Surveillance & Society
Special Issue on 'Surveillance and Criminal Justice' Part 2, 4(4): 329-345
http://www.surveillance-and-society.org

Privacy Outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning*

Krista Boa[1]

Abstract

Law enforcement uses surveillance to gather evidence about suspects. This is facilitated by advances in technologies. But these advances also create new dilemmas for privacy and its regulation and protection. This paper aims to understand how changing technologies and contexts affect the conceptualisation of privacy through an examination of decisions made in the Supreme Court of Canada. The paper concludes by identifying two sets of distinctions made in the judgements which highlight firstly, the dangers of making analogies with human senses and, secondly, the importance of recognizing differences between the degrees of attention paid by others to our activities.

Introduction

Law enforcement regularly uses surveillance to gather evidence about suspects. Technological advances are making the surveillance practices easier; but sometimes these new tools open individuals to potential invasions of privacy. The question becomes, is the use of newer surveillance technologies and practices qualitatively different from what was done before, or it is a matter of law enforcement have better tools to conduct surveillance as they have always done? The gathering of evidence in many jurisdictions is governed by some form of protection from unreasonable search and seizure by the state (e.g., Article 8 of the European Convention on Human Rights, and the Fourth Amendment in the United States Constitution). In Canada, this protection is found in Section 8 of the *Canadian Charter of Rights and Freedoms* (1982; hereafter the *Charter*).

The Supreme Court of Canada's decision on S.8 of the *Charter* was *Hunter v. Southam Inc*. (1984). In this decision, they clearly articulate what privacy protects in this context. Historically, legal protections of privacy in Canada and other common-law countries have

* This work was supported by two Canadian Social Science and Humanities Research Council (SSHRC) grants – a Canada Graduate Scholarship (Doctoral) and a SSHRC Initiatives for the New Economy Research Project – Digital Identity Creation.
[1] Faculty of Information Studies, University of Toronto. mailto:k.boa@utoronto.ca

 ISSN: 1477-7487

tended to focus on traditional understandings of what is private, such as the home, property, and secret or confidential information (Austin, 2003; *Hunter & Southam Inc.*, 1984; Solove, 2002; Solove, 2001), particularly outside the context of personal information privacy or data protection. The interpretation of privacy protection in *Hunter v. Southam* seems to steer away from the traditional, private-sphere perspectives on privacy. It states that privacy protection under S.8 of the *Charter* protects "people, not places" (para. 23), and is not restricted to notions of property and trespass. Privacy, however, does not cover everything and anything. *Hunter v. Southam* clearly explains that the *Charter* protects "a reasonable expectation of privacy" (para. 24-25), a concept also used in U.S. privacy jurisprudence. A search, therefore, will be deemed unreasonable if it affects what is found to be a reasonable expectation of privacy (*Hunter v. Southam*, 1984). Determining whether a reasonable expectation of privacy exists can be problematic. It is an inherently subjective process, depending on a given judge's understanding of the implications of the facts of a given case, and the relationship of those facts to his or her understanding of the nature and value of privacy. Furthermore, as Elizabeth Paton-Simpson (2000) argues, the concept of a reasonable expectation of privacy fails to adequately address situations where privacy invasions occur in what are typically considered public settings, or with regard to information deemed to be 'public'. Courts often use the fact that information was gathered in public as a means of denying an expectation of privacy (Paton-Simpson, 2000). Austin argues, "paying attention to the distinctive features of information technology can help highlight what is at stake" (2003: 164) and can help to provide a more nuanced analysis of whether a privacy interest exists in particular information, beyond simply determining whether it was gather in public or not.

This paper examines judicial reasoning to determine whether a reasonable expectation of privacy exists in four Supreme Court of Canada[2] judgements, focusing on the conceptualization of surveillance technologies and how the notions of public and private are framed. *R. v. Duarte* (1990), *R. v. Wong* (1990), *R. v. Wise* (1992), and *R. v. Tessling* (2004) all centre on the admissibility of evidence obtained through surveillance because in each case the police failed to obtain warrants to conduct the surveillance. The evidentiary dimensions of these decisions, although interesting, are not addressed here. The goal of this examination is to understand how surveillance technologies and distinctions between public and private affect conceptualizations of a reasonable expectation of privacy, to identify tensions and limitations of particular conceptualizations, and to develop conceptual tools for identifying these issues. As surveillance technologies become commonplace and increasingly sophisticated, there is an increasing need for such tools to help tease apart the implications of these technologies and to help avoid overly simplistic conceptualizations when determining how particular technologies and practices will affect privacy. Two ways of distinguishing the implications of various technologies are developed. The first deals with issues of capture, context, and exposure, and the second with distinctions between degrees of attention paid to individuals, the difference between seeing, watching, and monitoring, for example.

[2] The Supreme Court of Canada is Canada's highest court. Decisions of the Supreme Court cannot be appealed and as such, their decisions create strong precedents for future cases. Before a case comes before the Supreme Court, it is first heard by a trial judge, and then appealed to a provincial court of appeal, then appealed to the Supreme Court.

Privacy Protection in Canada

Before examining the theoretical and conceptual underpinnings of this paper, it is useful to contextualize privacy protection in Canada's legal regime. Canadian law protects privacy in several ways. The main body of privacy-related law focuses on privacy of personal information, referred as data protection in European jurisdictions. Personal information is protected by a number of federal, provincial, and territorial statues. The *Privacy Act* governs the collection, use, and disclosure of personal information by the federal government, the Government of Canada. Each province and territory also has an act that governs how it handles the personal information it holds (e.g., Ontario's *Freedom of Information and Protection of Privacy Act*). The most recent addition to Canada's personal information privacy regime is the *Protection of Personal Information and Electronic Documents Act*, which covers the collection, use, and disclosure of personal information held by private enterprises. Finally, other privacy-related areas are covered by law in the area of trespass, defamation, or nuisance.

