Employee Privacy And Disciplinary Actions

Employers should have strong privacy management programs in place and should consider potential privacy issues when making disciplinary decisions.

Generally, employees have a reasonable expectation of privacy on workplace computers and other devices, particularly where personal use is permitted or at least reasonably expected (which is most cases). While it may be possible for an employer's policies and practices to diminish the expectation of privacy in the workplace, the expectation may not be completely removed.

A recent Canadian labour arbitration decision, *Canadian Broadcasting Corporation v Canadian Media Guild,* highlights how employees may have a reasonable expectation of privacy even on shared computers. The decision also emphasizes the importance of taking into account employee privacy rights when carrying out disciplinary action.

Case Highlights – Expectation of Privacy on Shared Laptop

The arbitrator ruled that the employer, CBC, acted improperly in terminating the employment of a journalist after he set off "a chain of events" with his tweet calling comments regarding Remembrance Day poppies xenophobic and racist.

CBC believed the tweet violated a portion of its specific to the personal use of social media. The employer asked the employee to remove the tweet for violating the policy, and he obliged. Before the tweet was removed, a Toronto Sun columnist quoted the employee, identifying him as a CBC employee. Following internal meetings, the employee contacted other media outlets telling them about the tweet's deletion.

CBC terminated the employee's employment for contacting external outlets about the order to delete the tweet, for making disparaging comments about CBC management and policies to parties outside of CBC, and using a homophobic slur on WhatsApp (where his profile identified him as a CBC employee).

Prior to the termination, the employee left a shared laptop on his desk in the newsroom without logging out of Twitter and WhatsApp. Another employee retrieved the laptop and notified a manager that he had located unethical material on it, including the communication with other media outlets.

The termination of employment was grieved. The arbitrator applied the test from *R v Cole* to determine whether a reasonable expectation of privacy existed. The test involves exploring the totality of the circumstances, including:

1. the subject matter of the search;
2. whether the claimant had a direct interest in the subject matter;
3. whether the claimant had a subject expectation of privacy; and
4. an assessment of whether the subjective expectation of privacy was objectively reasonable.

The arbitrator concluded that the employee had a reasonable expectation of privacy in his messages on the shared laptop and reasonably believed a co-worker would log him out of his personal accounts and not review his private messages.

The arbitrator acknowledged that there may be situations where the misconduct is sufficiently serious to warrant the search of private messages such as if involving criminal actions, but this was not such a circumstance.

Consequently, the arbitrator determined that the co-worker and employer violated the employee's privacy rights, and that the violation tainted the entire process.

As such, the arbitrator concluded that the employee had a reasonable expectation that his messages, even though they were on a shared company laptop, were private and that they should not have been used by management in the decision to terminate his employment. The arbitrator further concluded that the employee should be reinstated and that he was entitled to damages for the violation of his privacy rights.

Key Takeaways for Employers

This decision serves as a reminder to employers that searches of workplace computers and devices must appropriately take into account the privacy interests of employees on those devices.

Employers need to be mindful that, if an employee's privacy rights are not appropriately taken into account when taking disciplinary action such as terminating an employee, the discipline may be overturned (in this case, the employee was not only reinstated but the employer may also be liable for damages).

To mitigate the risk of having disciplinary decisions overturned due to privacy violations, employers should develop and implement a strong privacy management program including appropriate policies that clarify the permitted use of the employer's technology.

Although policies and employer actions can reduce the expectation of privacy, they will not eliminate it. Thus, employers need to take privacy into account when planning and implementing disciplinary decisions. Even where an employer has legitimate concerns, it must consider the employee's privacy rights and investigate the concerns in the least intrusive way possible.

Here are some key tips for employers when it comes to addressing employees' privacy expectations on workplace computers and devices:

1. Have clear policies and expectations in place.
2. Implement policies appropriately such as by clearly communicating those policies and expectations to employees, having employees sign clear acknowledgements and providing appropriate training on and regularly reminding employees of policies and expectations.
3. Regularly review and update policies and expectations to reflect changes in legal requirements and best practices.
4. Carefully plan and execute searches of workplace computers and devices – especially when considering disciplinary action – and carefully assess the resulting disciplinary actions on a case-by-case basis.
5. Review searches and discipline with internal or external legal counsel where appropriate.

by Brent Matkowski , Kristl Kriel and Nicole Graham
MLT Aikins LLP