CORPORATE TECHNOLOGY POLICIES: AN INTRODUCTION TO ISSUES AND TRENDS

VirtualRaven's advice on corporate information technology policies can be summarized in a tweet: "If your company uses e-mail, you have to have a written e-mail policy. To not have one opens you up to all manner of headaches" (Tweeted February 2nd).

Corporate technology use has come to mean much more than e-mail access during business hours and, like VirtualRaven, most legal and human relations experts now recommend that companies have appropriate corporate technology policies. Unlike VirtualRaven, however, the advice of these experts, who must consider privacy legislation, proprietary works management, and the more abstract debate over the merging of personal and professional lives, is rarely able to fit into a 140 character tweet.

As of June 2009, there were 1.67 billion people using the Internet worldwide.¹ The Internet and other forms of technology have caused the definition of "workplace" to be revolutionized. Blackberries, i-Phones, and remote access applications have expanded the workplace beyond the building and across international boundaries. Alongside the redefinition of a technology driven workplace is the need for a company to develop a comprehensive suite of corporate technology policies.

Well established and consistently administered corporate policies in general are key to avoiding employment related litigation. More often than not, workplace conflict, and subsequent litigation, arises due to a misunderstanding between individuals. In the absence of clearly defined corporate expectations, employees are left to make their own assumptions and set their own expectations, and conflict arises when these are challenged. Corporate policies help prevent issues by clearly establishing the corporate organizational structure and expectations.²

---

¹ Online: Wikianswers
<http://wiki.answers.com/Q/How_many_Internet_users_are_there_worldwide>.
The administration of corporate policies are as equally important as the creation of such policies. By applying policies consistently to all employees, a corporation can foster fairness and equality, which in turn helps build positive employment relations. This consequently reduces litigation regarding human rights and employment issues.3

The proliferation of technology in the workplace has substantially escalated the need for technology policies in particular. Reliance on computers, the Internet, and smart phones has introduced new workplace challenges that require appropriate corporate regulation. Failure to properly deal with technology related issues costs corporations in lost productivity, employment unrest and reputational damage. Some of the most significant concerns include e-harassment, misuse of corporate technology, information security, protection of corporate reputation and resulting corporate legal liability. Each of these is briefly canvassed below.

**E-Harassment**

The expansion of technology in the work environment has spawned new modes of harassment. Harassment now comes in a variety of quick and easily accessible electronic forms of e-mails, text messages, social networking sites, and the like, and has facilitated more creative forms of harassment. Xerox, for example, had to defend a lawsuit from two employees after their heads were photoshopped onto the bodies of a Playboy poster, which was circulated throughout the office.4

The [Canadian Labour Code]5 establishes that an employee has a right to work in an environment free from harassment and that employers must take positive action in order to prevent harassment. This is becoming increasingly difficult given the ease and speed of e-harassment, which is becoming the predominant form of harassment in the workplace. A survey of 1,072 UK workers found that one in five had been bullied at work by e-mail and 1 in 16 had been bullied via text message.6 This same survey estimated that workplace bullying cost UK employers more than £2 billion a year in sick pay, staff turnover and lost production. According to research done by International Data Corporation, 27% of Fortune 500 organizations have defended themselves against claims of sexual harassment stemming from inappropriate e-mail.7

The issue of e-harassment was raised in *Russell v. Nova Scotia Power Inc.*8, where an employer used e-mail to embarrass an employee who had previously been dismissed. After the employee was terminated, the employer sent out a mass e-mail to the department stating that the employee was dismissed for incompetence. While the court held that an e-mail informing the department that the

---

3 Ibid.
4 Sacha C. Fraser, "The Evolving Workplace: A Practical Guide" (PowerPoint presented at the Employment in the Information Age Conference, January 29th and 30th 2001) [unpublished].
7 Online: Staff Monitoring Solutions [http://www.staffmonitoring.com/P32/stats.htm].
employee was no longer employed would have been appropriate, the comment that the employee was dismissed for incompetence was unfounded and made for no other purpose than to embarrass. The court awarded $40,000 in punitive damages against the employer. 9

The Journal of Applied Management and Entrepreneurship studied employee perceptions concerning e-harassment in their workplace. The majority of participants felt their workplaces had adequate harassment policies, yet few knew if those policies applied to e-mail and Internet. As noted above, employers have an obligation to provide a workplace free of harassment, so it is important that such policies are not only created, but also properly implemented. 10

Misuse of Corporate Resources

The misuse of the Internet at work has become so prevalent that it has been given a name - cyberslacking. Canadian companies are not only losing productivity due to this on-the-clock web surfing, but may be paying employees extra for cyberslacking. In one notable case, a unionized employer in Quebec discovered that one employee browsed the Internet for 328 hours in a five month period and over the same time frame claimed 467 hours of overtime pay. 11

There is no denying that the misuse of the Internet at work is costing Canadian companies money. Estimates suggest that Internet misuse costs Canadian businesses more than $16 billion in lost productivity per year. In the United States, this figure is estimated to be over $80 billion. 12 Employees engaging in cyberslacking spend company time browsing anything and everything – from the rather innocent online shopping, travel booking and social networking to the more inappropriate browsing of pornographic websites. 13

The impact of social networking sites on corporations is a rather recent development. Over the previous decade, there has been an unbelievable surge in social networking popularity. Facebook, for example, was launched in 2004 and by the end of the year had 1 million users. By the end of 2007, this number reached 50 million and at the close of 2010 Facebook had an astonishing 500 million

users. This phenomenon has two major implications for corporations: 1) the misuse of company time; and 2) potential damage to corporate reputation and data loss from employee postings on such sites, which will be discussed below.

The overwhelming use of social networking sites is not having an entirely negative impact on corporations. Many corporations are realizing the marketing potential that exists in these online sites. A Twitter and Facebook presence reportedly generated $9 million for Dell Computers in 2009. The key to benefit from this potential is to have a carefully drafted policy dealing with the appropriate use of such sites, without necessarily banning the use altogether.

A vice-president for Bajai Inc., an Ottawa firm that sells online activity monitoring software, suggests that many organizations are no longer concerned with how much time an employee spends on Facebook, but are concerned with reducing access to pornography, hate material and gambling to reduce the Corporation's liability exposure. Unlike social networking sites, there is no potentially positive corporate impact from employee use of these websites.

After monitoring 10,000 employees' Internet use, the Canadian Department of Fisheries and Oceans discovered that, on average, each employee visited seven pornographic sites per day. Xerox fired over forty employees for spending up to 8 hours per day on pornographic web sites. The downloading of pornographic videos was so prevalent that it actually clogged Xerox's computer network and prevented legitimate work e-mail from being sent and received. Corporate technology policies can help effectively deal with, and hopefully prevent, such behaviours.

### Ensuring Information Security

It seems no industry is immune from the threat of security breaches that have recently inundated the headlines. Government, financial services, and even online dating sites have all been subject to breaches in security. Protecting the security of information is multifaceted and requires a tool kit of comprehensive policies and practices in the following areas:

- Physical Security
- Network/Software Security
- Authentication/Password Protection
- Encryption
- Acceptable Use Policy
- Security Awareness

---

16 Supra, note 13.
The Rotman School of Management and TELUS Corp. perform an annual joint study on Canadian technology security practices. The study looks at organizations with more than 100 employees. Its 2009 findings confirmed the growing threat of security breaches, and a significant increase (97%) in the costs of handling them. However, a portion of the increase in these costs was found to be attributable to a greater investment in protection technologies during 2009.

The average number of breaches within the organizations surveyed has been increasing every year since the first study in 2008. In that year, there was an average of 3.0 security breaches per organization. This number increased to 11.3 in 2009 and increased again by 29% in 2010, largely as a result of increases in government security breaches. Government entities reported experiencing an average of 22.4 breaches in 2010, more than twice the number in private sector organizations.

As the survey indicates, government security breaches have been a common occurrence recently. A few examples include:

- **Passport Canada:** In 2007, a security gap in Passport Canada's online passport application system was detected. The gap allowed anyone to access personal information of applicants by merely changing a few numbers in the URL of their own online application. The breach allowed access to driver licence numbers, health card numbers, social insurance numbers, home addresses and telephone numbers.

- **Statistics Canada:** Statistics Canada has experienced numerous security breaches over the past 5 years. For example, in October 2010, a Purolator envelope containing 11 unencrypted, non-password-protected CDs for the Vital Statistics Program in Alberta went missing. The CDs contained more than 21,000 electronic images of confidential information about individual birth, death, stillbirth and marriage registrations. It was found on November 30, 2010 locked in a rarely-used filing cabinet. In 2008, Surrey RCMP officers recovered completed 2006 census questionnaires from a private residence during a bust of a major identity theft ring.

- **Alberta Health:** In December of 2010, seven laptops and digital devices were stolen that contained unencrypted health, employee and financial information in Alberta. One of the laptops contained medical charts belonging to 2,700 paediatric patients.

---

19 Online: Rotman’s School of Management at the University of Toronto <http://www.rotman.utoronto.ca/securitystudy/Rotman-TELUS-2010_executive-summary.pdf>.
gastroenterology patients participating in a study at the University of Alberta.\textsuperscript{22} This was not the first time that Alberta Health experienced a security breach. In 2009, laptops containing the health information of more than 300,000 patients was reported stolen from Alberta Health Services.\textsuperscript{23}

While government entities have experienced a greater number of breaches than private industries, security breaches pose a costly threat to private business. In 2007, the Canadian Imperial Bank of Commerce announced that it lost a file containing personal details from almost half a million client accounts of Talvest Mutual Funds, a subsidiary of CIBC Asset Management. The file reportedly went missing when being transported from Montreal to Toronto. The confidential information included all the necessities for identity theft - client names and addresses, birth dates, bank account numbers and social insurance numbers. CIBC responded to this situation by providing a free credit-monitoring service to catch potentially fraudulent transactions and offering to compensate clients for any monetary loss that may arise from the security breach.\textsuperscript{24}

Monster.com, a job posting website, also suffered a security breach in 2007 that affected approximately 1.4 million users. Hackers accessed the resume database and stole IDs, names, e-mail addresses and other client contact information. This information was used to send "phishing" e-mails that spread malicious software and allowed the hackers to monitor the client's computer for online banking activity and obtain access to such accounts.\textsuperscript{25}

In January 2011, a hacker from Argentina gained access to hundred of accounts from the Vancouver based online dating service Plenty of Fish. In a bizarre series of events, the hacker ended up contacting Plenty of Fish CEO and requesting a job in exchange for not disclosing the hacked information.\textsuperscript{26}

As demonstrated by the above examples, corporations in a wide range of industries are at risk of security breaches. Corporate technology policies can serve to minimize the occurrence of these breaches.

\textsuperscript{25} Supra, note 18.
Protection of Corporate Reputation and Liability

In our world of social networking and YouTube popularity, employers need to consider the potential fallout from employee Internet postings. At the very least, employee postings could negatively impact a corporation's reputation. At the opposite end of the spectrum, these postings could be interpreted as employer authorized and lead to employer liability for any number of claims, including breach of contract, defamation, or harassment.