The *Charter of Rights and Freedoms* offers the strongest legal protections in Canada because they are rooted in the Constitution. With respect to search and seizure by the state, privacy interests clearly fall under S.8 of the *Charter*. In addition, it is possible that privacy could be understood to fall under the broader protections of S.7 of the *Charter*, which reads "Everyone has the right to life, liberty and security of the person," but to date there has been no decision on this at the Supreme Court (CANLII, 2004a). By comparison, the Supreme Court has ruled on privacy interests in relation to S.8 in a range of contexts outside surveillance, for example, with respect to bodily privacy (*R. v. Dyment*, 1988; *R. v. Arp*, 1998) or with respect to one's electricity records (*R. v. Plant*, 1993).[3] These types of cases hinge on the question of whether the search was legal, that is whether law enforcement was entitled to gather the evidence without judicial oversight in the form of obtaining a warrant. As is clear from *Hunter v. Southam Inc.* (1984), a search is not legal if a reasonable expectation of privacy is found. Thus, the question becomes whether the individual had a reasonable expectation of privacy in the information or the situation.

Theoretical and Conceptual Positions

There are some significant challenges in using the concept of a reasonable expectation of privacy to establish the existence of a privacy interest. Its application is necessarily subjective, as is each of its elements. First, determining what is "reasonable", even when based on a history of reasonable-person jurisprudence both within and outside Canada, can easily be imbued with one's own values, particularly in the context of privacy in public and new technology. Technological capabilities and the resulting information practices are constantly changing. As a result, social norms of what is reasonable have not been, and arguably cannot be, established. Although "the concept of a 'reasonable' expectation of privacy is an amalgam of descriptive and normative notions" (Paton-

[3] For a full discussion of S.8 *Charter* jurisprudence, see CANLII 2004b.

Simpson, 2000:320-321), the makeup of this amalgam changes from person to person. The second problem involves the idea of "expectations", which is also closely tied to social conventions and practices. Yet, simply because a particular practice exists and individuals have come to expect it does not necessarily mean that it is right or that there is no privacy interest. This makes it difficult to identify privacy interests in situations where privacy-invasive practices are becoming commonplace. Finally, the concept of privacy itself poses challenges because it is defined differently in different contexts and by different conceptual frameworks (e.g., Austin, 2003; Cavoukian, 1999; Nissenbaum, 1998; Rossler, 2004; Solove, 2002). When all three function together, the result is a standard that is vague and subjective, making it difficult to identify, let alone adjudicate.
Historically, legal protections of privacy in the English-speaking Western countries have tended to focus on traditional understandings of the private sphere, including the home, personal property, trespass, and the secrecy or confidentiality of sensitive information (Austin, 2003; Nissenbaum, 1998; Solove, 2002; Solove, 2001). Although alternative conceptualizations exist, such as Nissenbaum's contextual integrity (2004; 1998), Alan Westin's (1968) informational self-determination, and data-protection and control-based legal regimes such as Canada's *Personal Information Protection and Electronic Documents Act* or the European Union's Data Directive on data protection, reasoning from traditional perspectives on privacy under the *Charter* persists. For instance, in *R. v. Tessling* (2004), the Supreme Court of Canada relied on the notion of the "biographical core": that one has a privacy interest only in personal information "which tends to reveal intimate details of the lifestyle and personal choices" and is "of a 'personal and confidential' nature" (*R. v. Plant*, 1993: para. 20) to deny Mr. Tessling a privacy interest in the heat patterns emanating from his home captured using forward-looking infrared (FLIR) technology.

Such traditional and arguably narrow constructions of privacy significantly limit the potential to legally protect privacy interests in non-traditional environments, such as "in public." In such reasoning, the public and the private are often positioned as dichotomous. Yet, they are not sharply distinct categories; they are fluid, overlapping, and contextual concepts (Marx, 2001; Marx, 1997; Nissenbaum, 1998; Paton-Simpson, 2000). Excluding an expectation of privacy from all public locations does not take into account this fluidity or individuals' understanding of it in daily life (see Viseu, Clement, & Aspinall 2004). "Simply by venturing into a public area we hardly give up all expectation of privacy" (Allen 1998, as cited in Marx, 2001:163). In ordinary life, "reasonable people assess roughly just how 'public' a situation is and adjust their behaviour accordingly" (Paton-Simpson, 2000:322). Jeffrey Reiman (2004) identifies yet another nuance: "privacy results not from locked doors and closed curtains, but also from the way our publicly observable activities are dispersed over space and time" (196).

