spriggs, supra note 18.

204 Gill and Spriggs, supra note 18, x.

of what effects CCTV could achieve and the types of problems it was best suited to alleviate.

Consequently, the justification for a proposal in a PIA must have regard to the results of the research studies. In particular, it should be taken into account that:[205]

a) CCTV is most effective in preventing and reducing property-related offences;
b) CCTV works best in areas with limited access points;
c) CCTV has no proven impact on reducing personal or violent crimes;
d) CCTV can increase public safety where it is monitored live (although this is dependent upon response times); and
e) The impact of CCTV is greatest when first installed.

Failure to have regard to these factors is likely to undermine the effectiveness of a system, rendering it a disproportional interference with privacy interests. To assist local authorities and the police in the preparation of their PIA (which is to be assessed by the independent specialized body), a template PIA should be developed. This template can be modelled on the Canadian examples.[206]

2 Accountability

CCTV systems should be subject to regular independent audits by a specialized independent agency.[207] Audits will ensure compliance with legal requirements and provide an opportunity to investigate and evaluate the effectiveness of a CCTV system. This may help indicate areas where there is room for improvement. The results may also suggest where CCTV surveillance is no longer necessary or is proving to be ineffective, such that its continued justification should be re-evaluated.[208] The Manukau report recognized the need to reassess whether the hours of live monitoring should be reduced during times of low incidences of anti-social behaviour.[209] In doing so, the Manukau City Council exhibited an understanding that CCTV systems should be subject to continued justification.

205 Manukau City Council, supra note 43, 12.

206 For a copy of the PIA template, see Office of the Information and Privacy Commissioner for British Columbia, *Privacy Impact Assessment Template* (Government of British Columbia, 2006) <http://www.oipcbc.org/sector_public/resources/pia.htm> (at 14 July 2009).

207 Office of the Privacy Commissioner of Canada, supra note 93.

208 Office of the Information and Privacy Commissioner for British Columbia, *Guidelines*, supra note 14, 7–8; New Zealand Police Commissioner, supra note 5.

209 Manukau City Council, supra note 43, 10.

3 Public Disclosure

The dearth of information available to the public regarding CCTV systems does little to dispel the concerns prevalent in the surveillance literature. At present, the little information available regarding CCTV systems usually comes from promotional material released by local councils or the police. Greater transparency will serve not only to foster trust between citizens and the state, but will also educate the public as to their rights and promote meaningful debate on the issues surrounding surveillance.[210] The United Kingdom Information Commissioner recently highlighted that the crucial role of the public in regulating surveillance "is about educating and encouraging people to use their own rights as much as about what we can do as the regulator".[211] It is thus proposed that a national register of all CCTV systems be developed. Ideally, as part of this process, information concerning the systems, such as the PIA, should be made available to the public.

4 Search Warrants

The Government intends to adopt the New Zealand Law Commission's recommendation to enact a generic surveillance warrant regime to govern all forms of surveillance (including audio, tracking, and visual surveillance) for law enforcement purposes.[212] Unfortunately, the new legislative framework will not extend to CCTV surveillance.[213] Prior judicial authorization alleviates concerns that CCTV surveillance will evolve to become excessive, arbitrary, and targeted. In order to assure the public against such fears, the new search warrant regime should be extended to cover the use of CCTV surveillance in the two circumstances outlined below.

First, a search warrant should be required where CCTV surveillance is paired with another form of surveillance, or has advanced capability. Described as 'mission creep', the concern in the surveillance literature is that a system introduced for one purpose will invariably be used for an alternative purpose, thereby heightening the intrusion into an individual's privacy. This would cover the situation where, for example, facial recognition software is added to enhance the system's capabilities.[214] A further example is the compiling of information into individual profiles:[215]

---

210 Ibid 1–2; Ministry of Service Alberta, supra note 16, 2–3; Siegel, Perry, and Gram, supra note 35, 14; Office of the Privacy Commissioner of Canada, supra note 93; Ball et al, supra note 77, 90.

211 The House of Lords has similarly recommended that the United Kingdom Government take a more proactive role in educating the public as to surveillance practices, and their implications for society. House of Lords Select Committee on the Constitution, supra note 2, 98; see also House of Commons Home Affairs Committee, supra note 6, 43–44.

212 Search and Surveillance Bill 2009 (No 45-1). The Bill is intended to reform New Zealand's surveillance laws, which have "failed to keep pace with technology": ibid Explanatory note, 2. See also New Zealand Law Commission, *Search and Surveillance Powers*, supra note 106.

213 New Zealand Law Commission, *Search and Surveillance Powers*, supra note 106, 26, 239.

214 Austin, supra note 7, 123; Solove, Nothing to Hide, supra note 7, 767; Petersen, supra note 1, 542.

215 Austin, supra note 7, 131.

> While isolated bits of information (generated, for example, by merely walking around in public spaces and not taking active steps to avoid notice) are not especially revealing, assemblages are capable of exposing people quite profoundly, which leads to the possibility of targeting individuals and even manipulating them.

