Knowledge is Power: The Criminal Law, Openness and Privacy

Scott C. Hutchison

Follow this and additional works at: http://digitalcommons.osgoode.yorku.ca/sclr

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 4.0 License.

Citation Information
http://digitalcommons.osgoode.yorku.ca/sclr/vol29/iss1/19

This Article is brought to you for free and open access by the Journals at Osgoode Digital Commons. It has been accepted for inclusion in The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference by an authorized editor of Osgoode Digital Commons.
Knowledge is Power:  
The Criminal Law, Openness and Privacy  

Scott C. Hutchison*  

I. THEMES FROM THE PRINCIPAL PAPERS  

1. Information and the Relationship Between Government and the Governed  

Citizens deserve to know, and in some cases need to know, what their governments — including their courts — are up to.  
Governments like to be able to, and in some situations need to be able to gather information about what “the governed” are up to.  
This mutual thirst for knowledge is driven by more than idle curiosity. Sir Frances Bacon’s famous aphorism that “knowledge is power” explains why the control of information defines the relationship between the state and the subject. The balance of power between the two is in many ways a function of, and can be measured by, the ability of each to control the flow of information between them.  
The substantive themes of the two principal papers — openness and privacy — underscore the point that in many ways the success of a democracy can be assessed by how easily the subject can access information about the operations of the state, and by how constrained the state is in gathering information about the subject. The administration of

* Partner, Stockwoods LLP.

1 Bacon is generally credited with this quotation. It has been reported that this motto sits over the office of John Poindexter, the American official responsible for the new U.S. Federal Government “Information Awareness Office” (an Orwellian institution if ever there was one). See W. Safire, “You are a Suspect” New York Times (13 December 2002).

criminal justice, especially in times of national crisis, tests the outer limits of these democratic metrics.

There are, however, elements of the administration of criminal justice that for obvious reasons must take place in secret, even in a democratic state, particularly at the investigative stage.3

In recent times the fear generated by an unknown enemy with unknown resources rightly leaves state authorities anxious to preserve whatever advantage they might enjoy in combating terror. To the extent that the value of information can be compromised by disclosure, there is an understandable desire to keep such information secret. The gravity of the perceived consequences associated with disclosure will sometimes overtake careful consideration of the likelihood of such danger ever actually manifesting itself. Indeed, the consequences of disclosure may sometimes justify secrecy at a lower threshold than might normally be demanded.

Similarly, the state’s desire to gather otherwise “private” information to prevent or prosecute crime, especially crime that challenges the existence of the community as a whole, is the state’s most compelling justification for trenching upon the privacy of citizens. Another aphorism — one overused in recent times — captures cleverly the in terrorem argument that national security provides an unanswerable justification for broadened, unrestrained state authority: “the constitution is not a suicide pact.”4 On this facile theory the continued existence of the democratic state is a value superior to otherwise defining elements of democratic life.

At the end of the day the test of a democratic legal system is not whether it permits secret proceedings, or gives the state the power to discover private information: obviously for any sovereign authority to

---

3 Even the landmark “openness” case of Nova Scotia (Attorney General) v. MacIntyre, [1982] 1 S.C.R. 175, 65 C.C.C. (2d) 129 acknowledged that there had to be recognition of the need for some pre-charge judicial proceedings to be secret for at least a time.

4 D. Corn, “The “Suicide Pact” Mystery Who Coined the Phrase? Justice Goldberg or Justice Jackson?” from the online magazine Slate.com online at: <www.slate.msn.com/id/2060342/> (last accessed 15 June 2005) sets out the competing claims of Robert Jackson and Arthur Goldberg JJ. for credit for the expression. (Jackson J. warned against allowing the constitution to become a “suicide pact” in 1949 in Terminiello v. City Of Chicago, 337 U.S. 1, at 37 (1949), while Goldberg J. warned that “[W]hile the Constitution protects against invasions of individual rights, it is not a suicide pact.” In Kennedy v. Mendoza-Martinez, 372 U.S. 144, at 160 (1963). Contrary to the popular use of the quoted expression, neither case stands for the proposition that the democratic values cease to control when the state is threatened.
function in a meaningful way it must be able do these things, at least some of the time. Our focus should be on the procedures in place to require the justification of these two departures from the (unattainable) democratic ideal of the perfectly unintrusive, transparent state.5

