**FTR Now**

# The Reasonable Expectation of Privacy: Where Does it End?

**Date:** October 11, 2012

Privacy is an expanding area of law, and it has particular impact on employers. In a recent decision outside of the employment context – *R v. Ward* – the Court of Appeal for Ontario speaks to the scope of an individual's reasonable expectation of privacy.

The decision in *Ward* highlights two points of importance to employers: (1) how organizations (such as employers) that operate information systems should use terms of use to shape an expectation of privacy; and (2) how to persuasively frame arguments related to the expectation of privacy and permissible use and disclosure of information. In this *FTR Now*, we discuss these issues and the implications of the *Ward* decision for employers.

## *WARD*: HOW DO WE DETERMINE THE SCOPE OF THE REASONABLE EXPECTATION OF PRIVACY?

In *Ward*, a child pornography investigation led police to obtain information that pornography had been downloaded from a number of Canadian Internet Protocol (IP) addresses. On the basis of this information, the police, pursuant to an established protocol, requested and obtained information from a Canadian Internet service provider (ISP) that led them to the accused. The accused's defence at trial was that the police violated his section 8 *Charter* rights by engaging in an unreasonable search and seizure: therefore the evidence obtained in that search should be excluded. The trial judge rejected this argument and the accused appealed. The key issue before the Court of Appeal was whether the accused had a reasonable expectation of privacy in these circumstances.

The Court found that there was no reasonable expectation of privacy and no breach of section 8. It commented that, in order to determine whether the accused had a reasonable expectation of privacy, it must first consider whether the accused had a subjective expectation of privacy and, if so, whether that expectation was reasonable in the totality of the circumstances.

In making this determination, the "ultimate question", as stated by Justice Doherty, is whether the personal privacy claim "must, upon a review of the totality of the circumstances, be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society." In *Ward*, the question therefore became whether the "appellant had a reasonable expectation that he could anonymously access the Internet on his computer without the state, with the cooperation of the appellant's ISP, being able to find out what he had accessed."

The Court found the accused's subjective expectation of privacy was not reasonable. It considered a number of circumstances in reaching this conclusion. For example, the Court determined that the police were not seeking broad disclosure of a "roadmap of the appellant's travels on the Internet" but, rather, narrow information capable of putting the accused at a specific place, at a specific time in his Internet travels. The Court also found that the police request, and the ISP's disclosure, were consistent with their rights, obligations and discretion under *PIPEDA* [1] and the *Criminal Code.*

Of particular interest to employers, the Court considered the relationship between the accused and the ISP, as reflected in the ISP's standard form service agreement. The accused had to agree to the ISP's terms in order to use the system. These terms contained an Acceptable Use Policy (the "AUP"), which specifically prohibited (among other things) the uploading or downloading of child pornography, or any activity that would constitute a criminal offence. The agreement made clear that the ISP would offer full co-operation with law enforcement agencies. The agreement also stated that by entering into it, customers consented to the collection, use and disclosure of their personal information, as noted in the ISP's policies and

practices, unless the customer specifically withdrew that consent by completing an “opt-out form” – which the accused did not do.

The Court concluded that these contractual terms reinforced the view that a reasonable and informed person would not expect that society should recognize that the appellant had a reasonable expectation of privacy in respect of the subscriber information held by the ISP.

The focus on contracts and policies that define the relationship between the parties echoes comments made in the Court of Appeal’s recent privacy-related decision in *R. v. Cole*. [2] In *Cole* the main issue was whether a teacher had a reasonable expectation of privacy in the contents of his work computer. In the circumstances, the Court recognized an expectation of privacy.

However, it is noteworthy that the Court in *Cole* demonstrated a willingness to allow employers to govern system information through properly drafted workplace policies and procedures. For example, that Court noted that “[t]here was no clear and unambiguous policy to monitor, search or police the teachers’ use of their laptops,” implying that the presence of such a policy could have affected the analysis. The absence of a policy in *Cole* is in sharp contrast to the specific terms in the ISP’s service agreement in *Ward*. Likewise, the Court in *Cole* noted that the school board had given “explicit permission to use the laptops for personal use and permission to take the computers home on evenings, weekends and summer vacation.” Finally, that Court also noted that the teacher’s reasonable expectation of privacy was “modified” to the extent he knew that the school board’s technician “could and would access the laptop as part of his role in maintaining the technical integrity of the school’s information network.”