Arbitrary and drag-net surveillance, recording the movements of individuals simply on the hunch that it may one day prove useful in the investigation of an offence, severely undermines the privacy interests discussed.[216] It raises the distinction between being incidentally observed by a security camera, and being subject to continuous state scrutiny.

Secondly, a search warrant should be obtained where the police, in the course of investigating an offence, wish to use CCTV surveillance to follow or track a person of interest through the public sphere. The Police Policy currently prohibits the use of CCTV surveillance to track an individual, except in circumstances where there is a reasonable suspicion that an offence is taking place. The use of state CCTV surveillance to track and monitor the activities of persons of interest is outside the objectives for which the system was implemented.

It is proposed that the search warrant requirement be modelled on the Regulation of Investigatory Powers Act 2000 (UK). The Act prohibits the police from conducting "directed surveillance", which covers covert surveillance where the police follow an individual in public without prior authorization.[217] Thus, before conducting direct surveillance, the police must have a reasonable suspicion that an individual has committed or intends to commit a crime, and be authorized by a superintendent or above.[218]

The obligation to obtain a search warrant allows the police to take full advantage of CCTV surveillance, while ensuring that this occurs within legally defined parameters. The procedure permits the lawful extension of the current purposes for which CCTV surveillance may be used.

5 Training

At present, there is no requirement in New Zealand that persons operating a state CCTV surveillance system attain minimum qualifications. The Police Policy provides that it is the individual camera officer's responsibility to train police and volunteer operators. The lack of national uniformity creates disparity among CCTV systems. Training is an important factor in the success of a system and the technology being used to its full advantage.[219]

---

216 Blitz, supra note 8, 1459.

217 New Zealand Law Commission, *Search and Surveillance Powers*, supra note 106, 323–324. For an overview of the Regulation of Investigatory Powers Act 2000 (UK), see Emmerson, Ashworth, and MacDonald, supra note 180, 295.

218 Emmerson, Ashworth, and MacDonald, supra note 180, 296–297.

219 Gerrard et al, *National CCTV Strategy* (United Kingdom Home Office, 2007) <http://www.crimereduction.homeoffice.gov.uk/cctv/National%20CCTV%20Strategy%20Oct%202007.pdf> (at 14 July 2009) 21; Siegel, Perry, and Gram, supra note 35, 15; Gill and Spriggs, supra note 18, xii.

International examples of abuse underscore the need to ensure that operators and those who have access to a CCTV system do not abuse their position of trust within the community. Hence, it is essential that operators are trained, professional, and respectful of privacy interests.[220]

It is recommended that minimum training standards be developed, the attainment of which should be mandatory for all CCTV operators. The qualification regime could be modelled on the United Kingdom Security Industry Authority licensing regime.[221] This regime makes it illegal for an operator to work with a public CCTV system without a Security Industry Authority licence. The training should encompass both ethical considerations and technical skills.[222] The United Kingdom licensing regime suffers from clear gaps — in particular, the licence requirement applies only to contracted CCTV operators.[223] In order to attain a uniform and minimum standard across all CCTV systems, the licence requirement should apply to all participants, whether they are police, contractors, employees, or volunteers.[224]

6 Penalties

In the past, regulatory bodies have been criticized as ineffective because they are notoriously under-resourced and reliant upon the co-operation of the agencies that they regulate.[225] It is essential that the specialist agency has the power and resources to enforce the regulations and to impose meaningful penalties, including fines, imprisonment, and public apologies.[226]

In the United Kingdom, an individual working without the necessary licence is exposed to a maximum penalty of £5,000, or 6 months imprisonment, or both.[227] It is also appropriate that civil or criminal penalties attach to the deliberate abuse of CCTV surveillance. The penalties would be designed to address egregious breaches of privacy, such as intentionally filming intimate activities within private premises. Like the licensing regime, meaningful deterrence of unacceptable behaviour

220 The House of Lords Select Committee has recommended more resources be devoted to training to ensure high standards and respect for privacy: House of Lords Select Committee on the Constitution, supra note 2, 76. See also Armitage, supra note 63, 4–5; Petersen, supra note 1, 539.

221 Gerrard et al, supra note 219, 21–22.

222 For example, training should cover the responsibilities and obligations under the legislative provisions, privacy concerns, how to deal with incidents, how to operate CCTV equipment, and surveillance techniques. For a description of the training requirements in the United Kingdom, see Security Industry Authority, "Public Space Surveillance (CCTV): Required Qualifications" <http://www.the-sia.org.uk/home/licensing/cctv/training/training_cc.htm> (at 14 July 2009).