Reiman's point brings us to a further challenge posed by surveillance technologies when determining reasonable expectations of privacy: "technology creates privacy issues that appear to fall outside the bounds of our traditional analysis" (Austin, 2003:164). Surveillance technologies can aggregate data, record interactions surreptitiously, and otherwise contravene social and physical norms (Austin, 2003; Marx, 2001; Marx, 1997; Nissenbaum, 1998; Paton-Simpson, 2000, Sheller & Urry, 2003). As Gary T. Marx argues, "many of our most basic social assumptions involve a physical rather than electronic world" (1997:2). He discusses the concepts of public and private in terms of

"personal borders" or boundaries, our intuitive sense of which electronic surveillance technologies undermine and transcend (Marx, 2001; Marx, 1997). From a physical understanding of the world, information about an individual in public would be "sparse and disjointed" and "limited by what any single human brain could reasonably and efficiently hold" (Nissenbaum, 1998:576). By contrast, in an electronic world, physical boundaries are reduced or eliminated, for instance, when physical memory is supplanted by near permanent recordings. Furthermore, sense boundaries demarcate what we are normatively able to perceive: "the assumption is that what you can 'normally' or 'naturally' see, hear, smell, or comprehend when your presence is not hidden, you are entitled to perceive" (Marx, 2001:158). In other words, there is an expectation of reciprocity in the physical world: if you can perceive me, I can perceive you. Finally, surveillance technologies provide the ability to capture information in one context and shift it to another (Nissenbaum, 1998), further disturbing normative and social expectations. This has significant ramifications for determining what properly constitutes a reasonable expectation of privacy.

The Cases

Two distinct and opposing approaches to determining a reasonable expectation of privacy with respect to technologically enabled surveillance are apparent across the first three cases discussed: *R. v. Duarte* (1990), *R. v. Wong* (1990), and *R. v. Wise* (1992). These cases form a series in that each includes opposing views on the nature of privacy, the implications of surveillance technology, and the nature of public and private activities, spaces, or communications, articulated by Justice La Forest on the one hand and Justice Cory on the other.

For Justice La Forest, the question must be framed in terms of what practices are acceptable to apply to any or all members of a free and democratic society. It is only from this perspective that a reasonable expectation of privacy can be determined. Justice La Forest also advocates judicial oversight in such cases, in the form of obtaining a warrant. His position is clearly expressed, for example, in *R. v. Duarte* (1990) when he writes, "this Court is accordingly called upon to decide whether the risk of warrantless surveillance may be imposed on all members of society at the sole discretion of the police" (para. 17). Prior judicial authorization requires police to provide reasons, based on a scale of appropriate levels of suspicion and probable cause, and therefore is a strong measure against police "fishing" for evidence.

The other approach, typified by Justice Cory, focuses only on the facts of the case in question and considers the privacy interest only in terms of the individual involved. It does not take into account a particular social value of privacy more generally, or the implications of the judgement for all members of society. The reasoning in *R. v. Tessling* (2004), the final case discussed here, is much closer to the Cory approach than that of La Forest. In examining this case, we can see that how the way in which the question is framed has direct implications for determining a reasonable expectation of privacy.

While ultimately these cases question the admissibility of evidence obtained through

surveillance, this is not the focus here. This analysis centres on how the surveillance technologies and public and private space are conceptualized in judicial reasoning regarding whether a reasonable expectation of privacy exists. It is important, however, to remember that the surveillance in each of these cases was conducted without judicial oversight. The police did not obtain a warrant. Thus, if a reasonable expectation of privacy is found, the search could be deemed illegal and the evidence obtained thrown out.

The following subsections discuss the cases individually. The analysis of each is based solely on the text of the Supreme Court judgement. All references to provincial Court of Appeal decisions are drawn from the text of the Supreme Court judgement. A Supreme Court judgement can either be a unanimous decision or a majority decision. In judgements where there is not a unanimous decision, those not in agreement will provide a dissent, which is also part of the judgement. Of the cases discussed here, only *R. v. Tessling* (2004) is a unanimous decision. Therefore, in addition to the decision itself, including its refutation of the reasoning of the lower courts, the judgements also contain dissents and additional reasons, which are written by judges who wish to make points not included in the decision itself, all of which is considered in the analysis of these cases.

R. v. Duarte (1990)

In *R. v. Duarte* (hereafter *Duarte*) the police make an audiovisual recording of a narcotics transaction. The transaction occurred in an apartment specifically wired to make recordings, which was occupied by an undercover agent and an informant. The conceptualization of the technology is central to determining a reasonable expectation of privacy in the judgement.

At first glance, this case does not appear to be a case of privacy in public. Presumably, this apartment is presented as the home of at least one of the two people working with the police. Thus, the surveillance occurs not in what is traditionally understood to be public space, but rather in a traditionally private space, a personal residence.[4] Nevertheless, the issues in *Duarte* (1990) are relevant to discussions of privacy in public. In addition to being specifically referenced in *R. v. Wong* (1990) and *R. v. Wise* (1992) with respect to the use of surreptitious surveillance technologies, the risk analysis that forms the basis of Justice Cory's position implies some degree of "publicness" in communications.

The Ontario Court of Appeal judgement, written by Justice Cory, treats the technology as merely an extension of human memory and the use of human informants. His reasoning relies on an analysis of the usual risks inherent to communication: there is always some risk when communicating with others that the receiver of the information will betray

[4] Traditionally, the home is the quintessential space protected by privacy rights (*R. v. Wong* 1990; Solove 2002). The surveillance in this case is not surreptitious third-party surveillance but participant surveillance, which is a form of "electronic surveillance in which one of the parties to a conversation, usually an undercover police officer or a police informer, surreptitiously records it" (*R. v. Duarte* 1990, para. 7). Clearly, the undercover agent and informer have consented, given their role in this operation. Nevertheless, visitors to the apartment could assume that conducting their business, such as drug transactions in this case or any other private business, in a personal residence would afford a greater degree of privacy than other more public spaces. Neither Justice La Forest nor Justice Cory addresses the potential of a greater expectation of privacy because of the location in which the transaction takes place.

one's confidence and report that information to others. In this way, the content of the conversation becomes more public by virtue of having been communicated to another, and the speaker risks further publication of the information should the first listener report it to others. By contrast, the Supreme Court majority decision, written by Justice La Forest, holds that using informants and relying on their memories is entirely different from surreptitiously recording conversations.