This potential liability was likely a concern of Cathay Pacific when one of its employees posted a video of a customer throwing a tantrum in the Hong Kong airport on YouTube. The video exploded into a viral sensation and obviously caused a great deal of embarrassment to the customer. While this situation did not result in litigation, in the right circumstances, the corporation could have been found to have infringed the customer's privacy rights.27

The power of social media can cause havoc on established, credible brands. In 2009, two Dominos' Pizza employees videotaped a "prank" at work and posted it to YouTube. The video depicts the employees violating numerous health code standards while preparing sandwiches for delivery. As one employee prepared a sandwich, the other employee narrated, stating:

"In about five minutes it'll be sent out on delivery where somebody will be eating these, yes, eating them, and little did they know that cheese was in his nose and that there was some lethal gas that ended up on their salami. Now that's how we roll at Dominos."

Within only a few days of posting, more than a million people had viewed the video. Needless to say, Domino customers were disgusted and voiced these opinions throughout Twitter and Internet blogs. The perception of corporate quality went from positive to negative, according to the research firm YouGov.28

Social media has the power to turn employee misconduct involving only a small number of people into a corporate marketing nightmare. When first learning about the video, Dominos executives chose not to respond aggressively in hopes that the controversy would dissipate. The executives severely underestimated the power of social media and their lack of response only worsened public opinion.

Employees need to be aware that postings to social networking or video sites such as YouTube, about workplace issues or other employer related issues, can have serious repercussions. For example, a February 5, 2011 AOL news report states that NBC fired an employee for posting a 1994 clip from the

"Today" show on the Internet. In the clip, Katie Couric and Bryant Gumbel have difficulty understanding and explaining the Internet and e-mail addresses. Bryant Gumbel asks "What is the Internet anyway?" and Katie Couric attempts to explain the Internet by calling it "that massive computer network, the one that's becoming really big now." NBC was understandably unhappy that its own employee had subjected its news anchors to ridicule. In regard to the firing, NBC stated: "The individual in question violated the company's standards of conduct by repeatedly copying and distributing a variety of materials without permission."

The Privacy Commissioner of Canada warns on her website that inappropriate disclosures of these kind may lead to:

- a defamation lawsuit;
- copyright, patent or trademark infringement claims;
- a privacy or human rights complaint;
- a workplace grievance under a collective agreement or unfair labour practice complaint;
- criminal charges with respect to obscene or hate materials; or
- damage to the employer's reputation and business interests.

Liability and potential damages resulting for any of the above actions could lay with the employee, management, or organization. Corporate technology policies can assist in making these repercussions clear to employees and in limiting behaviors that could lead to these harms.

In addition to helping prevent the liability discussed above, established technology policies can help avoid the mismanagement of technology related issues when a problem does arise. For example, in the unreported decision Leech v. British Columbia Television Broadcasting System Ltd., an employee was dismissed for making a copy of the company's payroll file. The employee stumbled across the payroll file when investigating why his work was taking so long to print. The employee noticed the payroll document in queue on the same local network to which the employee was printing and made a copy of the payroll document out of curiosity. The employer considered this information extremely confidential and terminated the employee. This case was adjudicated under the Canada Labour Code and the employer was ordered to reinstate the employee as he had not used any of the information for personal gain, nor disclosed the information to a third party.

The importance of this case is two fold. First, the manner in which management dealt with the situation depicts the employer's struggle in dealing with technology related incidents. Second, it underscores the need for a policy regarding the protection of confidential information. A simple

---

30 Ibid.
31 Ibid.
policy of printing confidential information to a private printer, as opposed to one that all staff members could access, may have prevented this situation.  

Similar mismanagement was demonstrated in Conrad v. Household Financial Corp. A password assigned to an employee of a financial institution was used to steal $1850 from multiple dormant accounts. Upon discovering this, the employer fired the employee the day before she moved to Halifax from Ottawa for a promotion within the company. The Court determined that her password had been stolen by another employee. The Court ruled that the employee was wrongfully terminated and was awarded punitive damages against the employer for its brash and unjust reaction.

This conclusion may have been avoided had the employer implemented an adequate policy concerning password protection. In fact, a US court concluded exactly that in Cervantez v. KMGP Services Company Inc. In this case, an oil field worker was fired for pornographic material being downloaded under his user ID on a shared computer. The employee sued, but the court ruled in favour of the employer. One of the reasons for the court's conclusion was that the computer policy of the company was clearly written, and it forbade users from sharing or writing down their passwords and expressly stated that “System Users are responsible for all transactions made using their passwords.”

TECHNOLOGY TOOLS AND LEGAL ISSUES

The number of employees using computers and accessing the Internet at work has increased significantly over the last decade. The U.S. Bureau of Labour Statistics reported that in 2003, 77 million Americans "used a computer at work, and these workers represented 55.5 percent of total working population of the United States." Of those workers using a computer, 2 out of 5 accessed the Internet or e-mailed while at work. Since that study in 2003, the number of workers using computers and accessing the Internet has profoundly increased.

This increased use of computers at work has increased the potential for their misuse. According to a 2005 survey by America Online and Salary.com, "the average worker admits to frittering away 2.09 hours per day, not counting lunch", which wasted time costs American employers $759 billion per

---

33 Supra, note 9 at 502 - 504.
35 Supra, note 9 at 503.
36 Sam Narisi, "Company sued for firing obscene Web browser" (10 November 2009), online: DocuCrunch <http://www.docucrunch.com/company-su...e-Web-browser>.
38 Ibid.
year in overpaid salaries. According to Salary.com, the number one employee time wasting activity is "personal Internet use." Similarly, in a July 2005 press release, Websense reported that "Internet misuse in the workplace costs American corporations more that $178 billion annually in lost productivity."

**a) E-MAIL**

On an average day, 110 e-mails are sent or received, per user, from 730 million corporate e-mail accounts (25 per cent of the estimated 2.9 billion e-mail accounts worldwide). Seventy-five per cent of North American companies will be monitoring all the e-mail sent and received, including the 18 per cent of e-mails that will be spam, and 25 per cent of companies will use that information to fire employees for misuse of company e-mail accounts. E-mail, once a purely technical concern, has become a significant human resource consideration.

Formulating a policy around the use of e-mail at work prevents more than just the headaches alluded to by VirtualRaven at the beginning of this paper. A well-written policy can protect an employer from employee complaints or grievances, mitigate the loss of employee productivity and company resources to web surfing and spam, ensure the privacy rights of employees are respected, and even protect an employer from charges under the Criminal Code. But in order for a policy to be effective, it must be supported by legal authority, and be written in a clear and concise fashion.

Before any specific policy provisions are considered, the overall purpose of the policy should be set out. Arguably, the best policy protects both employees and employers by doing the following:

- Making it clear to employees what appropriate use of the e-mail system does, and does not, include.
- Provide support to the employer should it need to rely on the policy to monitor the e-mail system or dismiss an employee for inappropriate e-mail use.

---

40 Ibid.
Legal Issues

Several legal issues surround employee use, and employer monitoring, of e-mail in the workplace. These include potential employer liability for harassing, discriminatory, or otherwise inappropriate e-mails that employees may send to each other, respecting employee privacy rights when monitoring e-mail, and the protection of confidential information.

Any e-mail policy should make it clear to employees that simply moving behaviour that is prohibited in the workplace to a virtual forum, or e-mail system, does not make it acceptable, or allow the offending employee to escape discipline. The policy should also reference or provide a link to pre-existing corporate policies on workplace harassment and discrimination.\(^\text{45}\) The problem facing an employer in such a situation concerns its ability to accumulate the evidence necessary to discipline an employee when the unacceptable behaviour has not occurred in front of managers or other employees with authority. Thus, this legal issue is intimately tied into the right of employers to monitor their employees' e-mail, and use material discovered through monitoring to discipline employees.

In Canada, the legal issues associated with monitoring employees' e-mail (and Internet use in general) center around privacy rights. Unlike the United States, where the assumption is that no e-mail accessed at work on company property is private, privacy legislation in Canada holds that employees do have some reasonable expectation of privacy when sending and receiving e-mails.\(^\text{46}\) The federal Personal Information Protection and Electronic Documents Act (PIPEDA), and its Alberta equivalent, the Protection of Personal Information Act (PIPA) set down how private organizations may collect, use, and disclose personal information in the course of commercial activity. Companies should understand the principles their legislation establishes, and how they define what is reasonable. This should be considered not only for monitoring employees, but in setting appropriate employee expectations for e-mail privacy. This is discussed below in the section “Employee Monitoring”.

"Common" Sense

When it comes to e-mail use at work, the jurisprudence seems to suggest that common sense is not all that common. Nevertheless, the law does support some basic, "common sense", prohibitions on e-mail use that can be enforced by a company, whether or not there was a clear corporate policy in place at the time of enforcement. In particular, the courts have found that storing or sending pornographic material can be grounds for termination, even if the employee was unaware of the e-mail use policy.\(^\text{47}\)

A well-drafted e-mail use policy provides clear and concise direction on the purpose of the corporate e-mail system, what constitutes appropriate use of the company e-mail system, and the consequences for using e-mail incorrectly. It may directly address:

- How employees obtain access to e-mail and become authorized for use.

\(^{45}\) Supra, note 2 at 8-88.2.  
\(^{46}\) Supra, note 44 at 86.  
Restrictions, or general guidelines, on personal use.

- Prohibit illegal or unethical use.
- Prohibit distribution of viruses or other harmful software.
- No indiscriminate copying of e-mails to individuals. No sending of irrelevant messages (jokes, pictures, junk mail, "chain letters").
- No disclosure of business or confidential information to unauthorized individuals.
- Do not express opinions that appear to be on behalf of, or representing the company unless authorized to do so.

Restrictions on use by third parties.

Company access to and monitoring of messages.

Confidentiality of computer and e-mail passwords.

Guidelines for language and content of e-mail messages.

Procedures for terminating access.

Penalties for breaching the policy. 48

It may also be important to review e-mail technology and the security and privacy issues that it raises in the policy. Although most people have an e-mail account today, some may still not realise that their e-mail is not inherently private. A company may want to review, in writing or through training, the following points:

- E-mail is not private. It is open to monitoring by management and may be accessible, through hacking or other means, to third parties.
- E-mail does not disappear after being sent, or even after being deleted. E-mails can be printed, saved or archived, and often are for legal or other reasons. Simply because the e-mail does not appear in an account does not mean it no longer exists.
- Never assume that the only person who will read the e-mail is the person to whom it is addressed. E-mail is easily and often forwarded. This can be to parties who were never intended to receive the message.
- E-mail can be broken into.
- E-mail can be monitored without any sign that the monitoring is occurring.

48 Supra, note 2 at 8-88.1 and David Corry & Cristie Sutherland, "Privacy Issues in Labour and Employment", Paper presented to the Legal Education Society of Alberta, Calgary, 11 June 2003 at 47.
• When you access or use e-mail at a remote site, it may leave traces on third-party computers over which the company has no control.