Read together, the decisions in *Ward* and *Cole* provide insight into the types of policy terms that the Court will consider to be persuasive in an analysis of an employee’s reasonable expectation of privacy.

## IT’S ABOUT “VALUES”

In *Ward*, the Court explicitly noted that the reasonable expectation of privacy is a “normative” rather than a “descriptive” standard. In other words, in deciding that an individual has a reasonable expectation of privacy, a court is making a value judgment more than a finding of fact in the traditional sense. When a court accepts that a person has a reasonable expectation of privacy, it is, in reality, declaring that “the values underlying contemporary Canadian society” are more in line with protecting privacy in that instance than with allowing the state to interfere with that privacy.

To this end, the Court in *Ward* contrasted the ISP’s “pure self interest” with the ISP’s other interests described in value-laden terms such as “preventing the criminal misuse of its services” and demonstrating “civic engagement” through a corporate commitment to assist law enforcement. The Court directed that the ISP’s interests must be taken into account in determining whether the accused had a reasonable expectation of privacy in the information held by that ISP.

The Court found that a customer’s reasonable expectation of privacy was circumscribed by the ISP’s discretion to disclose where it was both reasonable and within its legal rights to do so. Given the nature of the disclosure requested and of the crimes being investigated, the Court concluded that a reasonable informed person would accept that it was reasonable for the ISP to make the requested disclosure. Since disclosure was reasonable in the circumstances, the accused’s privacy claim could not be objectively reasonable.

## WHAT CAN WE TAKE FROM *WARD*?

The implications for employers that flow from this case are two-fold.

First, *Ward* demonstrates that the analysis of a person’s reasonable expectation of privacy will include a consideration of the relationship between the parties. The way the relationship is defined, documented and understood by the parties will be an

important factor in considering whether the individual has a reasonable expectation of privacy and whether disclosure or use of information is reasonable.

In *Ward*, this relationship was defined by the service agreement between the parties. In an employment relationship, by analogy, the relationship is defined by the employment contract and the various policies governing the workplace. Since the relationship between the parties matters, employers would do well to define it carefully, bearing in mind the terms discussed in *Ward* and *Cole.* This could include a policy on monitoring, searching and policing computer use, a code of use, or an outline of the potential situations in which information might be disclosed or where the contract may be voided. The important message is to think about the risks that your organization is trying to guard against and the goals it is trying to accomplish, and to draft your relationship documents to meet your objectives.

Second, where looking to defend an alleged invasion of "privacy", *Ward* demonstrates that a party is more likely to succeed if it can frame the legitimate interests it is seeking to protect as being in line with "the values underlying contemporary Canadian society." Where an employer can persuasively describe what it is trying to accomplish in broad, societal terms (*e.g.* similar to the ISP's "corporate commitment to assist law enforcement" in *Ward*) courts will be more likely to accept disclosure (or use) as reasonable.

Additionally, it can help if the employer is able to link its legitimate interests to an interest or value that is statutorily expressed. For example, in *Ward* the Court found that the ISP's legitimate interest in disclosure "[found] expression in the terms of *PIPEDA*." Such a link may assist in demonstrating that the interest is in fact legitimate and consistent with the values underlying contemporary Canadian society.

## CONCLUSION

Privacy law is particularly driven by value judgments – both in terms of defining a "zone of privacy" and in permitting reasonable incursions. The legal implications of these value judgments are only beginning to take shape. The Court's decision in *Ward* provides a further piece of the puzzle in sorting through the factors that will define the scope of an individual's reasonable expectation of privacy.

To sort through these "puzzle pieces" or for any information related to the issues discussed in this *FTR Now*, please contact Frank Cesario at 416.864.7355, Jacqueline J. Luksha at 416.864.7531 or your regular Hicks Morley lawyer.

---

**[1]** *Personal Information Protection Electronic Documents Act*, S.C. 2000, c. 5.

**[2]** An appeal in *Cole* was recently argued before the Supreme Court of Canada, and a decision is pending.