Justice Cory reasons that because police regularly use informants and undercover agents and this practice does not require judicial oversight, providing a complete electronic recording of a conversation is a "small step" (para. 11) from relying on an informant's memory to later report the substance of a conversation. He supports this position by drawing on the notion of a "faultless memory" from *Lopez v. United States* (1963), which explicitly claims there is no difference between "faultless memory and mechanical recording" (as cited in *Duarte*, 1990: para. 12). From this perspective, making and using recordings is simply a matter of technological progress, of law enforcement's access to better, more accurate tools to gather evidence they are already entitled to gather. Accordingly, the use of surveillance technologies cannot be said to have any ramifications for the individual in terms of an expectation of privacy.

By contrast, Justice La Forest denies the applicability of this risk analysis, arguing "the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic recording of them […] are of a different order of magnitude" (para. 30). Justice La Forest, however, does not explain this difference more precisely. His reasoning implies the nature of recordings is qualitatively different from individuals' memories of conversations. Exploring how memory and recordings differ requires us to focus specifically on the technology.

The difference between a person's memory of a conversation and a permanent electronic recording of a conversation can be understood by examining them in terms of three interrelated distinctions: capture, exposure, and context. First, as Justice La Forest suggests, there is the element of permanence to recordings. I prefer the term capture because it implies not only fixity, but also the act of gathering, of capturing the information. Generally, people assume that spoken words and verbal conversations are ephemeral (Marx 2001). Indeed, conducting affairs verbally is often used to keep the content of the conversation "off the record." A recording captures a conversation and fixes it permanently, verbatim, until that recording is destroyed or the technology no longer exists to play it. Speakers can, and should, assume that listeners will hear and remember a conversation, either its sense or the words; however, it is not likely that a listener will remember the entire conversation verbatim.

Exposure[5] and context, the remaining two distinctions of the series, are closely related.

[5] Exposure also relates to replicability, which is not part of the cases here but might be relevant if these distinctions are applied more broadly. Electronic recordings can be copied easily. If they are digital, this can be achieved without any loss in quality. If the recording is on magnetic tape, there will be a minor loss in quality with each copy. Generally, however, this would not become apparent to the human ear until many generations of recordings are made.

Once a conversation is captured in a recording, it can be exposed outside its original context. Furthermore, recordings can be played repeatedly for any audience at any time, and thus, the information may be exposed to a different audience than was intended. Normative social interactions are based on a shared understanding of contextual integrity; what is appropriate in one context may not be in another (Nissenbaum, 1998). An electronic recording is captured and preserved outside its original context, which might include the relationship or history between the parties, or other aspects of context that cannot be captured in a recording. Although in *Duarte* (1990) the context of the situation was likely clear, this will not always be the case. The problem of context is also associated with a memory of a conversation. However, one might not be as likely to pose questions about the context of a recording as one would with memory. Memory is often understood to be more subjective and, thus, more open to questioning. By contrast, a recording (and technology in general)[6] is more likely to be understood an objective capture of fact (Lessig, 1999; Marx, 2001). The difference between an electronic recording and memory-based repetition of a conversation is more than a matter of degree, or exactitude; it is also a difference in kind.

The concept of a "faultless memory" does not eliminate these differences between recording a conversation and reporting it from human memory. Certainly, a person can learn to remember events and conversations in great detail, even exactly. However, this is not a usual characteristic of the majority of listeners, and is hardly something a reasonable person would expect. Moreover, memory is qualitatively different from a recording in its ability to replicate what has been recorded. No matter how faultless someone's memory, a person cannot replicate a conversation with the same degree of precision as a recording. While the content of a conversation can be repeated from memory, a recording can expose the conversation as it transpired, including words, intonation, and other nuances of speech, particularly when combined with a visual recording as in *Duarte*, where body language and gestures are also captured. Furthermore, a recording captures a replica of the conversation that can be saved, well beyond the time when memory of it would fade. Making surreptitious recordings, as occurred in this case, contravenes normative understandings of physical and sense boundaries, as Marx describes them (2001; 1997).

Justice La Forest's position on the issues in *Duarte* (1990) pays closer attention to the nuances of the technology than exists in Justice Cory's position. He argues that recording a conversation is deeply and qualitatively different from using informers. Although Justice La Forest does not explain in detail how recordings differ from memories, some facets of these differences are suggested above: a recording can permanently capture a conversation, which allows it to be exposed to audiences not initially intended to hear it, outside the full context in which it originally existed. For Justice Cory, the difference between recording a conversation and relying on an informer's memory of it is a matter of progress, of law enforcement using better, more accurate tools to gather evidence. He does not accept that using a new technology changes the nature of the privacy interest.

R. v. Wong (1990)

In *R. v. Wong* (hereafter *Wong*), the police conducted electronic surveillance of a hotel room to determine whether it was being used as an illegal gambling parlour. The police

[6] For a full discussion of the ways in which technology is not as objective as it seems, see Lessig 1999.

installed a small camera in the drapery to visually monitor and record the activities in the room. The judgement addresses the difference between using undercover agents and surreptitiously monitoring, but the reasoning focuses on the issue of whether by inviting others (including strangers) to attend an event, that event becomes public, regardless of location.

