One Step Forward or Two Steps Back? R. V. Tessling and the Privacy Consequences for Information Held by Third Parties.

Lisa M. Austin

Version Publisher's version


How to cite TSpace items

Always cite the published version, so the author(s) will receive recognition through services that track citation counts, e.g. Scopus. If you need to cite the page number of the author manuscript from TSpace because you cannot access the published version, then cite the TSpace version in addition to the published version using the permanent URI (handle) found on the record page.

This article was made openly accessible by U of T Faculty. Please tell us how this access benefits you. Your story matters.
Notes and Comments

One Step Forward or Two Steps Back?
R. v. Tessling and the Privacy Consequences for Information Held by Third Parties

(1) Introduction

After the Ontario Court of Appeal ruled in R. v. Tessling that the RCMP's use of infrared camera technology without a warrant violated s. 8 of the Charter, Mr. Tessling's lawyer argued that this decision "raise[s] the protection of privacy for everyone". This comment disagrees and argues that although Tessling puts the brakes on the warrantless use of surveillance technology by the state, it actually makes it easier for the state to get access to information held by third parties without a warrant. This lowers, rather than raises, the protection of privacy in Canada. In particular, the Ontario Court of Appeal's attempt to distinguish the search in Tessling from the Supreme Court of Canada's decision in R. v. Plant may be detrimental to the overall privacy afforded to Canadians under the Charter.

(2) R. v. Tessling

The appellant in Tessling was accused of operating a marijuana-growing operation. The investigation at issue began when the police received information from two confidential informants indicating that the accused was involved in the production and trafficking of marijuana. However, upon inquiry, Ontario Hydro indicated that the electricity consumption at the property owned by Tessling was normal. Visual surveillance of the property revealed nothing. Suspecting that Tessling might be circumventing hydro in his energy consumption, the police then decided to use an RCMP airplane equipped with Forward Looking Infra-Red (FLIR) technology in order to determine the nature of the heat emanations from the buildings on the property.

As the Ontario Court of Appeal outlined, "The FLR takes a picture or image of the thermal energy or heat radiating from the exterior of a building. It can detect heat sources within a home depending on the location of the source, and how well the house is insulated, but it cannot identify the exact nature of that source or see inside the building." Given that the lights from a marijuana grow operation give off an unusual amount of heat, the pattern of specific heat sources in a particular building can lead to the inference that marijuana is being grown at that location. Indeed, on the basis of the FLIR examination and the information from the two informants, the police obtained a warrant to enter Tessling's home, where they found a large quantity of marijuana.

At trial, Tessling brought an application under s. 24(2) of the Charter to exclude the evidence obtained by the search of his home. He argued that the warrant was based on insufficient evidence and that the use of FLIR technology constituted an unlawful search within the meaning of s. 8 of the Charter. The trial judge disagreed with both propositions. In rejecting the s. 8 argument, the trial judge compared the use of FLIR technology to other forms of unobjectionable police surveillance:

There is nothing wrong in police officers [placing a home under surveillance] from outside its perimeter boundaries to determine if people come and go in such numbers as to indicate to experienced police officers that marijuana growing and/or trafficking activity is going on inside. This is simple surveillance.

If he was wrong regarding his determination that s. 8 was not violated, the trial judge determined that he would not exclude the evidence under s. 24(2). The accused was convicted as charged.

Tessling appealed his conviction on the ground that the trial judge was incorrect in holding that police use of a FLIR aerial

2. Shannon Karl, "Court shoots down evidence obtained by infrared eye in the sky", The Ottawa Citizen (January 28, 2003).
4. Supra, footnote 1, at paras. 2-5.
5. Ibid., at para. 9.
7. Ibid., at para. 21.
camera without prior judicial authorization did not violate s. 8 of the Charter of Rights and Freedoms. Abella J.A., writing for the court, disagreed with the trial judge’s analogy to other permissible forms of placing a home under surveillance. Abella J.A. held that although FLIR technology measures heat emanating from outside the home, it is more properly characterized as obtaining information about what activities are taking place within the home: “The fact that it is necessary for the police to draw inferences from the heat emanating from the external walls in order to deduce what those internal activities are, does not change the nature of what is taking place.” Moreover, the information disclosed by the use of FLIR technology is far more extensive than what may be gleaned by normal observation or surveillance.

