R. v. Cole and The Diminished Right to Privacy

Lessons for Employees & Employers

OVERHOLT LAW
Trusted Advisors

Canadian Bar Association (BC Branch)
Employment Law Section Meeting
March 25, 2013

Carman J. Overholt, Q.C.

Preston Parsons

600 – 889 West Pender Street
Vancouver, BC V6C 3B2

M: 604.568.5464

Introduction

OVERHOLT LAW
Trusted Advisors

- In a relatively short time, privacy has become a major area of legal evolution
- The impact of the multitude of technology and its continued advancement creates challenges in all areas of society, including in the context of employment relationships
- Blurring work and personal time as a result of growing connectivity through that technology continues to raise issues for employees and employers
- The Boundaries are not clear

Outline

OVERHOLT LAW
Trusted Advisors

1. Review of *R. v. Cole* up to SCC decision
2. Subsequent and related cases
3. Issues and Lessons for Employees
4. Issues and Lessons for Employers

OVERHOLT LAW
Trusted Advisors

1. *R. v. Cole*

R. v. Cole – The Facts

OVERHOLT LAW
Trusted Advisors

- Cole was a teacher given exclusive use of a work-issued laptop which he secured with a password
- Permitted some incidental personal use and could take the laptop home on weekends, on vacation, and summer break
- Cole also had administrative responsibilities to police use of school computers by students and staff and regularly did so
- Some school policies were in place regarding technology use
- A school technician who also had administrative responsibilities like Cole, found inappropriate material on Cole's computer regarding a student

Trial Judgment – Ontario Court of Justice

OVERHOLT LAW
Trusted Advisors

- Held: Cole had a subjective and objective expectation of privacy and the evidence must be excluded under s. 24(2)
  - Note: s. 24(2) analysis was done before the SCC decision in *R. v. Grant*, 2009 SCC 32

Appeal to Ontario Superior Court of Justice

OVERHOLT LAW
Trusted Advisors

- The primary issue on appeal was whether the trial judge had erred in determining that Cole had a reasonable expectation of privacy in the contents of the laptop's hard drive

- Held: While Cole may have had a subjective expectation of privacy, that expectation was not objectively reasonable and the evidence was admitted

Appeal to Ontario Court of Appeal

OVERHOLT LAW
Trusted Advisors

- The Court of Appeal found differently from the Superior Court, primarily due to its interpretation of the school policies
- Held:
  - Cole had a “modified” reasonable expectation of privacy
  - He had no expectation of privacy with respect to access to his hard drive by the technician for the limited purpose of maintaining the integrity of the school’s information network and the laptop
  - The technician was acting within this limited purpose when the material was discovered and so Cole’s modified privacy interest was not violated

Supreme Court of Canada

OVERHOLT LAW
Trusted Advisors

- The SCC emphasized that people's computer use leaves a highly sensitive information trail
  - Computers that are reasonably used for personal purposes – whether found in the workplace or the home – contain information that is meaningful, intimate, and touching on the user's biographical core (para 1)
  - Computers that are used for personal purposes, regardless of where they are found or to whom they belong, "contain the details of our financial, medical, and personal situations" (*Morelli*, at para. 105). This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices "reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet" (*ibid*). (para 46)

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

- Workplace policies & ownership of property are not determinative factors of employees' privacy but form part of the *context* to be examined with workplace practices and customs:
  - While workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the expectation entirely: The nature of the information at stake exposes the likes, interests, thoughts, activities, ideas, and searches for information of the individual user (para 3)
  - These "operational realities" may *diminish* employees' expectation of privacy however (para 52)

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

- The determination of whether Cole had a reasonable expectation of privacy depends on the "totality of the circumstances" – *R. v. Edwards*, [1996] 1 S.C.R. 128, at para 45 – including:
  1. an examination of the subject matter of the alleged search;
  2. a determination as to whether the claimant had a direct interest in the subject matter;
  3. an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and
  4. an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

1. Examination of the Subject Matter:

   The subject matter in this case is the *informational content* of the laptop's hard drive, its mirror image, and the internet files, not the devices themselves

2. Did Cole have a direct interest in the Subject Matter?

   Yes. This can be readily inferred from his use of the laptop to browse the Internet and to store personal information on the hard drive

3. Subjective expectation of privacy?

   Also readily inferred on the same basis

4. Objectively reasonable?

   Bulk of the SCC's analysis was here

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

4. Objectively reasonable?
   - The closer the subject matter of the alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy (para 46)
   - The private information in Cole falls at the very heart of the "biographical core" (para 48)