The Ontario Court of Appeal judgement, again written by Justice Cory, argues there is no reasonable expectation of privacy in the hotel room, based on the premise "that a person attending a function to which the general public has received an open invitation can have no interest in 'being left alone'" (para. 17). In this context, the hotel room ceases to be a private space when Mr. Wong invites others, strangers, into the room, thus eliminating a privacy interest in the activities conducted in that space. Although Justice Lamer supports the findings of the majority decision, he disagrees with some of the reasoning. In the additional reasons he provides, he argues "a reasonable person would know that when such an invitation is extended to the public at large one can no longer expect that strangers, including the police, will not be present in the room. In this case, the police effected their presence in the room via the video camera which was installed in the drapery valence" (para. 50).

This reasoning makes an unfounded logical leap. Indeed, by circulating invitations Mr. Wong likely expected strangers, among whom there could reasonably could be undercover agents. However, it is equally reasonable to expect these strangers to be present physically. The police in this case were not physically present, but "attended" through a minute, hidden camera. Justice La Forest supports this view when he writes, focusing on the aspect of recording, "it is not part of the reasonable expectation of those who hold or attend such gatherings that as a price of doing so they must tacitly consent to allowing agents of the state unfettered discretion to make a permanent recording of the proceedings" (para. 23). Justice La Forest argues for the difference between using physical undercover agents and surreptitious electronic monitoring and recording technology in much the same way he does in *Duarte* (1990). Furthermore, social conventions and their accompanying expectations generally assume reciprocity in visual space; when someone can see you, you can see that person. The monitoring in *Wong* breaches Marx's notion of normative sense boundaries (2001; 1997). For Mr. Wong to expect that by opening his hotel room to "the public", those privy to the activities in the room would include more than just those physically present is not reasonable.

Furthermore, the idea that Mr. Wong opened the hotel room to "the general public" (*Wong*, 1990, para. 17) or the "public at large" (para. 50) implies anyone could attend. This seems to misrepresent Mr. Wong's actions. The account is too broad. Mr. Wong circulated notices within a particular community, specifically Toronto's Chinese community. This narrower understanding is supported by the fact that the police did not believe they could use undercover agents because "they were certain that the gaming would be conducted behind locked doors, by and for Orientals alone" (para. 4) and all the Asian officers on the force were known in the community.[7] Therefore, to suggest that

[7] However, as Justice Wilson points out in his dissent, there were only 11 Asian officers on the Metro Toronto Police Force at the time, and he aptly asks, "can one really rely on one's own discriminatory

these events were somehow open to the general public is to overstate the situation and imply that the event was more public than it actually was. This is particularly problematic when the presence of "the general public" or the "public at large" is used to deny an expectation of privacy.

It seems likely that Mr. Wong had a reduced expectation of privacy because of the presence of strangers; but was the expectation of privacy so reduced as to eliminate any privacy interest whatsoever, even with regard to surreptitious recording and monitoring of events? Certainly, Mr. Wong would not have the same argument if undercover agents or informers were used. This case seems to fall somewhere between a full expectation of privacy and no expectation of privacy whatsoever.

R. v. Wise (1992)

The surveillance in *R. v. Wise* (hereafter *Wise*) involves the use of a tracking device, referred to as a beeper, to monitor movement of a motor vehicle. Mr. Wise was a suspect in a series of homicides and the police wanted to track his movement. The case hinges on whether there can be a reasonable expectation of privacy in one's movements when in public, namely on public roads. An interesting difference from *Duarte* (1990) and *Wong* (1990) is that Justice Cory, now part of the Supreme Court, writes the Supreme Court majority decision to which Justice La Forest provides a lengthy dissent. The reasoning in this judgement focuses primarily on the activity of driving on public roads and to a lesser degree on the sophistication of the technology used.

Justice Cory argues that because driving is a highly regulated activity, for which licenses are granted and rules enforced, a "reasonable level of surveillance of each and every motor vehicle is readily accepted, indeed demanded, by society to obtain this protection" (para. 6). Although he does not explain the scope of a "reasonable level of surveillance" here, monitoring public roads for speeding or dangerous or drunk driving can be construed as legitimate and expected. However, this is surveillance of compliance with established rules of behaviour in a particular place (public roads), and is not the same as constant surveillance of a particular vehicle over space and time, as occurred in *Wise*. Justice Cory's reasoning conflates two kinds of surveillance: monitoring compliance with regulations and conditions under which drivers are permitted to operate motor vehicles on public roads, and monitoring of the movements of individuals in their vehicles over geographical space and periods of time outside the context of driving regulations. While society may demand and reasonably expect the former, it in no way demands or expects the latter.

The reasoning underlying this position is that being seen is tantamount to being watched with scrutiny and that if one can be seen it is implicitly acceptable to monitor that person. This fails to acknowledge the qualitative difference between being seen and being watched closely. Indeed, Justice La Forest rejects the idea that just because one can be seen it is acceptable to monitor them by citing Marvin Gutterman (1988), who writes, "in a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be […] subject

---

hiring practices as justification for violating the rights of visible minorities? The idea somehow seems offensive" (para. 69).

to extensive surveillance, but seek to merge into the 'situational landscape'" (cited at para. 71). Seeing a vehicle involves only registering its presence visually, maybe noting its presence, maybe not. Watching, however, requires greater attention, yet can still be done in an idle or unfocused fashion. However, to watch a vehicle (or any moving object) for any length implies following it. Surveillance or monitoring in this case requires not only watching, but focusing on and following the movements of the vehicle, monitoring it across time and physical space. While it is certainly reasonable to expect that when driving, one's movements will be seen, perhaps even noticed or watched as you pass, it is not reasonable to expect that one's movements will subject to enduring scrutiny or tracking, unless one's road behaviour has legitimately attracted focused attention, as in the case of dangerous driving.