In determining that an individual has a reasonable expectation of privacy with respect to the heat emanating from activities within the home, Abella J.A. had to deal with the Supreme Court of Canada decision in Plant. There, the court had held that warrantless access to electricity consumption records did not violate s. 8 of the Charter because such records did not engage a reasonable expectation of privacy. Abella J.A. distinguished Plant by emphasizing the reasoning that Sopinka J. engaged in with respect to the question of confidentiality rather than privacy. She argued:

It is significant that the focus of the analysis in Plant was not on whether there is a privacy interest in home energy consumption, but on whether one has a reasonable expectation of privacy in records held by third parties. The court focused on the commercial relationship between the utility company and the accused as a utility user, concluding that the information available in the records was subject to inspection by members of the public at large. This supported the finding that the accused did not have a reasonable expectation of privacy in the records.

Later in her judgment, she stated: “Unlike Plant, where the information sought by the state is already known and in the hands of a third party, namely the utility company, this is information unknowable without the FLIR technology.”

Abella J.A. then held that, given that the breach to individual privacy in Tessling was serious, and given the growing “public, judicial, and political recognition that marijuana is at the lower end of the hierarchy of harmful drugs”, the evidence should be excluded under s. 24(2). The Court of Appeal set aside the conviction and ordered an acquittal. The Supreme Court of Canada has granted the Crown leave to appeal.

(3) Analysis

(a) The Problem of Plant

Part of the difficulty in Tessling is that the nature of the information at issue is strongly similar to the nature of the information at issue in Plant: both cases dealt with information about home energy consumption. However, in Plant, the Supreme Court of Canada held that

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

One way to distinguish the cases is to focus on the differences in the nature of the information disclosed by FLIR technology as compared to electricity consumption. Many of Abella J.A.’s comments regarding the extensiveness of the inferences that may be drawn about activities within the home from the use of FLIR technology suggests that she endorses this strategy. However, Abella J.A.’s explicit treatment of Plant focuses instead on aspects of the creation of the information in Plant and the relationship between the individual and the utility company, rather than on the nature of the information itself. It is this strategy that
is deeply flawed. The suggestion that s. 8 protection of privacy is significantly lowered when information is created by and in the hands of third parties outside of a confidential relationship would in fact sanction state access to vast amounts of information without judicial oversight. We would never permit the state to create a database of personal information about Canadians as extensive as the de facto database that exists throughout the private sector, and we should therefore be very cautious in permitting state access to such information without meaningful controls. Moreover, as this comment argues below, such a result is in tension with existing s. 8 jurisprudence.

Information Already Known vs. Information Created by the State

One of the major ways in which Abella J.A. distinguished Plant was by arguing that Plant dealt with a case where the information was "already known and in the hands of a third party" rather than created by the state. The implication of this is that the police must get a warrant to create information that, had it already existed in the hands of third parties, they could get access to without a warrant. The plausibility of this proposition depends upon the assumption that once information is already known and in the hands of third parties, there is no remaining expectation of privacy sufficient to engage s. 8 of the Charter. However, this assumption is deeply problematic.

One version of the argument that information in the hands of third parties does not engage a reasonable expectation of privacy is that an individual, in disclosing information to another, runs the risk of having this information divulged to the state. This indeed has been the much-criticized reasoning of the United States Supreme Court with respect to third parties. However, the importation of this kind of "risk analysis" was specifically rejected by the Supreme Court of Canada in R. v. Duarte and there is no compelling reason to revive it.

The assumption that an individual's privacy interest is lost once information is disclosed to third parties is also in tension with current Supreme Court jurisprudence regarding s. 8. As stated in R. v. Mills, privacy is not an "all or nothing" right and "Where private information is disclosed to individuals outside of those to whom, or for purposes other than for which, it was originally divulged, the person to whom the information pertains may still hold a reasonable expectation of privacy in this information." More recent cases have confirmed this and have held that information held by the state for one purpose may not be shared with law enforcement officers without a warrant.

Abella J.A.'s reasons are also in tension with the Supreme Court of Canada's treatment of information in the hands of third parties in R. v. Dyment. Dyment concerned a blood sample that had been taken by a physician from his unconscious patient and which was voluntarily handed over to the police. The question was whether the taking of the blood by the police violated s. 8 of the Charter. La Forest J. argued: "If I were to draw the line between a seizure and a mere finding of evidence, I would draw it logically and purposefully at the point at which it can reasonably be said that the individual had ceased to have a privacy interest in the subject matter allegedly seized." The implication of this is that just because information is in the hands of a third party and is voluntarily provided to the state does not mean, in itself, that the individual has no remaining privacy interest in that information.