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

4. Objectively reasonable?
   - Balancing the totality of the circumstances:

Factors for privacy	Factors against
1) Teachers had exclusive use of their laptops and used them on weekends, vacations, and at home	1) Laptop owned by school & used for Cole's employment, including in the classroom
2) Both written policy and actual practice permitted Cole to use his work-issued laptop for personal reasons	2) Server, network & data owned by school
3) Password protected	3) The policies in place weren't perfect, but they were brought to the attention of teachers annually, were to apply even if they did not expressly refer to teachers, and were put on notice that privacy teachers might expect is limited by the operational realities.
4) The close relation between the subject matter and Cole's biographical core	4) Given that others monitored the network, technological reality deprived Cole of exclusive control over and access to the personal information he recorded on it, irrespective of his password.

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

- Held:
  - Cole had a subjective and objective reasonable expectation of privacy in the laptop
  - This expectation was *diminished* in comparison to the finding in *R. v. Morelli,* 2010 SCC 8… that Canadians may reasonably expect privacy in the information contained on their own *personal* computers
  - However, the same applies to information on *work* computers, at least where personal use is permitted or reasonably expected
  - A diminished expectation of privacy is nonetheless, an expectation of privacy

Supreme Court of Canada – cont'd

OVERHOLT LAW
Trusted Advisors

- Comment: What they declined to say
  - "… I leave for another day the finer points of an employer's right to monitor computers issued to employees." (para 60)
- One needs to be aware of the applicable privacy legislation and case law that pertains to them as an employer and how this may impact their ability to monitor, collect, use, and disclose information pertaining to employees as outlined in those acts

OVERHOLT LAW
Trusted Advisors

2. Subsequent and related cases

Subsequent cases

OVERHOLT LAW
Trusted Advisors

- Though *Cole* has been cited several times, it is frequently in contexts inapplicable to the employment context
- There is one case which is very similar to *Cole* however and which mirrors the reasoning and analysis in *Cole*: *R. v. McNeice*, 2013 BCCA 98

R. v. McNeice, 2013 BCCA 98

OVERHOLT LAW
Trusted Advisors

- Facts:
  - McNeice was a teacher much like Cole and had a work issued laptop for his exclusive use much like Cole did
  - McNeice was not prohibited by any policy from using the Work Laptop for personal purposes
  - During an investigation, police found child porn on McNeice's home desktop and asked his employer, the Fort Nelson School District, for McNeice's school laptop ("Work Laptop") so they could search it as well
  - The police searched the Work Laptop and found child porn in the temporary internet files. The files had been deleted from the laptop, but the police were able to retrieve the files using special software

R. v. McNeice, 2013 BCCA 98 – cont'd

OVERHOLT LAW
Trusted Advisors

- Trial decision:
  - McNeice had no subjective expectation of privacy and even if he did, it would not have been objectively reasonable
  - Some facts were different from the facts of *Cole* which had released its Ontario High Court decision at the time
  - With regard to the deletion of the temporary internet files, the trial judge found that the deletion constituted an abandonment of any expectation of privacy given the facts above and ruled that the evidence was admissible

R. v. McNeice, 2013 BCCA 98 – cont'd

OVERHOLT LAW
Trusted Advisors

- Court of Appeal Held that:
  - McNeice had a subjective expectation of privacy that was objectively reasonable
  - Deleting the files was not "abandonment":
    - "In my view, deletion of the files is more consistent with an intention on the part of the user to destroy the information, or at least to conceal it from view by anyone else, including himself" (para 52);
    - "The act of deleting the files in itself can be seen as a very deliberate step towards preventing others from access to 'personal files'" (para 54).
  - Deleting the files is similar to using a password.
  - The absence of a policy prohibiting personal use on the Work Laptop increased the expectation of privacy

Non-technology case

OVERHOLT LAW
Trusted Advisors

- A broader way to apply *Cole*? See *Communications, Energy and Paperworkers Union, Local 707 v. Suncor Energy Inc.,* 2012 ABCA 307
  - Appeal from an injunction against Suncor from implementing a new random drug and alcohol testing policy
  - During the balance of convenience and irreparable harm components, it was noted that Suncor's argument of minimal intrusion was related to the "reasonable expectation" of workers privacy on the worksite, citing *Cole*. (para 7)
  - Conversely, the union argued that there was a 100% probability of impact on workers privacy in the personal, physical, and informational sense (para 35) versus the low probability that the new policy would actually capture any enhance workplace safety as Suncor argued.

Related cases

OVERHOLT LAW
Trusted Advisors

- Though not citing *Cole*, a couple recent privacy decisions are worth noting
- It's also important to be aware of provincial privacy legislation, BC's *Privacy Act,* RSBC 1996, c 373 and of developments in the common law of privacy
- The OIPC standard for monitoring employees
- Competing interests?