The second aspect of Justice Cory's argument for a lesser expectation of privacy hinges on the level of sophistication of the tracking device. It is a "low power radio transmitter. From the strength of the signal, it was possible to determine the general location of the vehicle" (para. 8). He argues that because the device is not very sophisticated, it is minimally intrusive. For example, the beeper was not "capable of tracking the location of a vehicle at all times" (para. 7). Thus, the surveillance is not constant and does not intrude as much on the suspect's privacy as would constant surveillance. Justice Cory also argues that the beeper "simply augments visual surveillance […]. It simply enhanced the ability of the police to observe its movements" (para. 28). Here Justice Cory draws an analogy to the completely acceptable use of binoculars to assist in visual surveillance. Although binoculars do enhance a physical sense, sight, they do not allow the user to find objects without first knowing where they are; the beeper does.

Much of the reasoning in Justice La Forest's dissent is similar to that found in the two previous judgements. He focuses on the electronic nature of the tracking device, its surreptitious use, and its difference from manual surveillance. He argues, "the crucial point is that there is a qualitative difference between the risk that one's movements in a car will be observed by others, including the authorities, and the risk that one's vehicle will be monitored by a device that follows its every movement" (para. 80). Indeed, just as there is a difference between seeing and watching, there is also a difference between watching and monitoring or tracking.

Finally, Justice La Forest does not accept Justice Cory's reasoning that simply because the beeper is relatively unsophisticated and requires some proximity to the subject, that its use should not be regulated. For Justice Cory, the combination of the vehicle travelling on public roads and the minimal intrusion of the tracking device based on its lack of sophistication results in a much-reduced privacy interest. Justice La Forest argues that the decision in this case should regulate the use of tracking technologies more generally because this technology will likely expand to new and unforeseen levels, through which surveillance can occur without the need to also physically or visually monitor. Indeed, one need only think of Global Positioning Systems (GPS), now a basic component of tracking devices and installed in most new vehicles, to validate La Forest's concern. As in the other two cases, Justice La Forest argues that this view does not take into account the implications of the technology. In terms of the expectation of privacy while travelling on public roads, or generally when in public, three distinctions can, and should, be made. We must distinguish between seeing, watching, and monitoring/tracking movement. The same

distinctions based on the degree of attention paid can be made for other sense perceptions, such as hearing, listening, and recording. Making these distinctions deflates easily made, but inaccurate, connections, such as that because one can be seen, one can be monitored.

R. v. Tessling (2004)

In *R. v. Tessling* (hereafter *Tessling*), the police flew over Mr. Tessling's home and used forward-looking infrared (FLIR) technology to capture an image of the heat distribution on the walls of his home in order to develop an idea of whether he was growing marijuana inside. The judgement focuses on the capability and sophistication of the FLIR technology, specifically whether it allows law enforcement to "see" inside the home, thus constituting a search of the home, which clearly requires a warrant.

Tessling is a unanimous judgement of the Supreme Court, written by Justice Binnie, which overturns the Ontario Court of Appeal judgement, written by Justice Abella (who has since joined the Supreme Court). Justice Abella finds that FLIR technology constitutes a search of the home, a space generally accorded the highest level of privacy protection, because it is used to gather information about what is happening inside that home. Justice Abella argues,

There is an important distinction between observations that are made by the naked eye or even by the use of enhanced aids, such as binoculars, which are in common use, and observations which are the product of technology […]. The FLIR technology goes beyond observation, disclosing information that would not otherwise be available and tracking external reflections of what is happening internally. (*Tessling*, 2004, para. 10)

A subtext of this argument is that there is also a difference between police use of technologies (sophisticated or otherwise) that are available to the general public and those that are not. Although somewhat vague, this notion of "in common use" seems to imply that expectations of privacy with respect to a given technology are influenced by its availability and the general public's ability to understand and "expect" its use. If this is indeed the meaning, the common use factor is somewhat problematic. As discussed earlier, simply because a particular practice exists, or even is in common use, does not imply that it therefore does not or cannot infringe on privacy.

Justice Binnie disagrees, arguing that using FLIR technology is not "*equivalent* to a search *of* a home but an external search for information *about* a home" (para. 27, original emphasis). The former requires a warrant and is protected under S.8 of the *Charter*, while the latter is not. Justice Binnie also rejects following the findings of the United States Supreme Court in *Kyllo v. United States* (2001), as a similar case regarding the use of FLIR technology, which he explains determines a privacy interest in this information "based largely on the 'sanctity of the home'" (*Tessling*, 2004, para. 45).

Justice Binnie disputes Justice Abella's first contention, that the information is not available to the naked eye but is the product of technology, by arguing that there is no serious privacy interest in this case because heat released from a home is a "voluntary exposure of information" (para. 39). Further, Justice Binnie explains, "Living […] in a land of melting snow and spotty home insulation, I do not believe that the respondent has a serious privacy interest in the heat patterns on the exposed external walls of his home"

(para. 41). His argument culminates with the fact that the current technology cannot "see" what is happening in the home because it cannot reveal the cause of uneven heat distribution. Justice Binnie chooses not to use this case to regulate FLIR technology, but explains that should the technology arrive at that state where it can see into a home, the findings of this case would be open to revision.