223 Gerrard et al, supra note 219, 22.

224 Ibid.

225 Gras, supra note 46, 218.

226 Ball et al, supra note 77, 86; Lyon, supra note 81, 173.

227 Security Industry Authority, "SIA Enforcement Policy: Code of Practice" (2008) <http://www.the-sia.org.uk/NR/rdonlyres/92C8C9DF-6C2E-41EF-B511-891ECDD85A6C/0/sia_enforcement_cop.pdf> (at 14 July 2009) 4.

requires a system of fines and imprisonment. Different penalties will be appropriate in different circumstances depending upon the harm caused by the breach. For example, the issuing of a public apology in *Peck*[228] was criticized as an inappropriate remedy in respect of a breach of privacy.[229] Unlike defamation, further publicity cannot remedy a breach of privacy but may actually serve to compound its effects. Rather, compensation for hurt and humiliation may be more appropriate in circumstances where a public apology will cause further embarrassment and distress.[230]

The above proposals are designed to address the weaknesses of the current legal framework, and the key issues of concern exhibited in the surveillance literature. In particular, state CCTV surveillance must be justified in the circumstances, and prior approval must be attained from an independent agency before implementation or expansion.

VI CONCLUSION

Well over 26 million CCTV cameras have been introduced internationally,[231] and the proliferation of state CCTV surveillance and the technical capabilities of CCTV cameras will only increase. CCTV surveillance technology is commonly promoted as an effective and valuable law enforcement tool that reduces the incidence of crime and other anti-social behaviour, and improves public perceptions of safety.

This article has identified that the intrusive nature of state CCTV surveillance poses a special threat to an individual's privacy, which has a social function that is necessary to human flourishing, self-development, dignity, and autonomy. Pervasive and excessive state CCTV surveillance increases an individual's self-consciousness, which in turn breeds inhibition. Over time, the loss of privacy in the public sphere may threaten freedom of expression and association — fundamental tenets of a democratic society.

International experience demonstrates the importance of ensuring adequate safeguards to protect individuals from the abuse of state CCTV surveillance. The monitoring or disclosure of sensitive or intimate activities can cause individuals immense distress, humiliation, and embarrassment. Effective regulation is necessary to ensure that state CCTV surveillance does not evolve into a modern mechanism of discrimination by targeting those sections of society perceived as 'undesirable'.

In light of these concerns, the current legal framework governing state CCTV surveillance in New Zealand is demonstrably weak and ineffective.

---

228 *Peck v United Kingdom*, supra note 85.

229 Gallagher, supra note 10, 281.

230 The House of Lords has recommended that compensation be made available where an individual is subject to illegal surveillance; House of Lords Select Committee on the Constitution, supra note 2, 39.

231 Farmer and Mann, Surveillance Nation: Part One, supra note 24.

New Zealand law neither prohibits, nor authorizes, the implementation of state CCTV surveillance. The Privacy Act 1993, supplemented by the Police Policy, is primarily designed to protect the security of personal information, and focuses on the management of CCTV surveillance. This narrow focus fails to appreciate the privacy interests that are inherently prejudiced by the existence of state CCTV surveillance. In particular, the current legal framework fails to address the preliminary and more significant issue concerning the justification for the implementation of state CCTV surveillance in the first place. The New Zealand Law Commission has recognized this:[232]

> It can be difficult for citizens to appreciate the privacy implications of routine surveillance and the collection of information that is not of itself discreditable or embarrassing. The laissez faire attitude, 'if I've got nothing to hide, I've got nothing to worry about', is prevalent, particularly where surveillance is justified for public interest reasons such as security.

Whether a particular state CCTV surveillance system is justified is open to considerable challenge. International research has revealed that the prevalent assumption that state CCTV surveillance reduces the incidence of crime and increases public perceptions of safety is largely unfounded. In particular, the research suggests that, while state CCTV surveillance may reduce the incidence of property-related offences, it has no impact on violent crime or the public's feelings of safety.

The Police Policy provides for a review procedure to assess the effectiveness and continuing necessity of a CCTV system. However, it is questionable whether the police — who have a vested interest in the system — should be responsible for undertaking the reviews. Further, the fact that oversight is confined to the police (as local councils and other state organizations remain outside the ambit of the Police Policy), is concerning. In the absence of effective oversight, the state must be trusted that it will use CCTV surveillance in an enlightened way.[233] In such circumstances, the necessity of recourse to the NZBORA is heightened. Nevertheless, an ex post facto judicial analysis does not by itself provide sufficient oversight and accountability against the spread of an increasingly sophisticated blanket of state surveillance.

Meaningful and effective control of state CCTV surveillance requires the enactment of a comprehensive legislative framework. This article has advanced a series of proposals that the legislative framework should incorporate, drawing upon the wealth of international experience and information. Most significant is the requirement that the implementation, continuation, and expansion of state CCTV surveillance be authorized

232 New Zealand Law Commission, *Privacy: Concepts and Issues*, supra note 2, 138.

233 Norris and Armstrong, supra note 80, 229.

by an independent specialized body. All surveillance should be shown to be justified in the circumstances as a necessary and proportionate law enforcement measure. In this respect, the Canadian PIA provides valuable guidance in assessing the justification of a CCTV system in New Zealand.

New Zealand is in a unique position to shape the way in which state CCTV surveillance develops, before it becomes wide-spread. The time to address the issues surrounding state CCTV surveillance is now. The enactment of a comprehensive legislative framework governing state CCTV surveillance will ensure that New Zealand strikes an appropriate balance between the recognition and protection of privacy interests, and the pursuit of legitimate law enforcement objectives. In doing so, it will influence the relationship between state and citizen in the years to come.