Commercial Relationship where Information is Available to the Public

The second, although not unrelated, way in which Abella J.A. distinguished Plant from Tessling was to argue that Plant did not

---

15. Tessling, supra, footnote 1, at para. 67.
turn on the nature of the privacy interest in home energy consumption but on the nature of the commercial relationship between the individual and the utility company and the fact that the utility company made the information available to the public. However, it is important to note that Sopinka J.'s comments in Plant regarding the fact that electricity consumption is information that is made available to members of the public who request it were made in the context of his finding that the relationship at issue was not one of confidentiality. For Sopinka J., confidentiality was one aspect of his "contextual" approach to determining a reasonable expectation of privacy. Abella J.A.'s reliance on this element of Plant as determinative suggests that the state may have warrantless access to all non-confidential information held by third parties. This reading of Plant is deeply problematic: privacy and confidentiality are not the same thing and an emphasis on confidentiality may narrow the scope of s. 8 protection of informational privacy.

Although privacy and confidentiality are often used loosely and interchangeably, they refer to distinct but overlapping ideas. The law of confidential information protects information that is confidential and that has been disclosed in circumstances giving rise to an obligation of confidence. Confidential information is information that is "secret" in the sense that it is not disclosed to the public. This is why Sopinka J. focused on whether information about electricity consumption was easily available to others: if so, then it could not be said to be confidential information. Whether information is confidential is therefore a factual inquiry into whether the information in issue has been kept secret to a sufficient degree.

Confidential information, understood in this manner, is not necessarily the same thing as "private" information. First, the inquiry into whether information is "private" is a normative inquiry into the nature of the information at issue and its connection to the underlying values protected by privacy. It is not a descriptive inquiry into whether others in fact have access to that information. Indeed, the conflation of privacy and secrecy that arises when privacy and confidentiality are not differentiated has been decried by many commentators as creating a situation in which it is very difficult to articulate a privacy interest in "public" information.

Second, there are many plausible claims to a privacy interest even where information is in some sense open to public view and therefore no longer "confidential". The Supreme Court of Canada has upheld publication bans in order to protect privacy even where the public is entitled to be present in the courtroom; it has recognized a privacy interest in an individual's movements in his car over public roads; and it has recognized a privacy interest in a photo taken of a young woman sitting in a public place. Similarly, the United States Supreme Court has recognized a privacy interest in a compilation of public records. In none of these cases would the information at issue qualify as "confidential". Abella J.A. herself cited with approval two Canadian cases that held that s. 8 required a "more textured analysis than simply asking whether the information in issue was accessible to public view".

Third, confidential information only receives protection where there is a relationship of confidence, which is part of the reason

23. See, for example, the analysis of s. 8 as it applies to therapeutic records in Mills, supra, footnote 18.
why Sopinka J. in *Plant* discussed the nature of the commercial relationship between the individual and the utility company. However, there are many plausible circumstances for the protection of privacy that do not involve a relationship of confidence. For example, the House of Lords, while holding that there is no general right to privacy in English common law, has acknowledged that the law of confidentiality would not apply to the complaints arising out of a strip search.30 Similarly, the European Court of Human Rights recently held that the law of confidentiality could not plausibly catch the broadcast of footage of an attempted suicide captured by a closed circuit television camera even though this was a violation of privacy.31

In these ways, confidential information is a potentially narrower category of information than private information. Confidential information is also a potentially broader category of information than private information, for it does not simply catch personal confidences but also business confidences. What is perhaps a source of confusion is that the Supreme Court jurisprudence on s. 8 has repeatedly included the language of confidentiality in its discussions regarding whether there exists a reasonable expectation of privacy. For example, in its recent discussion of informational privacy as it relates to business documents in *R. v. Law*, the court stated: “a proprietor’s control over confidential business documents implicates his individual autonomy and, in tum, ‘has profound significance for the public order’.”32 Rather than conflating privacy and confidentiality, however, it is preferable to argue that s. 8 protects both private and confidential information.