Much is made in this judgement of the technology's inability to "see" into the home. However, it is not clear what exactly Justice Binnie means by "seeing." It is true that FLIR technology does not produce an image like a photograph or like something a person would see with his or her eyes. FLIR technology produces an image of heat distribution within a space. However, in a way, this is seeing what is happening inside of the home, but differently than one would see with one's eyes. Is this a case of law enforcement using better tools to do what they have always been entitled to do, to examine the outside of a home, or is it something qualitatively different?

Justice Binnie's analogy to the ability to physically see the result of heat leakage from a home because of poor insulation and melting snow, although possibly made flippantly, is not particularly helpful and does not fully refute Justice Abella's position that the images are the result of technology and are not observable with less sophisticated technologies. Furthermore, if taken seriously, this type of information is only voluntarily exposed, by virtue of being observable, in the winter (and when there is snow). If this were to be used as a basis for regulating warrantless use of FLIR technology, then it would be acceptable in winter, but not at other times, which is absurd. While this is likely not Justice Binnie's intent, it points to the problem of drawing analogies to human abilities to justify use of surveillance technologies.

Justice Binnie's overall approach in this judgement is closer to the Cory approach than to the La Forest approach. Justice Binnie stays closely focused on the facts of the case and technology as it exists at the time of the incident. He does not, as does the La Forest approach, determine the existence of a privacy interest by starting from the broader perspective of asking whether using FLIR technology to capture the heat distribution patterns of any home without judicial oversight should be acceptable in a free and democratic society. That *Tessling* finds a warrant is not needed to conduct this sort of surveillance could be construed as opening the door to "fishing" for evidence among the general population. If the reasoning had followed an approach closer to that of Justice La Forest, and considered whether this type of police action is acceptable to conduct on any or all members of society, it is possible that the judgement would have found a need for judicial oversight in the use of FLIR technology.

Conclusions

The discussion of each of the four cases focuses on how the judgements understand a reasonable expectation of privacy with respect to the implications and "salient features" (Austin 2003) of the specific technologies used, and the distinctions between private and public.

The discussion of *Tessling* (2004), like *Duarte* (1990) and *Wong* (1990), reveals the danger of drawing analogies to human capabilities to justify use of more sophisticated surveillance technologies. More importantly, this case highlights the strength, in terms of privacy protection, inherent in Justice La Forest's approach to determining privacy interests. Asking whether it is appropriate to conduct electronic surveillance on any member of society at the sole discretion of the police, not only the person in question in a given case, tends toward findings that require judicial oversight. This also helps prevent finding lower thresholds of privacy for those who have committed a crime or are suspected of committing a crime. Through examining the facts and reasoning in *Duarte* (1990), *Wong* (1990), and *Wise* (1992) two series of distinctions were developed – the capture, exposure, context series, and the see/hear watch/listen, monitor/capture series.

The facets of the capture, exposure, and context series were developed in an attempt to identify implications of the surveillance technology used, specifically the qualitative differences between electronically recording conversations and activities, and human reporting on the same things. Recording an event, for example, captures that event precisely as it transpired. It is permanent and can be saved for use later. This action freezes time in a sense, removing the ephemeral or transitory nature inherent in the passage of time. Recording an event also allows it to be exposed to others not originally present and outside its original context. These facets have distinct implications for privacy because they alter who controls the information and how it is controlled. Those captured by a recording are no longer in control of what they expose about themselves and to whom. In a particular conversation, the parties involved may be content to share information with each other, but might not want that information to be more widely known. A permanent recording, however, can easily and at any time present the conversation itself to others without the knowledge or consent of the parties involved.

The second series of distinctions is based on the importance of recognizing differences between the degrees of attention paid by others to our activities. Justice Cory claims in *Wise* (1992) that, when in a public place, such as when driving on public roads, there is a minimal expectation of privacy because one knows one can be seen. This type of reasoning is unsatisfying. Further, it completely ignores distinctions between being seen, being watched, and being monitored or recorded. Justice La Forest notes the difference between being seen/heard and being recorded in *Duarte* (1990) and *Wong* (1990), but this paper suggests that these distinctions break down further to include the intermediate step of watching/listening. Distinguishing to this degree helps in determining a reasonable expectation of privacy. If we accept that being seen or being visible in public is different from being watched, then one can still have a reasonable expectation of privacy despite being in public, and it helps avoid simplistic justifications for surreptitious monitoring achieved through conflating seeing (visibility) and watching (monitoring).

The two interrelated series of distinctions developed here are helpful in understanding the nuances of surveillance technology with respect to determining privacy expectations outside these cases. If we turn to *Aubrey v. Editions Vice-Versa* (1998), a Supreme Court of Canada judgement of a Quebec civil law case, we can see that the distinctions developed here can be helpful in a broader context. Editions Vice-Versa photographed Ms. Aubrey, without her consent, and proceeded to publish and circulate the photo in their magazine. Ms. Aubrey argued her privacy was invaded. Ms. Aubrey's expectation,

sitting in public, was certainly that she would be seen, possibly even noticed or watched, but she had no expectation of being photographed, or of having her image captured and then exposed to others beyond those she could also see during the time she sat on the steps, in other words, to those outside her immediate, temporal, and geographic context. The distinctions developed here help us identify and articulate what is at issue in *Aubrey v. Editions Vice-Versa* (1998).