I tend to the view that the Supreme Court of Canada has, by and large, struck an appropriate balance in matters related to the flow of information between and about state and individual. I think, for example, that the Court’s response to the “closed-court” presumption advocated by the Crown in Vancouver Sun6 was correct. We have a very specific conception of what judicial proceedings are supposed to look like, and openness (or at least presumed openness) is an essential element of such proceedings. Again, some departures from this ideal are inevitable: what matters is our commitment to the presumption of openness and the processes by which any departure from that presumption is tested and justified. Similarly, the judgments in Tessling7 and Mann8 are consistent with the Court’s previous jurisprudence and continue to approach issues of privacy and search in a principled, responsible manner. Section 8 guarantees only a reasonable expectation of privacy, a standard which requires an internal balancing of the state’s interest in the prompt and expeditious investigation of crime against the democratic ideal of an unintrusive government. Too broad a reading of reasonable expectation of privacy runs the risk of creating too many hurdles to investigations without significantly increasing the scope of democratically meaningful privacy.

2. Inspiring a Culture of Constitutional Respect

In addition to their examination of the role that information plays in defining the relationship between state and citizen, the two principal papers share a further theme: the importance of a proper constitutional indoctrination for state officials responsible for the invocation or execution of processes that have the potential to infringe constitutional values.

---

The danger they properly identify is that state officials, who normally take the rule of law as a core value, develop a laxity around, or worse yet, a contempt for, the constitutional rights of the individuals they are investigating.

I agree with the principal papers that more must be done to inculcate in every state actor a sophisticated appreciation of, and respect for, constitutional rights. I would offer only two points to supplement their comments. First, I would see national security enforcement as just about the last place to start the process of improving the culture of the enforcement community. A project of improving constitutional respect must begin “from the ground up,” with routine policing rather than with the high stakes world of national security. Second, I would suggest that part of the project has to be to make the constitutional law governing investigations more coherent and accessible. The intricate, finely spun web of constitutional limitations developed over the last two decades has left police with a sort of “constitutional fatigue” which can easily evolve into contempt. Brighter lines (or at least some signal that such lines are being attempted) will enhance constitutional respect by police and other similarly positioned state actors.

II. OPENNESS AND THE INVESTIGATION OF CRIME

Few advocates would go looking for a brief to defend secret court proceedings. The moral and doctrinal deck is stacked against any party trying to encourage a court in this country to conduct judicial business covertly. From at least the time of the Court of Star Chamber under the Stuarts, secrecy has been synonymous with abuse and tyranny. As Professor Paciocco observes, this abhorrence of the covert administration of justice is in some ways peculiar to the common law tradition.

But secrecy is sometimes legitimate and necessary to ensure that the administration of justice (including the investigation of crime) is able to operate effectively. As the majority said in Michaud9 (justifying the rule in wiretap cases which substitutes presumptive permanent secrecy for

---

9 Michaud v. Quebec (Attorney General), [1996] S.C.J. No. 85, 3 S.C.R. 3, at para. 51. Michaud was not, strictly speaking, an open court case, but rather a case examining the standard for access to the sealed packet filed on a wiretap application. While the formal ratio of the case might thereby be distinguished, it is hard to say that the underlying rationale of the case carries no weight in the openness debate.
the usual rule of openness) “[t]he reality of modern law enforcement is that police authorities must frequently act under the cloak of secrecy to effectively counteract the activities of sophisticated criminal enterprises.”

How the presumption of openness is to be set aside is very much driven by the context of the particular case. The Supreme Court of Canada and parliament have consistently called for a context sensitive approach to openness. In *Sierra Club* Iacobucci J. emphasized that these principles “must be tailored to the specific rights and interests engaged” in the particular case. It is intended to be an “adaptable” test used to “balance freedom of expression and other important rights and interests.”

There are at least eight different contexts (and arguably eight different tests) for how openness can be set aside:

(i) *Permanent* trial publication *bans* to protect generic police investigatory techniques (*Mentuck*; *O.N.E.*) (the most demanding standard);

(ii) *Temporary* trial publication *deferrals* to Protect Fair Trial Interest (*Dagenais*);

(iii) *Permanent* trial *bans* to protect Privacy Interests of Complaining Witnesses (*C.B.C. v. New Brunswick*);

(iv) *Automatic* trial and pre-trial publication deferrals to protect privacy and fair trial interests of accused persons (bail publication bans (section 517); preliminary inquiry temporary bans (section 539); proceedings not in the presence of a jury (section 648);
(v) Permanent confidentiality orders arising in Civil Litigation (Sierra Club v. Canada);¹⁷
(vi) In camera orders for investigative hearings into terrorism offences (section 83.28 and Vancouver Sun);¹⁸
(vii) Presumptive permanent sealing and secrecy mandated for authorization materials for both executed and pre-execution wiretap applications (section 187 and Michaud)¹⁹
(viii) Access delay or temporary sealing orders to protect warrant application materials.²⁰

There is a real challenge for those seeking to defeat the openness presumption for court proceedings that take place during the investigative phase. Clearly the onus must be on the party seeking secrecy. But almost by definition, knowledge is imperfect at the investigative stage. Indeed, it is often the lack of knowledge or intelligence about the facts that compels the desire for secrecy.