• Not all e-mail is encrypted.

• When you access e-mail wirelessly, it is even more vulnerable to interception. 49

After an e-mail policy has been drafted, its usefulness is limited by how fully and frequently it is reviewed with employees. The policy itself should also be reviewed often to ensure that it captures any changes in the technology (such as a switch to a cloud-based e-mail service) or to address any workplace-specific problems that may have arisen over time.

b) BLOGGING AND SOCIAL NETWORKING

"IT" is an area laden with acronyms, but WILB may be a new one. Coined by the researchers in a 2009 University of Melbourne study, it stands for Workplace Internet Leisure Browsing. According to the study, WILB is a powerful workplace tool, capable of sharpening workers' concentration and making them 9 per cent more productive than their unconnected colleagues (assuming they limit their browsing time to 20% of their workday). 50 Controversial as this study may be, it highlights a serious problem facing companies today: what limits do you put on employees use of the Internet for social networking or blogging or tweeting?

In 2009, 47% of workers were accessing their Facebook account at work, for an average of 15 minutes a day (although some employees admitted to spending at least two hours a day). This amounts to an estimated 1.5 per cent loss in total employee productivity. 51 But the use of Facebook and similar sites poses risks to companies that are unrelated to productivity drain. Facebook messages, unlike personal or corporate e-mail accounts, cannot be monitored by employers, and employees' posts on Facebook can be viewed by any 'Friend' with access to that employee's account. Allowing employees to access Facebook can circumvent system management software designed to prevent the loss of confidential information and make it difficult for a company to regulate what information about it is circulating on the Internet. This is particularly concerning if any of the postings about the company are defamatory. As of yet, there are few cases directly related to Facebook use or blogging at work, although an employee's blogging was specifically addressed in Alberta v. Alberta Union of Provincial Employees. 52

50 The University of Melbourne, Media Release, "Freedom to surf: workers more productive if allowed to use the Internet for leisure" (2 April 2009) online http://archive.uninews.unimelb.edu.au/view-58003.html
Personal Blogging

In *Alberta v. A.U.P.E.* writing a post entitled "Aliens Around the Coffee Table," amongst others, resulted in "Running Girl" being fired from her job as an Alberta Public Service Employee (this case was subject to judicial review, but not on the reasons for termination). Although the author (whose name was kept confidential) used aliases to describe her fellow employees, the aliases were easily recognized by her colleagues as members of the department. She also copied and pasted entire e-mail exchanges between herself and a supervisor regarding her health and wellness claim under "Cat Fight Coming - Me and the Power Hungry Wench in Charge" and disclosed confidential file information in a post labelled "Office of the 'O'". The employee also posted negative comments on her work and fellow employees on other blogs, which were eventually traced back to her. After the employee admitted to writing the blogs, she refused to remove them, and was terminated. Her supervisors found her conduct "totally contrary to the Department's values of respect and cooperation" and in violation of the Code of Conduct and Ethics, particularly with respect to a breach of confidentiality in "Office of the 'O'". It was unclear how the employer became aware of the blogs, but it was through a means other than employee monitoring.

Company Blogs

Having employees who are experienced in operating within the blogosphere or social networking environment is not always a disadvantage; many companies wish to have a corporate presence in the blogosphere or on social networking sites and having employees familiar with this area can be helpful. Like all Internet use, the key is to regulate what is appropriate at work.

If a company is going to allow employees to blog, either under their own name through a company-sponsored link, or on a company-run blog, a strict blogging policy is necessary to protect the company’s reputation and confidential information. The following points should be addressed in a corporate blog policy:

- What does the company defines as a 'blog'? Are websites, non-commercial sites, or internal communication postings included?
  
- Employees must continue to comply with any existing code of conduct.
  
- The company should identify a resource person that an employee should consult if they are unsure what may or may not be included in a blog.
  
- Bloggers should add a disclaimer to their posts stating that the views expressed are purely their own. When appropriate, a disclaimer may also be added stating that nothing written constitutes professional advice.
  
- Blogs should conform to current policies on confidentiality and non-disclosure.

---

• Blogging should not interfere with work commitments.\textsuperscript{54}

A company should be particularly wary of allowing blogging under a company banner, or even through a link on an employee’s e-mail signature, without clear policy. Blogging is an especially easy way for defamatory statements to be made public, or for confidential information to be lost. Blogs and social networking sites are public forums, and sometimes employees need to be reminded of that.

\textbf{Social Networking}

The increasing use of social networking websites has added a layer of complexity to employee Internet use. Employees can make statements on websites like Facebook that can affect the work environment. In a recent U.S. case, Dawnmarie Souza and the National Labor Relations Board settled a lawsuit with a Connecticut ambulance company over Souza’s firing for making "derogatory remarks about her employers on Facebook."\textsuperscript{55} Souza apparently made the comments from her home computer when she was not working and therefore the National Labor Relations Board argued such actions were considered protected speech.\textsuperscript{56} In response to the incident, the employer has now changed its policies "in ways that will no longer prohibit employees from talking about work online, even if such talk constitutes what the company called 'online badmouthing.'"\textsuperscript{57}

The Privacy Commissioner of Canada recommends that when setting out a policy regarding social networking, a company should first make employees aware that their social network information could potentially be viewed or accessed by:

• current or potential employers;
• recruitment agencies;
• co-workers;
• the employer's competitors;
• government and law enforcement; or
• others outside the employee's "trusted network.”\textsuperscript{58}

\textsuperscript{54} Jason Young, The Blogger in the Workplace: Considerations for Employers and Employees, (2005-06) 6 I.E.C.L.C.
\textsuperscript{55} Jolie O'Dell, "Employee Fired Over Facebook Comment Settles Lawsuit" Yahoo News (8 February 2011) online: Yahoo <http://news.yahoo.com/s/mashable/20110208/tc_mashable/employee_fired_over_facebook_comment_settles_lawsuit_1>.
\textsuperscript{56} Ibid.
\textsuperscript{57} Ibid.
\textsuperscript{58} Office of the Privacy Commissioner of Canada, Fact Sheet: Privacy and Social Networking in the Workplace, May 2009 http://www.priv.gc.ca/fs-fi/02_05_d_41_sn_e.cfm
One out of every 33 employees has built their complete Facebook profile at work, and the Privacy Commissioner recommends that companies develop policies on social networking sites (SNS), which include the following:

- Whether the organization permits the use of personal or employer-hosted SNS in the workplace.
- If SNS are permissible, in what context and for what purposes may they be used?
- Whether the employer monitors SNS sites.
- What legislation applies to the collection, use or disclosure of personal information in the workplace.
- What other rules may apply to the use of SNS in the workplace (collective agreements other relevant legislation).
- The consequences of non-compliance with the policy.
- Any other existing policies about the proper use of electronic networks with respect to employee privacy and handling confidential information.

Employee use of social networking sites makes employers vulnerable to defamation lawsuits, IP infringement claims, privacy or human rights complaints, workplace grievances, criminal charges, and can result in serious damage to a company's reputation. For all of these reasons, developing a clear policy and communicating that policy to employees is critical.

c) PROPRIETARY WORKS MANAGEMENT

With the increased use of the Internet at work, the problem of proprietary information management has moved far beyond employees secretly photocopying confidential files late at night. A company's intellectual property or confidential information has been made more vulnerable by increased accessibility and increased opportunity for dissemination by employees. Corporate trade secrets are clearly understood to be confidential, but companies today also deal with information that must be treated as confidential under statute, such as personal health information or information collected from employees in the course of their employment. Companies are also bound by many license agreements, with restrictions imposed on access and use. For a variety of reasons, the value of keeping information confidential is greater than it has been before.

When it comes to the protection of company information, employees are bound by the same common law duties they were in the age of the telegram: obligations of good faith and fiduciary duty. And, having developed over the 20th century, these duties have received significant judicial consideration, especially as it relates to employment contracts.

---

59 Supra, note 51.
60 Supra, note 58.
61 Supra, note 58.
Legal Issues

All employees have a basic duty to serve their employer with good faith, loyalty and fidelity. This duty, unlike a fiduciary duty, does not depend on the nature of employment; it is a duty that all employees owe. This duty would preclude the employee from engaging in "any conduct that is incompatible with the due or faithful discharge of the employee's duty."\(^{62}\) These duties end at the termination of the employment relationship. Fiduciary duty, which is owed by directors and senior employees in companies, will outlast the employment relationship and is much more extensive. However, common to both is the obligation to not reveal confidential information.\(^{63}\)

Unfortunately, being bound by a common-law duty does little to prevent an employee from scanning and e-mailing files, or posting a trade-secret (or client file information) on their personal blog. The recent Wikileaks scandal has proven that even being bound by law will not prevent the loss of information. However, through a comprehensive policy and technical solutions such as encryption and network firewalls, a company can reduce the risk of lost information.

Protection through Policy

There are four key elements to any policy geared to protect proprietary information:

- Defining "Confidential"
  - Setting out what the company considers its confidential information or information it does not want disclosed.
  - What "keeping it confidential" means.
- Identifying employee obligations.
- Stating employer expectations and obligations.
- Setting out the consequences if an employee is found to have breached the policy.

Defining confidential, or proprietary, information and telling employees what keeping information confidential entails may seem like an obvious exercise, but is an essential part of any policy for several reasons. First, the employer may want certain information, that is not technically "confidential" (such as a company's financial statements or employee know-how) to be labelled as such for the purposes of its policy.\(^{64}\) Secondly, the very notion of "confidentiality" must be thought of in the context of a sharing culture that has developed since the rise of Facebook, Twitter, and other social networking sites. Employees today are increasingly comfortable disclosing personal information to their virtual networks, and the idea of confidential or private information is being slowly diminished over time. Thus, it is an important first step for a company to remind employees

---


\(^{63}\) Ibid. at 40.

that certain data should not be shared. Much like the technical discussions surrounding e-mail, a corporation may need to remind people that Facebook accounts and blogs are not private. Not only are they accessible by whatever "Friends" or followers an employee may have, their privacy settings are ultimately controlled by an external authority. It may also be advisable to remind employees that software and other programs they use at work are not meant to be used at home unless specifically authorized for that purpose.

Companies may, depending on the nature of their business, face serious economic, legal, and human resource consequences if confidentiality is breached. These problems range from being liable for a breach of license if employees are downloading corporately-licensed software at home, to a privacy investigation if employee information is not handled according to the applicable legislation. The right to patents are especially easy to lose if an employee has disclosed the invention, and there is no way to calculate the potential loss if a company loses a piece of proprietary information critical to its business operations. For these reasons, an employer should implement a strict code of discipline to deal with breaches of confidentiality.

Any policy on confidential information should set out the workplace-specific discipline employees could face if found to have breached the policy. The policy should also highlight that a company has more options open to it than progressive discipline up to and including terminating the employment relationship; the duty of good faith and the fiduciary duty allow a company to seek a remedy against the employee in court, even after he or she has left the company.65 Any disciplinary action that could flow from a breach of these should also be set out.