Being clear on the relationship between private information and confidential information is important. Information that is both private and confidential is, and should be, protected by s. 8. In addition, according to *Law*, confidential business information is protected by s. 8 and there seems no reason to require the further argument that this information is also private. It should also be the case that information that is private but not confidential should be protected by s. 8. However, Abella J.A.’s reliance on Sopinka J.’s statements regarding the commercial relationship at issue in *Plant* implies that information in the hands of third parties must be both private and confidential to attract constitutional protection. This reasoning dramatically reduces the scope of s. 8 protection.

Furthermore, to protect only information that is both private and confidential cuts against most developments of the protection of privacy outside of the constitutional realm. Private sector data protection law such as the federal Personal Information Protection and Electronic Documents Act33 put in place a regime that provides protection for personal information in the hands of third parties that far exceeds the protection offered by the law of confidentiality. However, all such laws permit the sharing of information with the state for law enforcement purposes.34 Therefore it is s. 8 of the Charter that determines the question of when the state will be permitted access to information in the hands of third parties. It would be contrary to the spirit of all such private-sector gains in privacy protection to permit the state to have warrantless access to such information unless that information can meet the requirements of confidentiality.

(b) An Alternative: An Emphasis on the Nature of the Information

Although there are criticisms that may be made of the *Plant* decision, the Supreme Court of Canada has invoked it in many recent cases and is not likely to explicitly overturn it.35 Assuming therefore that *Plant* is, and will remain, good law, it must be distinguished from *Tessling* on different grounds than those focusing on circumstances where non-confidential information is in the hands of third parties. A better distinction is one that directly confronts their differences in terms of the nature of the information itself. However, this question should not be cast in terms of electricity consumption versus heat emanations. What is important is the question of what kind of inferences about activities

---

31. *Peck v. United Kingdom*, [2003] E.M.L.R. 15. Because of this, the court held that the applicant had no effective domestic remedy for the violation of his right to a “private life” as protected by article 8 of the European Convention on Human Rights.
33. S.C. 2000, c. 5.
34. Section 7(3)(c), (d) and (d).
within the home may be drawn from electricity consumption records on the one hand and FLIR technology on the other.

Electricity records provide aggregate information about electricity use over a period of time. The inferences that can be drawn from such information are very general. The information can be compared to other similar households in order to determine if the electricity consumption is higher than average, which is the basis for suspecting a marijuana grow operation. However, other inferences that may be drawn regarding the types of activities that might account for a particular pattern of electricity consumption are quite speculative and not particularly revealing. This is not because electricity consumption is not tied to activities within the home but rather because one cannot draw many specific inferences from such general information. Even McLachlin J., as she then was, who would have found a reasonable expectation of privacy in the electricity records, acknowledged that for her the case was "close to the line".36

In contrast, although thermal imaging technology captures heat emanating from the home, it does so in a manner that shows patterns of heat emanation and not simply the overall aggregate amount of heat emanating from the home. Moreover, this information can be pinpointed to the time that the picture or image is taken. In this way, FLIR technology allows its users to determine the general location of heat sources and to do so at particular times. This ability enables users potentially to draw many more inferences regarding the activities that may be going on in the home than the electricity consumption records that were at issue in Plant would have provided. Indeed, it makes this technology much more like the rudimentary tracking device at issue in Wise, where police had installed a radio transmitter in a suspect's vehicle that could determine its general location.37 Cory J. described the tracking device at issue as:38

unsophisticated and indeed simplistic. It did not provide a visual record of the movement or position of the vehicle. Nor was it able to pick up and record conversations in the vehicle. Rather, it was capable of giving only a very rough idea of the vehicle's location. Certainly, it could not be said

that the device was capable of tracking the location of a vehicle at all times.

Nonetheless, even this rudimentary level of information collection was held to meet the threshold for engaging s. 8 and it did so even though it involved tracking movements made in public while engaging in what is a highly regulated activity — driving.

(4) Conclusions

The result that the Ontario Court of Appeal came to in R. v. Tessling is the right one. However, the major stumbling block for this result is the Supreme Court of Canada's decision in Plant. The strategy that the Ontario Court of Appeal used in order to distinguish Plant is deeply problematic and could potentially undermine privacy much more than if the court had simply upheld the warrantless use of FLIR technology. Instead, Plant should be distinguished from Tessling on the basis of the nature and type of inferences about household activities that may be drawn from the FLIR images in distinction to the electricity consumption records.

Lisa M. Austin*

38. Ibid., at para. 7.

___

* University of Toronto, Faculty of Law. I would like to thank Martha Shaffer and Hamish Stewart for their helpful comments on an earlier draft of this article.