In Vancouver Sun the Court appeared to accept the need for an approach to the question of when judicial investigative hearings should be held in camera that acknowledged the problem of an “information deficit” at the investigative stage. The majority held that such hearings should be presumptively public but, applying an adaptable, context sensitive approach, held the test for confidentiality had to be modified to recognize the realities of the procedure in question:

In applying the Dagenais/Mentuck approach to the decision to hold the investigative judicial hearing in camera, judges should expect to be presented with evidence credible on its face of the anticipated risks that an open inquiry would present, including evidence of the information expected to be revealed by the witness. **Even though the evidence may reveal little more than reasonable expectations, this is often all that can be expected at that stage of the process and the presiding judge, applying the Dagenais/Mentuck test in a contextual manner, would be entitled to proceed on the basis of evidence that**

---

satisfies him or her that publicity would unduly impair the proper administration of justice.  

As the court said in another context, such an assessment should be informed by “evidence supplemented by common sense and inferential reasoning.”

III. PRIVACY

I would urge that Tessling is not, as Professor Young argues, a case that sees the Court pay “lip-service” to the sanctity of the home or a case in which the Court has opened the door to constitutionally immunized invasive state use of technology.

Privacy is itself “a broad and somewhat evanescent concept.” The Court, in the context of Charter jurisprudence, has over the last two decades developed a purposive and flexible approach to identifying the privacy interests protected at a constitutional level. As Sopinka J. observed in Evans, “… the Court must inquire into the purposes of s. 8 in determining whether or not a particular form of police conduct constitutes a ‘search’ for constitutional purposes.” The inquiry is contextual and requires a consideration of all the relevant circumstances: “[A] reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances.”

This purposive and flexible approach to constitutional privacy draws heavily upon the analytical framework and rationale put forward

---

21 Supra, note 18, at para. 43 (emphasis added).
in the influential 1972 report, *Privacy and Computers*. This approach to understanding the *constitutional* dimensions of privacy was first articulated on behalf of the Court in *Dyment* by La Forest J., writing:

The first challenge, then, is to find some means of identifying those situations where we should be most alert to privacy considerations. Those who have reflected on the matter have spoken of zones or realms of privacy; see, for example, *Privacy and Computers*, …. The report classifies these claims to privacy as those involving territorial or spatial aspects, those related to the person, and those that arise in the information context.

The same approach to privacy has been accepted by the Ontario Commission on Freedom of Information and Individual Privacy and by the Law Reform Commission of Canada:

The Ontario Commission… has identified three sorts of privacy: territorial, personal and informational. Territorial privacy is privacy in a spatial sense and involves the right to be free from uninvited entries or unwarranted intrusions into one’s home. Privacy of the person protects the dignity of the person and encompasses freedom from physical assault. Privacy in the information context concerns a person’s claim to control over personal information.

These “realms of privacy” identify the different exemplifications of the individual’s interest in being “left alone” by the state (and others). They are inherently valuable in and of themselves as manifestations of what the citizen can expect in a free and democratic society. As the Court said in *Dagg*, “…privacy is grounded on physical and moral au-

---


27 Supra, note 26.

tonomy — the freedom to engage in one’s own thoughts, actions and decisions...” Each kind of privacy contributes to the underlying purposes of privacy, the fostering of individual dignity and autonomy.

Privacy is, as Binnie J. observes, a “protean” concept. In the context of section 8, the best approach is, I would suggest, a purposive one. Why do we wish to protect privacy from the investigative agencies of government? This purposive assessment assists in understanding how privacy should be understood in the context of the legal rights provisions of the Charter. If impugned state action occasions no meaningful harm to those interests then there is no need (at least under section 8) to constrain it.