When dealing with proprietary information "an ounce of prevention is worth a pound of cure" should be the guiding principle, as a breach of information cannot be undone. A proprietary works management policy is a first line of defence in protecting proprietary information. A comprehensive policy helps protect employees and employers from accidental disclosure of information, and provides the employer with a remedy to discipline employees who do intentionally breach confidentiality.

The first step in implementing a comprehensive corporate technology use policy is developing one unique to company needs, taking into account some of the considerations listed in this paper. But a policy may be useless if not communicated clearly or enforced in the workplace. Companies need to consider the legal ramifications of policy enforcement, including how to enforce policy through employee monitoring and discipline.

MONITORING EMPLOYEES

Employers have responded to the trend of employee computer and Internet misuse by monitoring employees. According to the 2007 Electronic Monitoring & Surveillance Survey conducted by the American Management Association and The ePolicy Institute, 28% of the companies surveyed had fired employees for inappropriate e-mail use and 30% of the companies surveyed had fired

employees for misuse of the Internet. Of the employers that fired workers for e-mail use, 64% reported doing so for "violation of any company policy", 62% for "inappropriate or offensive language", 26% for "excessive personal use", 22% for "breach of confidentiality rules" and 12% fired employees for "other" reasons. With regard to the companies that fired employees for Internet misuse, 84% had fired employees for "viewing, downloading, or uploading inappropriate/offensive content", 48% for "violation of any company policy", 34% for "excessive personal use" and 9% for "other" reasons.

With regard to the types of measures employers were using to monitor employees or to control their Internet use, the results showed that 65% of the companies surveyed block access to inappropriate web sites. These employers are generally trying to prevent workers from accessing pornographic, gaming, social networking, entertainment, shopping and sports web sites as well as "external blogs."

In addition to blocking access to web sites, 45% of the employers surveyed tracked "content, keystrokes, and time spent at the keyboard." Another 43% store and review computer files. In addition, 12% monitor the blogosphere to see what is being written about the company, and another 10% monitor social networking sites. The majority of the companies that monitor e-mail use "technology tools to automatically monitor e-mail" while the minority actually assign a person to "manually read and review e-mail."

Some of largest and most respected companies in the United States have had problems with inappropriate employee Internet use, and have taken direct steps to control it. For example, in a 2003 article, Dr. Kimberly S. Young & Dr. Carl J. Case state:

The New York Times fired 22 employees in Virginia for allegedly distributing potentially offensive electronic mail (Associated Press 2000). Xerox terminated 40 workers for spending work time surfing pornographic and shopping sites on the Web (AP, 2000). Dow Chemical Company fired 50 employees and suspended another 200 for up to four weeks without pay after an e-mail investigation uncovered hard-core pornography and violent subject matter (Collins, 2000). Merck disciplined and dismissed employees and contractors for inappropriate e-mail and Internet usage (DiSabatino 2000). According to a survey of human resource directors, approximately 70% of companies provide Internet access to more than half of their employees ... In a survey of 1439 workers by Valty.com, an online analyst firm, 37% admitted to

66 Supra, note 43.
67 Ibid.
68 Ibid.
69 Ibid.
70 Ibid.
71 Ibid.
72 Ibid.
73 Ibid.
surfing constantly at work, 32% surfed a few times a day, and 21% surfed only a few times a week (Adschiew, 2000). In a survey of 224 corporations by Websense, Inc., an electronic monitoring firm, 64% of the companies have disciplined, and more than 30% have terminated, employees for inappropriate use of the Internet (Websense, 2000). Specifically, accessing pornography (42%), online chatting (13%), gaming (12%), sports (8%), investing (7%), and shopping at work (7%) were the leading causes for disciplinary action or termination. In an online usage report conducted in 2000 by eMarketer.com, 73% of U.S. active adult users accessed the Web at least once from work, 41% access the Web a majority of the time at work, and 15% go online exclusively at work (McLaughlin, 2000).74

Employee Internet misuse has also affected large Canadian companies. For example, Bruce Power, a privately owned operator of a nuclear plant northwest of Toronto, fired "dozens" of contract workers in September of 2009 for improper computer activities such as Internet and e-mail misuse.75 Bruce Power spokesman Ross Lamont stated "[n]one of the information that we're dealing with here is business related. There are no trade secrets, and absolutely no impact on operations, on security, on safety. It was just inappropriate behaviour."76 Fortunately for Bruce Power, it appears the employee Internet use had not compromised the security or safety of its nuclear power plant. However, such a possibility illustrates the magnitude of the problems employee computer misuse may cause. Perhaps in recognition of this risks, Lamont also stated that: "[a]ny significant company has some monitoring of their systems."77 However, it is not clear that Bruce Power had effectively implemented a computer or Internet policy. One former Bruce Power employee, who had apparently worked at Bruce Power over twenty years, called the situation "bizarre" and said he did not remember reading Bruce Power’s code of conduct, which prohibits personal Internet use.78

Legal Principles Relating to Employee Monitoring in Alberta

As noted above, employers are utilizing employee monitoring techniques to minimize the risks associated with employee computer and Internet misuse. The balance of this section will discuss the basic legal principles regarding employee monitoring in Alberta.

Balancing Employer Needs and Employee’s Privacy Rights

Melanie R. Bueckert notes "[t]he legal dimension of employee monitoring primarily relates to workplace privacy interests, and the extent to which employee privacy concerns should yield to other

---

76 Ibid.
77 Ibid.
78 Ibid.
competing demands.\textsuperscript{79} The key at the outset is to understand that while there are many legitimate reasons to monitor employees, there must be a balance between these and the privacy rights of employees.

Kris Klein\textit{ et al.} explain that because employers own the work computer, they generally consider that any messages or content on it is employer property, and as such, the employee has no reasonable expectation of privacy.\textsuperscript{80} There appears to be significant support for this position in Alberta. In 2009, the Alberta Court of Appeal stated "[t]he workplace is not an employee's home; and employees have no reasonable expectation of privacy in their workplace computers."\textsuperscript{81} It should be noted, however, that the Court of Appeal in that case was determining the merits of a wrongful dismissal action and was not specifically conducting an in-depth analysis of the extent to which employers may monitor an employee's computer use. Klein\textit{ et al.} also explain that the basic tension between employer's rights and employee's privacy rights stems from the fact that:

courts and legislators in the United States and Canada have come to hold that the right of privacy is a "personal right" which is held by everyone and cannot be alienated. For this reason in part, therefore, it is inappropriate to suggest that ownership rights negate or subordinate privacy rights as the two kinds of rights are different and overlapping in nature, and are not mutually exclusive.\textsuperscript{82}

Moreover, the issues surrounding these overlapping rights have yet to be clarified in Canada. Klein\textit{ et al.} note that "[t]here is no definitive Canadian ruling addressing the issue of employee e-mail. Who owns the e-mail in the context of e-mail sent or received by an employee via his or her employer's computer system is a question which has yet to be addressed by the Canadian judicial system or by statute."\textsuperscript{83} This uncertainty also applies to employee monitoring in general. However, it does appear that in Canada, employers do not have unlimited discretion to monitor employees, as Klein\textit{ et al.} note:

[p]rivacy legislation, jurisprudence and doctrine suggests that the issues require a balancing of employee's privacy rights against the employer's legitimate business interests; however, the emerging case law indicates that employee privacy rights militate against the position that employers have an unfettered right to monitor employee's e-mail and Internet use.\textsuperscript{84}

With this background, this section will turn to an examination of Canadian and Alberta statutes relevant to employee monitoring.

\textsuperscript{80} \textit{Supra}, note 44, at 85.
\textsuperscript{81} Poliquin v. Devon Canada Corporation, 2009 ABCA 216 at para. 45.
\textsuperscript{82} \textit{Supra}, note 44.
\textsuperscript{83} \textit{Ibid.} at 90.
\textsuperscript{84} \textit{Ibid.} at 90-91.
**Criminal Code**

Section 184 of the *Criminal Code* makes the "interception" of a "private communication" by electromagnetic or similar means an indictable offence. However, Klein *et al.* note that "it appears section 184 does not protect electronic communication where the communication is not private, or if consent to intercept is obtained from at least one of the parties. A communication is only private if the parties to the communication have a reasonable expectation of privacy." At present, it is far from clear that employees should have a reasonable expectation of privacy in materials contained on work computers. For example, in a 2003 wrongful dismissal action in which the employer alleged it had terminated for cause in part due to excessive e-mail use, the Alberta Court of Queen's Bench stated:

> Even where an e-mail policy is published within a workplace, and even where the published policy outlines some privacy rights for an employee, an employee may not have a reasonable expectation of privacy when the contents of the employee's e-mail is of an unprofessional nature, offensive, or where access by the employer is in furtherance of investigating illegal activity, in which case the employer's interests would outweigh an claimed privacy right. Where there is no e-mail policy in place, an employee has no reasonable expectation of privacy in relation to e-mails received and sent in the workplace on the employer's time and equipment ... It is obvious that it is best for an employer who provides e-mail and Internet access to its employees to develop for, and publish to, its employees a policy concerning the use of e-mail. In the absence of any such policy, an employee has no reasonable expectation of privacy in relation to e-mails sent and received using corporate assets, particularly once the e-mail is accessible to, or passes through, the hands of third parties, or once the individual has communicated unprofessional comments to a second person over an e-mail system utilized by the entire company.

As Klein *et al.* note, "section 184 of the *Criminal Code* was enacted to protect private communication only. The protection afforded by the Code is inherently limited by its terms and does not really affect an employer's right to access business communications paid for by the employer and made in the conduct of business."