The two series of distinctions developed here can also help outside the context of search and seizure identify the implication of surveillance technologies in the area of policy development, for instance when making decision about implementing or expanding use of CCTV in public spaces. Often in such discussions, concerns of the implications for privacy are too easily dismissed on the grounds that those captured on camera have no privacy interest because they are in public and should expect to be seen. Furthermore, asking if subjecting everyone and anyone to particular forms of surveillance opens allows a broader discussion to occur, taking into account not only those intended targets of surveillance, like criminals or potential terrorists.

As surveillance technologies become increasingly sophisticated and pervasive, and are used by both law enforcement and the private sector, sometimes collaboratively, as well as by individuals, it becomes particularly important to understand the subtle distinctions of the technologies, and their relation to social and contextual norms and expectations when determining privacy interests. If these issues and the nuances of surveillance technologies and of the relationship between private and public are not accurately reflected in judicial reasoning and policy making, the ability to protect individuals' privacy interests will be at risk.

References

Cases

Aubrey v. Editions Vice-Versa. 1 S.C.R. 591. (1998)
Hunter v. Southam Inc. 2 S.C.R. 145. (1984)
Kyllo v. United States. 533 U.S. 27. (2001)
Lopez v. United States. 373 U.S. 427. (1963)
R. v. Arp. 2 S.C.R. 339. (1998)
R. v. Duarte. 1 S.C.R. 30. (1990)
R. v. Dyment. 2 S.C.R. 417. (1998)
R. v. Plant. 3 S.C.R. 281. (1993)
R. v. Tessling. S.C.C. 67. (2004)
R. v. Wise. 1 S.C.R. 527. (1992)
R. v. Wong. 3 S.C.R. 36. (1990)

Other sources

Allen, A. (1998) *Uneasy access: Privacy for women in a free society.* Totowa, NJ: Rowman and Littlefield. As cited in Marx 2001.

Austin, L. (2003) Privacy and the question of technology. *Law and Philosophy* 22: 119-166.

Canada. Privacy Act. R.S. 1985, c. P-21. http://laws.justice.gc.ca/en/P-21/index.html [Accessed March 22, 2005]

Canada. *Personal Information Protection and Electronic Document Act.* S.C. 2000 c. 5. http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp [Accessed January 15, 2006]

Canadian Charter of Rights and Freedoms. In United Kingdom. (1982) *Canada Act*. (Schedule B). http://laws.justice.gc.ca/en/charter/ [Accessed October 12, 2005]

Canadian Legal Information Institute (CANLII). (2004a) *Canadian Charter of Rights Decisions Digest – Section 7*. http://www.canlii.org/en/ca/charter_digest/s-7.html [Accessed February 12, 2007]

Canadian Legal Information Institute (CANLII). (2004b) *Canadian Charter of Rights Decisions – Section 8.* http://www.canlii.org/en/ca/charter_digest/s-8.html#_Toc68428968 [Accessed February 12, 2007]

Cavoukian, A. (1999, September) *Privacy as a fundamental human right vs. and economic right: An attempt at conciliation*. Toronto: Information and Privacy Commissioner/Ontario. http://www.ipc.on.ca/index.asp?navid=46&fid1=317 [Accessed October 2006]

Cavoukian, A. & Tapscott, D. (1995) *Who Knows: Safeguarding Privacy in a Networked World.* Toronto: Random House.

European Union. (1995) *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm [Accessed July 19, 2007]

Gutterman, M. (1988) A formulation of the value and means models of the Fourth Amendment in the age of technologically enhanced surveillance. *Syracuse Law Review* 39. As cited in *R. v. Wise* (1992).

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books

Marx, G.T. (2001) Murky conceptual waters: The public and the private. *Ethics and Information Technology* 3: 157-169.

Marx, G.T. (1997) The declining significance of traditional borders (and the appearance of new borders) in an age of high technology. In P. Drogue (Ed.). (1997). *Intelligent Environments*. New York: Elsevier, 484-494. http://web.mit.edu/gtmarx/www/ascbord.html [Accessed June 14, 2005]

Nissenbaum, H. (2004) Privacy as contextual integrity. *Washington Law Review* 79: 119-158.

Nissenbaum, H. (1998) Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy* 17: 559-596.

Ontario. Freedom of Information and Protection of Privacy R.S.O. 1990, c. F-31. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm [Accessed March 22, 2005]

Paton-Simpson, E. (2000) Privacy and the reasonable paranoid: The protection of privacy in public places. *University of Toronto Law Journal* 50(3): 305-346.

Reiman, J. (2004) Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the information technology of the future. In B. Rossler (Ed.). *Privacies: Philosophical Evaluations*. Stanford, CA: University of Stanford Press, 194-214.

Rossler, B. (2004) Privacies: An overview. In B. Rossler (Ed.). *Privacies: Philosophical Evaluations*. Stanford, CA: University of Stanford Press, 1-18.

Sheller, M. & Urry, J. (2003) Mobile transformations of 'public' and 'private' life. *Theory, Culture and Society* 20(3): 107-125.

Solove, D.J. (2002) Conceptualizing privacy. *California Law Review* 90(4): 1087-1155.

Solove, D.J. (2001) Privacy and power: Computer databases and metaphors of information privacy. *Stanford Law Review* 53(6): 1393-1462.

Viseu, A., Clement, A., & Aspinall, J. (2004, March) Situating privacy online. *Information, Communication and Society* 7(1): 92-114.

Westin, A.F. (1968) *Privacy and Freedom*. New York: Atheneum.