Protection of privacy is intended to contribute to the well-being of individuals and to society as a whole: total or perfect privacy is only achieved by the recluse who excises himself from all human intercourse to lead a completely atomistic life. A purposive approach to the issue examines privacy in terms of securing or enhancing individual dignity and autonomy within a community that is free and democratic. Our constitutional understanding of privacy must protect values and interests that contribute to how people conceive of themselves and their role in, and relationship to, such a community. Intrusions which involve no meaningful diminution of these underlying values ought not to be classified as searches. To do so would be to erect barriers to investigation just for the sake of creating a barrier, not to serve some other constitutional value.

Expectations of informational privacy are generally the most challenging to identify and quantify. Participation in society necessarily means that information about ourselves flows constantly — our appearance, social interactions, movements, and a variety of transactions with state and private actors who may cooperate with the police mean that a broad range of data is available to those who might be inclined to observe or record them.

29 Dagg v. Canada (Minister of Finance), supra, note 26, at para. 65, per La Forest J. (dissenting in the result, for the majority on this point).
30 Tessling, supra, note 7, at para. 25. For those (like me) who do not find themselves using the term every day, something is protean if it takes on varied shapes, forms, or meanings.
Not every acquisition of information can be characterized as a search. To do so would stifle legitimate police inquiries and create investigative gridlock. In Evans and again in Plant the Court cautioned against taking too broad an approach to what investigative actions might be constitutionally labelled as “searches”:

The word “search” is defined by The Oxford English Dictionary (2nd ed. 1989), vol. XIV as: “1. a. The action or an act of searching; examination or scrutiny for the purpose of finding a person or thing....Also, investigation of a question; effort to ascertain something.” In this sense, every investigatory method used by the police will in some measure constitute a “search”. However, the scope of s. 8 is much narrower than that, and protects individuals only against police conduct which violates a reasonable expectation of privacy. To hold that every police inquiry or question constitutes a search under s. 8 would disregard entirely the public’s interest in law enforcement in favour of an absolute but unrealistic right of privacy of all individuals against any state incursion however moderate.

Not every investigative technique is a search: “it is only where a person’s reasonable expectations of privacy are somehow diminished by an investigatory technique that s. 8 of the Charter comes into play.”

Insofar as expectations of informational privacy are concerned, the Court (taking a purposive approach to a reasonable expectation of informational privacy) has stated that in order to attract constitutional protection information should be at the “biographical core of personal information” which individuals in a free and democratic society would wish to maintain and control from dissemination to the state” and which, if disclosed, would “reveal intimate details” about the “personal lifestyle or private decisions” of the subject.

In Plant, the leading section 8 case on expectations of informational privacy, the Court considered a form of information much like (indeed, if anything, more private than) the information in issue in Tessling. The police obtained access to the electricity consumption records of a par-
ticular home. The records would not, by themselves, disclose how the energy was used, who used it, or what was being done in the house, but could, when considered with other evidence, provide some insights into the goings on within the home. The information was not normally available to the public\(^{37}\) and the police only gained access through a special arrangement with the utility. The accused complained that by discovering this information the state had trenched upon his expectation of informational privacy. The majority in the Supreme Court of Canada disagreed, however, concluding that “electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence”\(^{38}\) and such does not give rise to a reasonable expectation of informational privacy.

Our understanding of privacy in a constitutional context must, of course, be cast in terms of the relationship between the individual and the state, and the legal prohibitions on the state which flow from a conclusion that the activity in question is a “search.” As well, the test should be cast with reference to what citizens in a free and democratic society should be able to expect from their government, rather than what circumstances cause them to expect. In Wong, La Forest J. said:

\(R. \text{ v. Duarte}\) approached the problem of determining whether a person had a reasonable expectation of privacy in given circumstances by attempting to assess whether, by the standards of privacy that persons can expect to enjoy in a free and democratic society, the agents of the state were bound to conform to the requirements of the \textit{Charter} when effecting the intrusion in question. This involves asking whether the persons whose privacy was intruded upon could legitimately claim that in the circumstances it should not have been open to the agents of the state to act as they did without prior judicial authorization. To borrow from Professor Amsterdam’s reflections, ... the adoption of this standard invites the courts to assess whether giving their sanction to the particular form of unauthorized surveillance in question would see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society.\(^{39}\)

\(^{37}\) \textit{R. v. Plant}, \textit{id.}, at para. 44 (though Sopinka J. seemed to take a different view of the evidence).

\(^{38}\) \textit{R. v. Plant}, \textit{id.}, at para. 20.

Put another way:

whether an individual’s privacy interests will attract s. 8 protection depends on whether a “reasonable person would expect that the investigative technique in question so trench on personal privacy that it should only be available with some form of judicial pre-authorization.”