The *Criminal Code* also includes an anti-hacker section that makes the interception of any computer function without colour of right an indictable offence. The question with regard to employee monitoring is whether the employer has any right to monitor the employee's computer system. Klein *et al.* note that:

---

85 R.S.C. 1985, c. C-46, s. 84.
86 *Supra*, note 44 at 89.
88 *Supra*, note 44 at 89.
89 s. 342.1(1)(b).
While Canadian courts have yet to apply the *Criminal Code* provisions to the context of employee monitoring of employee e-mail, in light of these provisions it is very important for an employer to have a policy concerning the use of office equipment which clearly informs employees that telephone calls, voice mail, and e-mail may be monitored for legitimate business purposes. Such a policy, combined with the fact that the employer pays for telephone and e-mail services and expects these services to be used for business purposes, may defeat any expectation of privacy that an employee might have in his or her communications.\(^{90}\)

**Privacy Legislation**

Both PIPEDA and PIPA set ground rules for how private sector organizations may collect, use and disclose "personal information" in the course of commercial activities. PIPEDA defines "personal information" as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."\(^{91}\) PIPA defines "personal information" as "information about an identifiable individual."\(^{92}\)

Both PIPEDA and PIPA are based on the principle that an organization cannot collect, use or disclose personal information unless (1) it obtains consent of the individual and (2) the collection, use or disclosure of the information is reasonable. According to the 2009-10 Annual Report of the Office of the Information and Privacy Commissioner of Alberta, PIPA "seeks to balance the right of an individual to have his or her personal information protected, with the need of organizations to collect, use or disclose personal information for reasonable purposes."\(^{93}\) The report notes that "[c]omplaints regarding surveillance in the workplace - monitoring employee use of computers and other corporate equipment, as well as video surveillance - appear to be increasing."\(^{94}\)

Section 4.3 of Schedule 1 of PIPEDA states: "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."\(^{95}\) In addition to obtaining consent, PIPEDA also states that "[a]n organization may collect use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances."\(^{96}\) Melanie Bueckert notes:

> While PIPEDA is primarily concerned with consent, from an employee's perspective perhaps the most important provision in PIPEDA is the additional requirement that organizations only collect, use, or disclose

\(^{90}\) *Supra*, note 44 at 90.
\(^{91}\) Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 s. 2(1) [hereafter PIPEDA].
\(^{92}\) *Personal Information Protection Act*, 2003, c. P-6.5, s. 1(1)(k) [hereafter PIPEDA].
\(^{94}\) Ibid.
\(^{95}\) PIPEDA Schedule 1, s. 4.3.
\(^{96}\) PIPEDA s. 5(3)
personal information for purposes that a reasonable person would consider appropriate in the circumstances. This objective reasonableness component helps counteract the difficulties that an entirely consent-based model would present in the employment context, due to the imbalance of power inherent in the employment relationship.\textsuperscript{97}

Section 7 of PIPA also states that an organization cannot collect, use or disclose personal information unless the individual consents to such collection, use or disclosure. In addition, PIPA mandates that organizations only collect personal information for reasonable purposes, and that the actual collection must occur in a manner that is reasonable for satisfying those purposes.\textsuperscript{98} Unlike PIPEDA however, PIPA establishes specific requirements in regard to the collection of \textit{personal employee information}. Section 15(1) states:

An organization may collect personal employee information\textsuperscript{99} about an individual without the consent of the individual if:

\begin{enumerate}
\item a) the information is collected solely for the purposes of (i) establishing, managing or terminating an employment or volunteer-work relationship; or (ii) managing a post-employment or post-volunteer-work relationship between the organization and the individual;
\item b) it is reasonable to collect the information for the particular purpose for which it is being collected; and
\item c) in the case of an individual who is a current employee of the organization, the organization has, before collecting the information, provided the individual with reasonable notification that personal employee information about the individual is going to be collected and the purposes for which the information is going to be collected.
\end{enumerate}

It is also important to note that PIPA has similar provisions regarding the "use" and "disclosure" of personal employee information.\textsuperscript{100} An Alberta employer can, therefore, collect an employee's personal information if such collection is reasonable and the employee consents. Furthermore, an employer can collect and use personal employee information without the employee’s consent if such collection meets the requirements of Section 15 or 18 of PIPA, in which an employer must demonstrate that the information was collected or used for the purposes of managing the

\textsuperscript{97} Supra, note 79 at 27.
\textsuperscript{98} PIPA, s. 11.
\textsuperscript{99} PIPA s. 1(1)(j) states "'personal employee information' means, in respect of an individual who is a potential, current or former employee of an organization, personal information reasonably required by the organization for the purposes of (i) establishing, managing or terminating an employment or volunteer-work relationship, or (ii) managing a post-employment or post-volunteer work relationship.
\textsuperscript{100} See PIPA sections 18 and 21.
employment relationship, that it was reasonable to collect or use the information for that purpose and that reasonable notice was given to the employee that the information would be collected or used.

The current jurisprudence with regard to specific types of employee monitoring practices that might satisfy the requirements of Section 15 and 18 of PIPA is underdeveloped. It does appear, however, that the Alberta Court of Appeal is sympathetic to employers' concerns. In a 2009 wrongful dismissal case involving the use of work computers to view and transmit pornographic images, the Alberta Court of Appeal stated in dicta that "an employer is entitled not only to prohibit use of its equipment and systems for pornographic or racist purposes but also to monitor an employee's use of the employer's equipment and resources to ensure compliance."\(^{101}\) It should be noted that the case was not dealing specifically with PIPA or PIPEDA.

In contrast to the unqualified statement from the Court of Appeal, the language of Section 15 or 18 of PIPA would suggest that at the very least, reasonable efforts must be made to ensure that the information collected or used was related to managing the employment relationship and that the collection or use of such information was reasonable.

In light of the lack of jurisprudence on the issue, it is only possible to provide general conclusions with regard to the types of monitoring activities that would be considered reasonable for purposes of PIPA and PIPEDA.

The Privacy Commissioner of Canada has used the following four-part test for determining whether employee monitoring is reasonable.

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?\(^{102}\)

Melanie Bueckert also notes that, in determining the reasonableness of employee monitoring, the following factors should be weighed:

- The nature of the monitoring.
- The employee's awareness of the monitoring.
- Whether the monitored activity is classified as "business" or "private".
- The egregiousness of the monitoring.\(^ {103}\)

In addition, Bueckert notes that Professor Geist has suggested the following factors be balanced:

\(^{101}\) Supra, note 81 at 49.
\(^{102}\) PIPEDA Case Summary #351, [2006] C.P.C.S.F. No. 28 (QL)
\(^{103}\) Supra, note 79 at 157.
• The target of the surveillance.
• The purpose of the surveillance.
• The prior use of alternatives to surveillance.
• The surveillance technology.
• The adequacy of notice provided to the target of the surveillance.
• The implementation of the surveillance.  

Conclusion

Employers would likely prefer concrete answers regarding the types of monitoring practices that satisfy the requirements of PIPEDA and PIPA. However, as noted, the law in this area is undeveloped. In addition, as with many legal test that employ a reasonableness standard, the ultimate conclusion as to whether a specific monitoring practice was reasonable for the purposes of PIPEDA or PIPA will be fact dependant. Therefore, care should be taken to craft employee monitoring policies that address the specific needs of the employer and are reasonable in light of the potential damages an employer may suffer as a result of e-mail or Internet misuse.

POLICY ENFORCEMENT - HOW TO MAKE POLICIES ENFORCEABLE AND THE FAILURE TO ENFORCE

Introduction

The enforcement of workplace technology policies is undoubtedly now a major issue for employers. A 2010 survey regarding enforcement by companies in the United States indicated the following:

• 38 per cent of the companies surveyed indicated that they now employ staff to analyze the contents of outbound e-mail with 48 per cent of companies surveyed now conducting regular audits of outbound e-mail content.
• 20 per cent of the companies surveyed reported that employee e-mail had been subpoenaed for use in legal proceedings.
• 35 per cent of the companies surveyed had investigated an e-mail-based leak of confidential information; 50 per cent had disciplined an employee for violating e-mail policies, and 20 per cent had terminated an employee for violating e-mail policies.
• 24 per cent of the companies surveyed had disciplined an employee for violating blog or message board policies, with 11 per cent of companies reporting to have terminated an employee for such a violation.

---

104 Ibid. at 157-158.
105 Survey conducted of 261 companies, each with more than 1000 employees.
• 21 per cent of the companies surveyed had disciplined an employee for violating multimedia and sharing policies, with 9 per cent reporting having terminated an employee for such a violation.

• 20 per cent of the companies surveyed had disciplined an employee for violating social network policies, with 7 per cent reporting to have terminated an employee for such a violation.\(^{106}\)

As of 2010, 53% of companies now completely block social networking sites.\(^{107}\)

**Incorporation of a Technology Policy into the Contract of Employment**

A threshold issue in considering the enforceability of policies, is whether the policies have actually been incorporated into the contract of employment. It is likely that the introduction of a new workplace policy which imposes additional obligations on employees, including new grounds for dismissal, may be considered as a variation of the existing employment contract with an employee. As a result, in order to make a technology policy binding each employee must agree to incorporate the policy as a term of the employment contract.

The court in *Starcevich v. Woodward’s Ltd*\(^{108}\) confirmed that mere awareness of a company policy by an employee is insufficient for a employee to be bound by a particular policy, but that “there would have to be clear and unequivocal evidence to establish that the [employee] had agreed to the policy forming part of his own contract of employment.”\(^{109}\)

The importance of the acceptance of a workplace policy by an employee was illustrated in the seminal case of *Hill v. Peter Gorman Ltd.*\(^{110}\) in which an employer had sanctioned an employee for a breach of a company policy introduced after the date of employment. With respect to the incorporation of the policy in to the employment contract, the Court concluded:

> I cannot agree that an employer has any unilateral right to change a contract or that by attempting to make such a change he can force an employee to either accept it or quit ... [w]here the employer attempts to vary the contractual terms, the position of the employee is this: He may accept the variation expressly or impliedly in which case there is a new contract\(^{111}\).

\(^{106}\) Proofpoint, Inc., "Outbound E-mail and Data Loss Prevention in Today's Enterprise, 2010", Results from Proofpoint’s seventh annual survey on outbound messaging and content security issues, http://www.proofpoint.com/outbound.


\(^{110}\) (1957), 9 D.L.R. (2d) 124 (Ont. C.A.).

\(^{111}\) *Ibid.*, at p. 132.
Further, the Manitoba Court of Appeal in *Wiebe v. Central Transport Refrigeration (Man.) Ltd.*\(^{112}\) recognized the distinction between the situation where a workplace policy had been accepted by the employee and incorporated into the contract of employment, thereby providing the employer the contractual right to immediately terminate an employee for a breach of policy, and the situation where a policy has not been accepted as a term of the contract of employment thereby preventing an employer from relying on breaches of policy as grounds for dismissal. The Court concluded that, where a workplace policy has not been incorporated into the employment contract, the employer may not exercise its automatic right of termination pursuant to the policy but is restricted to the claim that the employee's conduct was inappropriate according to the common law principles of just cause for dismissal.\(^{113}\)

Similarly, where an employer seeks to summarily dismiss an employee pursuant to the terms of a corporate technology policy, the Court will consider whether the policy has been incorporated as part of the contract of employment. In *Poliquin v. Devon Canada Corp.*\(^{114}\), the court noted that "Devon had promulgated a comprehensive Code of Conduct and specifically required its employees, including Poliquin, to acknowledge that they had read, understood and accepted its terms"\(^{115}\), before eventually concluding that the employer, Devon Canada Corp. was warranted in terminating an employee pursuant to the terms its technology policy.

Thus, when implementing a technology policy, it is important that an employer obtain evidence that its employees have read, understood and agreed to be bound by its terms. It would be prudent for an employer to obtain the employee's acceptance of the policy in writing, in order to prevent the future argument that the policy had not been incorporated as a term of the contract. It is common practice to present to an existing employee, at the time of the annual performance review, all new or revised corporate policies promulgated in the preceding year, for review and execution by the employee. Such evidence in writing, concurrent with the obvious contractual "consideration" that often accompanies a successful performance review in the form of a raise or bonus, renders the employment contract appropriately varied at law and enforceable. In the event a corporate technology policy is not deemed to have become part of the employment contract, the employer must address improper conduct through the use of the common law.