OIPC AB - Calgary Police Service Order F2012-07

OVERHOLT LAW
Trusted Advisors

- In both *McNeice* and *Cole*, the Courts ultimately found that the employer's actions were lawful
- This Calgary Police Service ("CPS") case however shows an example of where the employer's investigation through IT was not lawful
- CPS received complaints about a civilian employee ("CE") with regard to inappropriate sexual conduct and her bragging about it

OIPC AB - Calgary Police Service Order F2012-07

OVERHOLT LAW
Trusted Advisors

- The CPS began to monitor CE's computer activities and reviewed her past work e-mail activity.
- IT Security Manager found a personal e-mail that the CE sent to a family member outside the office. The contents of the e-mail included her login and password for her personal e-mail account.
- The IT Security Manager then used this to access the CE's personal e-mail, where he found photos of a sexual nature taken on CPS premises.
- The CE's job was terminated and the CPS used the photos throughout the CE's grievance process, and the CE complained to the OIPC.

OIPC AB - Calgary Police Service Order F2012-07

OVERHOLT LAW
Trusted Advisors

- Issue:
  - whether the CPS collected, used, and/or disclosed the CE's personal information in contravention of Part 2 of the *Freedom of Information and Privacy Act*, R.S.A. 2000, c. F-25

OIPC AB - Calgary Police Service Order F2012-07

OVERHOLT LAW
Trusted Advisors

- Held:
  - Collecting the login & password was in the course of reviewing the work e-mail and was okay.
  - Using that information to access the CE's personal account was not.
  - The "exceptionally invasive" search was patently unreasonable in the circumstances and would not even be authorized on a legitimate search for data leakage (which was found not to be the case here) unless the employer had *cause* for such a search.
  - As the photos were collected as a result of unauthorized use, the collection of the photos and subsequent use was not justifiable.

OIPC BC – UBC
Order F13-04, 2013 BCIPC No. 4 (CanLII)

OVERHOLT LAW
Trusted Advisors

- UBC has GPS installed in Campus Security patrol vehicles
- Issue was whether UBC was collecting and using "personal information" in contravention of s. 26, 27, and 32 of *FIPPA*
- Decision:
  - The information that the GPS collects with regard to the vehicles' location, movement, speed, and ignition status is personal information here as it can be related to an identifiable individual in order that UBC accomplish its purposes for having the GPS
  - UBC was authorized to collect and use that information, including for employee performance reasons

OIPC BC – UBC
Order F13-04, 2013 BCIPC No. 4 (CanLII)

OVERHOLT LAW
Trusted Advisors

- Comments: Food for thought
  - "There is, to be sure, a difference between routine monitoring of employee actions through GPS and cause-based, after-the-fact, resort to GPS information, yet UBC's policy fails to distinguish between the two." (para 67)
  - "…it is not appropriate to interpret what is 'personal information' under FIPPA by applying a reasonable expectation of privacy test." (para 40)

Significant common law development: *Jones v. Tsige,* 2012 ONCA 32

OVERHOLT LAW
Trusted Advisors

- A bank employee repeatedly accessed banking records of her husband's ex-wife (at least 174 times)
- New tort of "intrusion upon seclusion" recognized at common law
- Elements:
    1. Defendant's conduct must be intentional, including reckless;
    2. Defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns;
    3. A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.
- Proof of damages is not a required element

Privacy Act, RSBC 1996, c 373

OVERHOLT LAW
Trusted Advisors

- BC is one of four provinces in Canada with provincial privacy acts.
- The statutory cause of action in BC is similar to that recognized in *Jones v. Tsige*, 2012 ONCA 32, and is found in s. 1.
    1. Defendant's conduct must be wilful;
    2. Defendant's conduct must be without claim of right; and
    3. The nature and degree of privacy to which the plaintiff is entitled is what is reasonable in the circumstances, giving due regard to the lawful interests of others.
- Like the common law tort of intrusion upon seclusion, no proof of damage is required.

OIPC – Employee monitoring

OVERHOLT LAW
Trusted Advisors

- Though the SCC in *Cole* declined to comment specifically on "the finer points" of an employer's right to monitor employees' computers, there is a four-part test to guide private employers already:
  1. Is the measure demonstrably necessary to meet a specific need?
  2. Is it likely to be effective in meeting that need?
  3. Is the loss of privacy proportional to the benefit gained?
  4. Is there a less privacy-intrusive way of achieving the same end?
- See *Schindler Elevator Corporation (Re),* 2012 BCIPC 25 (CanLII) and *Eastmond v. Privacy Commissioner of Canada,* 2004 FC 854 (CanLII).