Considering privacy, or expectations of privacy, from a constitutional perspective, one must consider the extent to which — if at all — the questioned government conduct would, if permitted without judicial pre-authorization, undermine the values of personal autonomy that are the underlying purpose of the privacy protection in section 8. I would suggest the following heuristic to assist in assessing whether such privacy is being curtailed by government action:

• Would the unauthorized use of the questioned investigative technique “see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society”?
• Would it inhibit individuals from leading autonomous, meaningful lives independent of government meddling?
• Would it impair the creation or development of networks of individuals in intimate, personal relationships?
• Would it change the way we perceive our ability to participate in personal, family, community or political life?

Any lesser test would radically lower the threshold for the identification of state conduct said to intrude on privacy and effectively place a search label on any investigative actions. Unintrusive state action to acquire even the most mundane data would become a search. It would amount to a trivialization of privacy as a constitutional concept and undermine the public’s perception of the balance between individual protection and the law’s ability to permit the police a reasonable ambit of activity to gather evidence of crime.

In *Tessling* one consideration was the “technological” concern: the fear that permitting the use of FLIR would be seen as a licence to use a range of as yet undreamed of technologies to surveil citizens. No doubt the courts carry a great trust for the future to ensure that approbation of a particular search does not become a licence for later, more intrusive activities. The challenge in the context of investigative techniques which involve the use of a technology is to craft a rule which does not unintentionally invite the use of more advanced and more intrusive versions of the same technology at some future point in time. Clearly this was a concern for the Court of Appeal in *Tessling* and for Scalia J. in *Kyllo*.41

But a concern for the careful development of the law is not a mandate to lose sight of the case that is actually before the Court. The Court’s duty to the future is discharged not by ignoring the relatively mundane issue before it in a particular case (for example, gross measures of waste heat in *Tessling*), but by articulating a rule or test that is substantive rather than mechanical. There is no need to fear an FLIR device or any other similar device simply because it is a “technological” aid, so long as the test used to assess any alleged search is substantive. One can never lose sight of the need to examine whether there exists a reasonable expectation of privacy based on the facts actually before the court: “[T]he consideration of whether an individual has a reasonable expectation of privacy can only be decided within the particular factual context of the surveillance”42 and not based on open-ended ideas about ideal privacy.

*Tessling* is a natural product of the Court’s purposive development of a conception of privacy intended to foster other democratic values while permitting the state a range of investigative action not antagonistic to such values.

It is argued that the police ought not to be able to engage in activities such as using FLIR because they might then be able to use that relatively neutral information, in conjunction with other investigative data, to draw some inference about activities in a house. Such an approach confuses an investigative conclusion with investigative intrusion. Police are expected to investigate and find out what is happening behind doors. Our concern should be with how they do this, not with the conclusions

---


or inferences they are able to justify based on what evidence they gather using otherwise unintrusive techniques.

IV. POLICE CULTURE AND THE DEVELOPMENT OF CONSTITUTIONAL NORMS

I have in the past joined in efforts to encourage the more complete and effective education of police officers and others on the constitutional limits of their powers.43 I also believe strongly that the notion of “institutional bad faith” at the section 24(2) stage is the appropriate way for the courts to integrate the state’s duty to adequately train officers into the constitutional equation.44

But if the courts are to expect that the police will know and obey the law, then there is a concomitant obligation on the courts (and parliament) to make the law more accessible to those charged with its execution. Police disregard for the law may in part be a reaction to the growing perception that the law in this area has become “unknowable.” Search and seizure law is now profoundly complex and subtle. In 1982 the annotated Criminal Code dedicated about seven and one-half pages to the core search provisions. The 2005 edition has more than 70 pages of text in the statutory portion and an additional 11 pages of annotations to section 8.45

The Criminal Code search provisions are textually dense and in places almost unreadable.46 A good first step in improving police obedience of the law would be a thoughtful legislative overhaul of this morass of legislative and judicial authority.47

---

44 The notion of institutional bad faith is the idea that even if an individual officer has done his or her best to obey the law as they understand it (conventional “good faith”).
46 Section 487.015(3) is a good example of the poor drafting endemic in this area. Read literally it authorizes a production order upon a showing of reasonable grounds to believe that there is a suspicion of an offence.
47 This is not first time someone has suggested this indictment of the present regime: R. Pomerance “Criminal Code Search Warrants: A Plea for a New Generic Warrant” in D. Stuart, Towards a Clear and Just Criminal Law (Toronto: Carswell Co., 1999).