**How to Make Technology Policies Enforceable**

The enforcement of the terms of a corporate technology policy most commonly includes making employees aware of acceptable standards of conduct and taking disciplinary measures against those employees who breach the terms of the policy, up to and including dismissal. Ultimately, the enforcement of an IT policy speaks to the ability of an employer to justify the dismissal of an employee based on a breach of the policy. As stated in *Roney v. Knowlton Realty Ltd.*\(^{116}\), the

---


\(^{113}\) Ibid., at p.8.

\(^{114}\) *Supra*, note 81.

\(^{115}\) *Supra*, note 81 at para. 71.

\(^{116}\) (1995), 11 C.C.E.L. (2d) 205 (B.C.S.C.) ("Roney")
following criteria must be satisfied in order for the breach of a company policy to constitute just cause for dismissal:\footnote{Ibid., at para. 8; confirmed in Poirier v. Wal-Mart Canada Corp., 2006 BCSC 1138 at para. 61.}{\footnote{Discussed in greater detail beginning at p. 32 below.}}\footnote{2007 ABQB 349 ("Foerderer").}{\footnote{Ibid., at para. 67.}}\footnote{David M. Doubilet & Vincent I. Polley, Employee Use of the Internet and E-Mail: A Model Corporate Policy, David M. Doubilet (American Bar Association, 2002) at pg. 27.}{\footnote{Charles Morgan & Julien Saulgrain, E-Mail Law, (Markham: LexisNexis, 2008) at pg. 96-97 ("E-Mail Law").}

1. it has been distributed to employees;
2. it is known to the employee affected;
3. it is unambiguous;
4. it is consistently enforced by the company;\footnote{Discussed in greater detail beginning at p. 32 below.}  
5. employees are warned that they will be dismissed should they breach the rule or policy;
6. it is reasonable; and
7. the breach thereof is sufficiently serious to justify dismissal.

This criteria was reiterated in the more recent decision of \textit{Foerderer v. Nova Chemicals Corporation}\footnote{2007 ABQB 349 ("Foerderer").} where it was stated that an Internet use policy was enforceable because it was "reasonable, unambiguous, well published, consistently enforced, and the [dismissed employee] knew or ought to have known of their content, including the consequences of their breach."\footnote{Ibid., at para. 67.}

In addition to the guidelines above which address the enforceability of corporate policies generally, the following are additional considerations which are specific to the enforceability of corporate technology policies.

First, the policy should alert the employee that the electronic communication tools subject to the policy are the property of the employer,\footnote{David M. Doubilet & Vincent I. Polley, Employee Use of the Internet and E-Mail: A Model Corporate Policy, David M. Doubilet (American Bar Association, 2002) at pg. 27.} and that the employer will routinely monitor the use of such tools without notice. Alerting employees to the fact that their use of company-owned property will be monitored, serves to counter any potential claims that the employee had a reasonable expectation of privacy. In terms of electronic communication tools, the policy should also expressly apply to both internal communications between employees and external communications outside of the company so as to be sufficiently broad in scope.\footnote{Charles Morgan & Julien Saulgrain, E-Mail Law, (Markham: LexisNexis, 2008) at pg. 96-97 ("E-Mail Law").}

The policy should also clearly set out the prohibited uses of the communications tools subject to the policy. By clearly defining the prohibited uses, the company will establish the conduct which constitutes a breach and which will in turn allow the employer to impose sanctions on the employee. For instance, the policy may state that electronic communications which include harassing, racist,
sexist or otherwise inappropriate content are prohibited, in addition to viewing, downloading, generating, or possessing offensive or inappropriate materials.

Similarly, a workplace technology policy should set out the parameters of allowable personal use of electronic communication tools, if any. Allowing for limited personal use of electronic communication tools (especially e-mail) underscores the reasonableness of the policy, which is a factor often taken into account by a court or arbitrator in determining if an employer’s discipline pursuant to a policy is appropriate. While an employer clearly has the right to restrict personal use of the computer, it has been determined that it is not reasonable for an employer to expect that an employee will never use e-mail for personal use. As a result, it may be prudent for an employer to state that its electronic communication tools are to be used for business purposes, with the allowance for “occasional” personal use involving incidental amounts of employee time (coffee breaks, lunch), where such uses are not prohibited above and which do not hinder the conduct of its business.

With respect to a technology policy’s enforceability, it is important that the policy clearly reserves the right of the employer to discipline employees for breaches of the policy, including a right of termination. If a policy does not clearly communicate the consequences of a breach of policy, an employer may be subsequently prevented from disciplining an employee, even in response to a breach of its terms. In Canadian National Railway Co. and United Transportation Union, the labour arbitrator concluded that it was inappropriate for the employer to have dismissed an employee for a breach of its policy since the policy did not clearly indicate that such a breach could result in termination. The employee was ordered to be reinstated as a result.

In the Foerderer case mentioned above, the employer had terminated an employee for breach of the employer’s anti-harassment and Internet use policies. The Court considered the enforceability of the policies, which had been introduced after the employee had commenced work. The terms of the policy stated that employees were only to use the employer’s computers for appropriate business purposes while also alerting employees to the fact that the employer will routinely monitor Internet use and that the penalty for breach of the policy included termination. While the policy permitted some personal use of the Internet, offensive websites were prohibited.

The Court also noted that the employer’s practice in enforcing the policy, where an employee had used the Internet in an inappropriate manner, was to notify the particular employee of the breach, provide a warning, and potentially blocking Internet access. In light of the allowance for limited personal use of the Internet, the employer sent out a clarifying memorandum to all employees (prior to the plaintiff employee’s misconduct) which reiterated the unacceptable uses of the Internet and the potential consequences of breaching the policy. The Court considered the clarifying memo as a warning to all employees regarding inappropriate use of the Internet. As a result of the above, the

123 Foerderer, supra, note 119 at para. 67; Roney, supra, note 116 at para. 8.
126 Ibid., at para. 13, 15.
127 Foerderer, supra, note 119.
Court concluded that policy was both enforceable and known to the plaintiff employee and that he had simply chosen to ignore it.

Therefore, when implementing or simply maintaining a corporate technology policy, a company would be well advised to follow the criteria set out in Roney and Foerderer, in addition to the specific recommendations regarding technology policies discussed above. Further, in order to counter any possible argument that the technology policy was not known to employees (or similarly forgotten) and therefore not enforceable, it is good practice for an employer to send out occasional clarifying memorandums or alerts to employees which reiterate the fundamental terms of the technology policy, including penalties for non-compliance.

**Failure to Enforce a Corporate Technology Policy**

Since a corporate technology policy includes the ability to sanction employees conduct, including termination, where such conduct constitutes a breach of policy, the effect of failing to enforce an technology policy, whether initially or in response to a breach, may constitute condonation of the employee's conduct. The failure to enforce a technology policy is relevant to whether the employer has just cause for dismissal of an employee who has breached the terms of the policy.  

Conduct which constitutes just cause for dismissal must be "serious misconduct that is incompatible with the fundamental terms of the employment relationship." The leading decision of McKinley v. BC Tel sets out the principles to determine whether an employer has just cause to terminate an employee:

> Based on the foregoing considerations, I favour an analytical framework that examined each case on its own particular facts and circumstances, and considers the nature and seriousness of the dishonesty in order to assess whether it is reconcilable with sustaining the employment relationship. Such an approach mitigates the possibility that an employee will be unduly punished by the strict application of an unequivocal rule that equates all forms of dishonest behaviour with just cause for dismissal. At the same time, it would properly emphasise that dishonesty going to the core of the employment relationship carries the potential to warrant dismissal for just cause.

In applying the principles from McKinley, courts have found that the approach is equally applicable to other misconduct as it is to dishonesty. Thus, in order to dismiss an employee for breach of a company policy, the breach must be considered in light of the facts and circumstances of the case to determine whether the breach goes to the heart of the employment relationship.

---

131 Ibid., at 189-190.
In determining whether an employer had just cause to dismiss an employee, the failure to enforce a
corporate technology policy on prior occasions may be deemed to be condonation of a breach of the
policy. The principle of condonation was summarized by the New Brunswick Court of Appeal in

*Backman v. Maritime Paper Products Ltd.*\(^{133}\)

[t]he law holds that an employer who does not discipline an employee
within a reasonable period of time for a known act of misconduct
cannot later dismiss the employee for that particular act of misconduct,
but, if the employee engages in further misconduct, the previous
misconduct can then be considered by the employer in determining the
appropriate sanction for the latter misconduct.\(^{134}\)

Further, where an employer fails to enforce a policy, it runs the risk that, in the event it attempts to
rely on subsequent breaches of that policy by an employee as a basis for discipline or dismissal, a
court may conclude that the effect of the previous failure to properly enforce the terms of policy
essentially created a "permissive culture" whereby breaches are condoned. When seeking to
discipline or dismiss an employee for cause for breach (or several breaches) of a technology policy,
condonation of past policy breaches will be taken into account by a court or labour arbitrator. Thus,
a corporate technology policy must be consistently and fairly enforced by the employer in order to be
effective.

The failure to enforce an IT policy may often be attributed to a lack of employee monitoring, which
provides the employer with the necessary facts to allow it to take steps to enforce the policy. In
failing to implement an effective monitoring system to ensure that compliance is taking place, the
employer may effectively create a "permissive culture" where it is expected that breaches of a
technology policy go unpunished.

For instance, an Ontario labour arbitrator in *Consumers Gas v. Communications, Energy and
Paperworkers Union (Primiani Grievance)*\(^{135}\) considered the impact of the lack of consistent
enforcement of an Internet use policy on the dismissal of an employee for cause. In *Primiani*, the
employee breached the employer's Internet use policy by both possessing pornographic pictures on
her computer and for forwarding those pictures by e-mail to external parties and other employees.
In considering whether the termination for cause was proper, the arbitrator concluded, that since the
employer had failed to monitor and enforce the Internet use policy in the past, the employer had
been deemed to have contributed to the plaintiff’s breach by "turning a blind eye to the permissive
culture that existed at the company."\(^{136}\) The arbitrator also noted that the Internet use policies had
been enforced in an inconsistent manner, since another employee who was discovered to have also
breached the policy was not disciplined at all.

The labour arbitrator concluded that, despite the fact the employee's conduct was improper and in
clear breach of company policy, the employee's dismissal was determined to be inappropriate in the
circumstances due to the failure to enforce prior policy breaches by employees and in light of the

\(^{133}\) 2009 NBCA 62.


\(^{135}\) *Supra*, note 47.

inconsistent discipline given to employees who had breached the policy in a similar manner to the dismissed employee. The employee was ordered reinstated as a result.