Competing interests – possible legislative change?

OVERHOLT LAW
Trusted Advisors

- In *United Food and Commercial Workers, Local 401 v Alberta (Attorney General),* 2012 ABCA 130, the Court found significant portions of Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5.
  - A union took video and still photos of workers who were near or crossed the picket line and using those workers' photos on posters at the picket-line as well as newsletters and leaflets.
  - Ultimately, the union argued that *PIPA* infringed its freedom of expression under Charter s. 2(b) and the Court agreed.

Competing interests – possible legislative change?

OVERHOLT LAW
Trusted Advisors

- SCC hearing is set for June 2013
- If upheld, legislative changes are likely to follow in other provinces besides just Alberta

OVERHOLT LAW
Trusted Advisors

3. Issues and Lessons for Employees

Issues & Lessons for Employees

OVERHOLT LAW
Trusted Advisors

1. How am I using the devices I have in connection to the workplace?
2. What information should I not retrieve/access on my work devices if I want to ensure that it stays private?
3. What is the Employer's Policy?

<u>Key Take-away</u>

If you would be embarrassed showing the material to your grandmother or the police, don't view it on your work technology!

OVERHOLT LAW
Trusted Advisors

3. Issues and Lessons for Employers

Issues for Employers

OVERHOLT LAW
Trusted Advisors

- What law applies?
  - *Charter*? Provincial Privacy Acts?
  - *FIPPA (BC), PIPA (BC), PIPEDA (Fed)?*
- Who owns the technology the employee is using for work?
  - An employee will be afforded a greater expectation of privacy with regard to an employee owned device. If the employer owns it, it does not automatically follow that the employee has no expectation of privacy
- What workplace policies are in place?
  - Are they clear? Are the consequences of a breach or repeated breaches clear?
  - Have they been specifically brought to all employees' attention?
- Workplace practices:
  - Are you enforcing the policies? Could an employee later argue that breaches of the policy are condoned?

Lessons for Employers

OVERHOLT LAW
Trusted Advisors

- Employees may reasonably expect privacy in the information on work computers (which can touch on their biographical core and therefore must be treated sensitively) where personal use is *permitted or reasonably expected*
  - In today's age, entirely eliminating all expectation of personal use and privacy, and attempting to enforce it, is probably unreasonable
  - Employers should only monitor personal employee communications and data in exceptional circumstances

Lessons for Employers – cont'd

OVERHOLT LAW
Trusted Advisors

- To *diminish* the expectation, *draft* and *enforce* clear policies regarding technology use for employee phones, computers, tablets, and so forth:

  1. Acceptable and Unacceptable Technology Use, Internet Use, Social Media Use, and Privacy policies should be drafted so that each policy compliments the next, is clear, and is easy for all employees to understand

Lessons for Employers – cont'd

OVERHOLT LAW
Trusted Advisors

2. Make it clear that:
   a) the employer owns the content on its technology and owns work related content kept on employee personal devices;
   b) the employer has the right to monitor its work devices, why it may do so, and in what (reasonable) circumstances it will do so and that no notice need be provided before so doing;
   c) the employer may require the employee to return or exchange devices periodically and;
   d) employees should not expect privacy in information on work servers, data, and work technology, and that data in these areas may be deleted at any time and employees who choose to store personal data risk losing it

Lessons for Employers – cont'd

OVERHOLT LAW
Trusted Advisors

3. Set out clearly what is acceptable use and what is unacceptable (give examples of unacceptable use)

4. Set out clearly the consequences for breaching the policies.

5. Regularly remind employees and consider having them sign off on the policies at regular intervals

6. Obtain express consent from employees to collect, use and disclose personal information transmitted or stored and for what purposes this may occur

Lessons for Employers – cont'd

OVERHOLT LAW
Trusted Advisors

- Password Protection:
  - It is good practice to require employees to secure work technology and personal technology which may have work information on it with a password
  - Consider requiring the employee to give their password on work-owned technology to someone at the employer's office who could access the information on the device if necessary (more important where the data on the device cannot be accessed remotely)

Future Issues?

OVERHOLT LAW
Trusted Advisors

- Make your policies prospective where possible, and update them as technology evolves
- Google Glass

OVERHOLT LAW
Trusted Advisors

Questions?

Thank you for attending

600- 889 West Pender Street
Vancouver, BC V6C 3B2

Carman J. Overholt, Q.C

Direct: (604) 676-4196
carman@overholtlawyers.com

Preston Parsons

Direct: (604) 676-4197
preston@overholtlawyers.com