Similarly, in White v. Enterprise Rent-A-Car Ltd an employee was terminated for a "violation of company policy". In determining whether the employer had just cause for dismissal, the Court noted that the company "had a history of policy breaches by its employees" and that such breaches were "widespread". The Court also noted that the company had not established that it had enforced its policies in a consistent manner, or that it had been brought to the attention of the dismissed employee that the penalty for failing to follow company policy was dismissal. As a result, the Court concluded that the employer was not warranted in dismissing the employee for a breach of company policy and awarded damages.

The effect of inconsistent enforcement of a corporate technology policy was considered in Re Owens-Corning Canada Inc., and C.E.P., Loc. 728. All employees were required to acknowledge their understanding of the employer's Internet use policy before being granted access to the Internet. Subsequently, there was found to be widespread abuse of the Internet among employees resulting in a collective warning issued and the suspension of several employees. An employee (the Grievor) was found to have breached the employer's Internet use policy along with several other employees and was terminated as a result. However, despite the fact that other employees also had breached the Internet use policy after the collective warning, the Grievor was the only employee to be terminated. In considering whether the termination of Grievor was proper, the arbitrator concluded that the employer had treated the Grievor in a significantly harsher fashion than other employees and stated:

> Where, as in the present case, an employee can show that other employee(s) who engaged in the same conduct suffered no discipline, or much less severe punishment, arbitrators generally will find the employer to have discriminated against the employee, or to have acted in an arbitrary manner.

As a result, the arbitrator found the employer's response to be excessive and substituted the termination of the Grievor with a suspension only.

Conversely, where an employer has consistently enforced a corporate technology policy and where the breach of policy is sufficiently serious, the employer may be warranted in summarily dismissing the employee for just cause. In the Poliquin case mentioned above, the plaintiff was a senior supervisor with the defendant, and had both viewed and transmitted pornographic and racist material to parties outside of the company over several years, in breach of the company's code of conduct. Once the misconduct was discovered, the employee was given a formal warning. The employee nonetheless continued to misuse his Internet access in breach of the code of conduct and

---

137 2005 ABPC 178.
138 Ibid., at para. 2.
139 Ibid., at para. 11.
140 Ibid., at para. 29.
142 Ibid., at para. 106.
143 Supra, note 81.
was subsequently dismissed. In determining whether the employer had just cause for dismissal, the Court rejected that the employer had condoned the improper behaviour of the employee or that there was a "culture of permissiveness" regarding pornography in the workplace, since the employee had both read and acknowledged the employer's code of conduct and already been warned about misusing his Internet access. Therefore, as a result of the employee's serious continual breaches of the policy, the Court found that the employer had established cause for dismissal.

The principle of "progressive discipline" requires that, in situations involving employee misconduct other than in the most egregious cases, a series of disciplinary measures must be taken before an employee may be dismissed for just cause. The principle of progressive discipline is especially relevant to the enforcement of corporate technology policies, and applicable regardless of whether the employer has adopted a zero-tolerance policy with respect to the misuse of such technology equipment. The arbitration board in Hamilton Health Sciences v. Canadian Union of Public Employees Local 4800 commented on the applicability of the principle of progressive discipline in response to a breach of policy by an employee:

Employers are both entitled and right to prohibit this sort of activity and to adopt a "zero-tolerance" approach to this sort of misuse of their equipment. ... But zero-tolerance means that the particular misconduct is never tolerated. It does not mean that the maximum penalty of discharge is appropriate in every case of abuse. The principles of corrective and progressive discipline apply even in cases of serious misconduct that no employer can be expected to tolerate. It is well established that the ultimate penalty of discharge should only be imposed as a last resort, when there is no reasonable prospect that any lesser penalty would be sufficient to both provide sufficient correction and deterrence, and protect the legitimate interests of the employer. Thus is as true of cases where the misconduct is misuse of the employer's computer system, whether or not during working hours, as it is for other kinds of serious misconduct. (emphasis added)

In Hamilton, the board of arbitration found that an employee who had been dismissed for breaching the Hospital's Internet use policy was not specifically made aware of the policy or warned that misuse of the Hospital's computers would result in significant discipline. Further, the arbitration board concluded that the Hospital had not given consideration to "all of the circumstances" of the case, including the likelihood of success of progressive discipline. The employee was ordered to be reinstated as a result.

Where a single act of misconduct (such as breach of a company technology policy) is insufficient to warrant just cause for dismissal, based on the principles of progressive discipline, an employer may establish just cause by proving:

---

144 Supra, note 81 at para. 71.
146 Ibid., at para. 37.
147 Ibid., at para. 18.
1. that reasonable standards of performance have been set and communicated to the employee;

2. that the employee was warned clearly that his or her continued employment was in jeopardy if such standards were not met;

3. a reasonable period of time was given to the employee to meet such standards; and

4. the employee did not meet those standards.\textsuperscript{148}

For instance, in \textit{Westcoast Energy Inc. and C.E.P., Local 686B (1999)}\textsuperscript{149} an employee had used a company computer to send a female co-worker several inappropriate messages, which was in clear breach of the company’s policy regarding computer use. The employee was terminated as a result. The employee challenged his dismissal, and at the subsequent arbitration the labour arbitrator emphasized the fact that the company had been "lax" in its enforcement of its policy, and that the employee did not have any prior instances of misconduct. As a result, the arbitrator concluded that the approach of progressive discipline was appropriate in the circumstances and ordered the employee to be reinstated.

In \textit{Canadian National Railway Co. v. National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-TCA) Local 100 (McConnell Grievance)}\textsuperscript{150}, a 27-year employee (the Grievor) was terminated for violating the employer's computer policies by downloading pornographic materials onto his computer. The arbitrator had found that the employee had not been disciplined at any point prior to his discharge for breach of company policy. In determining whether the dismissal of the employee was warranted, the arbitrator noted:

\begin{quote}
To support the discharge of a twenty-seven year employee an employer must establish that the discharge is justified as the next step in a system of progressive discipline, or that the misconduct is so grave as to justify dismissal regardless of the employee's record.\textsuperscript{151}
\end{quote}

After looking at the entirety of the circumstances, the arbitrator emphasized the long service of the employee, and his otherwise clean record that had not warranted any discipline or warnings on any prior occasions with respect to the improper content of his computer. Further, in light of the principles of progressive discipline, the arbitrator concluded that the dismissal of the employee for what was considered to be his "first infraction" (due to the failure to warn) was unreasonable in the circumstances. The employee was reinstated as a result.\textsuperscript{152}

Conversely, where an employee has been terminated for breach of a corporate policy, the fact that on prior occasions the policy has been enforced in a consistent and fair manner, has been taken into account by the courts in support of a finding that the employer had just cause for dismissal. In \textit{Krain v. Toronto-Dominion Bank}\textsuperscript{153} the employee, Mr. Krain, was dismissed for inappropriate use of his


\textsuperscript{149} (1999), 84 L.A.C. (4th) 185.


\textsuperscript{151} \textit{Ibid.}, at para. 11.

\textsuperscript{152} \textit{Ibid.}, at paras.: 13-14.

work computer (downloading pornographic material, downloading software, games and movies, copying pirated software) contrary to the employer's Internet use policy. Mr. Krain argued that he received no warnings in response to his prior breaches of the company's policy and that he had a right to progressive discipline before being terminated. In response, arbitrator Luborsky concluded:

This is a case of the existence of reasonably clear rules, that were within the legitimate interest of the Employer, which the evidence indicated were communicated or ought to have been known, monitored for compliance and consistently enforced. There was no evidence suggesting a complacent attitude by the Employer that might have lulled the Complainant into a false belief that his breach of the rules respecting Internet use might be condoned.”

In **Krain**, the dismissal of the employee was deemed appropriate in the circumstances.

Consistent with the principle of progressive discipline, the law is clear that condonation of employee misconduct will not be found where some form of either formal or informal discipline is handed-out to the employee in response to the misconduct. Such discipline may include reprimands or warnings, the last of which should threaten dismissal if the behaviour re-occurs. Such an approach to termination for cause is consistent with the contextual approach taken in **McKinley**.

In the case of **Backman v. Maritime Paper Products Ltd.** an employee who was dismissed for repeatedly breaching the company's computer policy by viewing pornography at work, claimed that his employer had condoned his repeated breaches of company policy and was therefore unwarranted in dismissing him for cause. In response, the Court concluded that the employer clearly had not condoned the employee's behaviour or created a lax atmosphere with respect to enforcement of the policy, since the employer had reprimanded the employee in response to each instance of misconduct and threatened termination if the misconduct continued, such that the employee clearly recognized that his behaviour was unacceptable to his employer.

Therefore it is imperative that employers consistently enforce corporate technology policies as outlined above by both making such policies known to its employees, and in responding to breaches of policy by employees. It is important that employers apply consistent sanctions against employees who breach a corporate technology policy in a similar manner and degree to one another.

**CONCLUSION**

The core lesson from the foregoing case law: a company should not bother creating corporate technology policies unless it is prepared to then monitor employee use of technology in some

---


156 2009 NBCA 62.

reasonable fashion, and then to reasonably enforce the policies according to their terms. Without these three legs to the stool, a corporation can not effectively manage its employees' use of its technology.
SECTION 1. INTRODUCTION

ABC Company (the "Company") is a leading developer and user of many communications and information technologies. These technologies, when properly used, support our business activities and enable closer and more timely communications within the Company and with our clients. There is a continuing evolution of associated laws and conventions governing acceptable use, and careless use of electronic communication tools can have dramatic consequences, harming the Company, our clients, and our employees. These guidelines are intended to minimize the likelihood of such harm by educating our employees and by acting as the basis for written policies whose existence will serve to protect the Company in litigation and other disputes.

Company business units should adopt and communicate a formal "policy" based on these guidelines that is appropriate for their own needs (e.g., reflecting different product lines, business conditions, employee populations, countries, and laws). Please direct any questions to your local IT, Electronic Commerce and/or legal departments.

These guidelines address the appropriate use of electronic "communications tools" at the Company. These tools include the following:

- Company-supplied telephones, pagers, personal digital organizers, and voice-mail facilities;
- E-mail accounts;
- Company-supplied fax machines, modems and servers;
- Company-supplied computers; and
- Company-supplied network tools (like browsers and Internet access facilities).

Commentary:

The introductory language of Section 1 is useful in explaining why an electronic communications policy is necessary for the employer, and how the terms of the policy are reasonable. Under Canadian law employers do not have an unlimited discretion to adopt workplace policies or to make such policies terms of their employment contracts. Where an employer takes action pursuant to such a policy (e.g. by
terminating or disciplining an employee for a violation thereof) the courts are prepared to scrutinize the reasonableness of the policy to determine whether it is rationally connected to furthering the legitimate interests of the employer. By explaining how it may be adversely affected by breaches of the policy, the employer illustrates that the obligations being imposed upon employees are not capricious or arbitrary.

SECTION 2. USE AND MISUSE OF COMMUNICATIONS TOOL

2.0 Access. Access to Company communications tools is provided in conjunction with the Company's business and your job responsibilities. Your use of these tools is subject to this policy and to other Company policies and procedures. Company communications tools also may be made available to individuals who are not Company employees (e.g., members of the Company Spouses Association; and subcontractors, temporaries, customers and vendors). Use of these tools by such persons is subject to this policy and to applicable agreement(s) (e.g., the Non-Employee Access Agreement, and the Company Spouses Association Agreement.).

Communications tools and all messages produced or carried by such tools are Company property, subject to reasonable Company inspection.

Commentary:

It is useful to stress that the communications tools are the property of the employer in order to preserve the employer's right of access. Securing the employee's acknowledgement that the communication tools belong to the employer will support an argument that monitoring the use of such equipment does not constitute an invasion of the employee's privacy, or the employee had consented to surveillance as a term of the contract of employment. This acknowledgment also provides a foundation for the legitimacy of rules imposed in respect of the employees' use of these tools.

Although Section 2 asserts that use of the company's communications tools "is subject to this policy," there may be a risk that this statement is insufficient to make the policy, and the employees' obligations to comply therewith, a term of the employment contract. The introduction of a new workplace policy that imposes new obligations and gives the employer new grounds for discipline or dismissal, however, can be seen as a variation of the existing employment contract. To make the policy binding upon the employee there must be some evidence that the employee agreed to this new term of the employment contract. Simple awareness of the policy is not enough; a policy does not become a term of the employment contract merely because it is published and distributed to employees. An employee cannot be taken to have agreed to the policy simply because he or she continues to work after the employer purports to enact the policy.
Where it is concluded that the policy has not become part of the employment contract, the employer cannot rely upon breaches of the policy as grounds for discipline or dismissal. In such circumstances, the employer is left with the task of establishing that the impugned conduct constitutes cause at common law. Accordingly, it may be preferable to go beyond what is currently included in Section 2 and require employees to execute some form of document acknowledging their awareness of the policy and their agreement to be bound by its terms.

2.1 Acceptable Use. In the course of your job, you may use these communications tools to communicate internally with Company coworkers or externally with customers, consultants, vendors, and other business acquaintances. The Company provides you with electronic communications tools to facilitate business communications and to enhance your productivity. As with the telephone, there may be occasion to use these facilities for personal purposes. Personal use is permitted so long as it does not interfere with the performance of your job, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other employees. Under no circumstances shall such facilities be used for personal financial gain, or to solicit others for activities unrelated to the Company's business, or in connection with political campaigns or lobbying. The local Personnel Department may make available or otherwise authorize special-purpose bulletin boards and web pages enabling employees to market and sell personal property (other than for-profit), and in connection with Company-approved social events, sporting events, and other sanctioned activities. When making use of these Company-provided facilities for personal use, always remember that you have a very limited expectation of privacy (see discussion below).

In addition to other restrictions and conditions discussed here, you may not use any communications tool:

• to carry any defamatory, discriminatory, or obscene material;

• in connection with any infringement of another person's intellectual property rights (e.g., copyrights);

• in a manner that violates the terms of any applicable telecommunications license or any laws governing transborder data flow (e.g., laws dealing with data collection, protection, privacy, confidentiality or security);

• in connection with any attempt to penetrate computer or network security of any Company or other system, or to gain unauthorized access (or attempted access) to any other person's computer, e-mail, voice-mail accounts or equipment;

• in connection with the violation or attempted violation of any other law;

• to send confidential information without the proper protections;

• to express personal opinion as Company opinion;

• to share jokes, send chain letters or solicitations;
• to mislead the recipient of any message as to the actual identity of the sender, or
• to waste time on excessive personal use.

The Company understands that web "surfing" may be business-related and serve a legitimate business function, but the potential for abuse exists. The Internet provides access to a huge amount of information and resources that can greatly enhance our ability to deliver services efficiently to our customers. Today there is no single, comprehensive directory of resources available for the Internet and users sometimes must "navigate" through much unneeded information to reach useful material. The Company encourages exploration of the Internet for legitimate business-related or professional activities, but you should avoid "browsing the web" on Company time, creating personal "Home Pages," or otherwise using Company facilities to access Internet sites for reasons unrelated to the Company's business and your job responsibilities.

Commentary:

The express prohibitions of certain types of use by employees serves a number of interrelated purposes. First, it serves an informational purpose by letting employees know that certain uses of communications tools are matters that may have adverse consequences for the employer and which the employer has a legitimate interest in prohibiting. Second, it serves a preventative function, hopefully discouraging employees from engaging in the prohibited conduct. Third, if this is unsuccessful, and the employee does use the communications tools for prohibited purposes, this may constitute a breach of the employment contract justifying disciplinary action or (if the policy does not form a term of the employment contract) it may establish that the misconduct constitutes "just cause" at common law warranting action on the employer's part. Last, prohibiting certain uses distances these acts from the employer possibly affording a defence in any litigation seeking to ascribe vicarious liability for the employee's actions.

With regard to this last point, however, it should be noted that there are limitations to the efficacy of a workplace prohibition. Under Canadian law an employer may be held vicariously liable for the acts of its employees when those acts are performed by the employee "in the course of" his or her employment. The focus is upon the employee's actions rather than the way in which they were performed. Where the employee performs a task on behalf of, or for the benefit of, the employer, the employee's conduct remains within the course of his or her employment even if the task is performed in a negligent or prohibited manner. Indeed, if this were not the case, the doctrine of vicarious liability would be of little significance.

Because of this, the employer is generally unable to shield itself from liability simply by expressly prohibiting certain conduct on the part of its employees. This is not limited to such obvious examples as a prohibition
against performing job tasks negligently. Even where the conduct is expressly prohibited or unauthorized, if it is done as part of the employer's business the employer will be liable. On the other hand, a prohibition expressed as a term of the contract of employment may serve to delineate the "course of employment" so that acts in breach of the prohibition are outside the employment relationship and the employer is not liable for any harm caused thereby.

Accordingly, the fact that the policy prohibits defamatory content in e-mails, or prohibits the infringement of copyrights will be of less significance than the purpose for which such prohibited acts are performed. For example, if an employee downloads copyrighted material from the Internet to plan his or her vacation, the employer may not be vicariously liable for any infringement. If the material was downloaded for the purpose of preparing a report in connection with the employer's business, liability would likely be found notwithstanding the fact that the employee was prohibited from performing his or her job in this way.

2.2 Representing the Company in Your Postings. The information you publish electronically (sometimes called a "posting") reflects on the Company in general. Despite all disclaimers that you make (e.g., that your views are your own and may not reflect those of your employer) readers elsewhere will make the association between your posting and the Company. You should know that true anonymity is very difficult to obtain when using these tools. While Internet relay chat, newsgroup visits, and net "surfing" sometimes appears to be done anonymously (e.g., by employing pseudonyms), accessing such services/servers through the Company's network facilities normally leaves an "audit trail" indicating at least the identity of the Company proxy/server (and may leave a trail pointing directly to you). Inappropriate use of Company facilities may damage the Company's reputation and could give rise to corporate and individual liabilities. Accordingly, you should make every effort to be professional in all usage of Company communications tools.

Certain newsgroups and industry groups relate so directly to the Company's business that you must take special care in posting to them. These newsgroups include, but are not limited to:

- [●]
- [●]
- [●]

[...]

Please ensure that your information is correct and that you have proper permission from third party contributors/author before posting any article in a newsgroup related to the Company's businesses. For topics relating to Company products or services, the appropriate marketing group, engineering manager and intellectual property lawyer should be consulted before making the posting. Postings should never reference unannounced products or unpublished details about Company technology.
Your postings also should not compare or contrast different products or customers, advocate one customer or product in favour of another, or refer to our competitors (either directly or indirectly).

Commentary:

The ability of employees to post information on bulletin board services or elsewhere has the potential to make every employee an advertiser on behalf of the company. The risk is that few employees will recognize that their postings may be regarded as "advertisements" in law and even fewer will know what constitutes a permissible advertisement for the product or service in question.

In Canada, as in most other countries, advertising is regulated by a myriad of statutes, regulations and industry codes. Perhaps the most significant are the provisions of the Competition Act that criminalize false or misleading advertisements. Several provinces have also enacted consumer protection legislation that prohibits deceptive advertising. [...] However, the foregoing legislative enactments may not present the greatest risk for employers. Even without specific knowledge of the governing legislation, it is likely that employees will be generally aware of the impermissibility of misleading advertisements and will not post untrue representations about the company's products and services in the mistaken belief that this is acceptable. The greater threat is that posed by the arcane and detailed regulations governing the advertising of particular classes of products. For example, the federal Food and Drugs Act contains provisions making it an offence to advertise any food, drug or medical device in a manner that is "false, misleading or deceptive or is likely to create an erroneous impression regarding its character, value, quantity, composition, merit, safety or other attributes." However, the meaning of "false," "misleading" and "erroneous impression" are not left open to interpretation in the same way as under other misleading advertising statutes. Rather, there are the lengthy Guide to Food Labeling and Advertising and Drugs Directorate Guidelines: Consumer Drug Advertising, published by the Ministries of Agriculture and Agri-Food Canada and Health and Welfare Canada, respectively, setting out what is required for an advertisement to comply with the obligations under the Food and Drugs Act. There are countless ways in which a seemingly innocuous posting by an employee could violate these guidelines by omitting some mandatory information or by using a particular term in a prohibited way.

[...]

2.3 Unacceptable Content. Although the Company does not regularly monitor voice-mail or electronic messages, please be aware that even personal e-mail and voice-mail messages may be viewed publicly or by Company management without further notice. Under no circumstances may
any posting, voice-mail or e-mail originating at the Company be in violation of the letter or the spirit of the Company's Equal Employment Opportunity or Sexual Harassment policies. Examples of unacceptable content include:

- sexually explicit messages, images, cartoons or jokes;
- unwelcome propositions, requests for dates or love letters;
- profanity, obscenity, slander or libel;
- ethnic, religious or racial slurs; and
- political beliefs or commentary;

or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs. As a general rule, no jokes, chain letters or solicitations are permitted.

Everyone should be aware that "sexual harassment" includes unwelcome sexual advances, unwelcome requests for sexual favours, or other unwelcome conduct (including comments) of a sexual nature. The standard for sexual harassment is whether the recipient could reasonably consider the message to be offensive - the sender's intentions are irrelevant.

In addition to prohibitions on sending or uploading offensive materials, Company communications tools (e-mail, browsers, newsreaders, etc.) also shall not be used to access or download obscene materials or other "content" that maybe illegal under local law. For example, possession and distribution of certain kinds of neo-Nazi documentation and propaganda may be unlawful in Germany, and other countries likewise may impose restrictions on possession or use of other kinds of "content."

Commentary:

Although it is perhaps prudent to include reference to an employer's prohibition of sexual harassment in its electronic communications policy, it does not appear that e-mail and the Internet raise any novel issues or problems in this area. If the employer has already instituted a comprehensive sexual harassment policy there should be little difficulty in applying it to employees' use of new communications technologies. If the policy prohibits the sexualization of the work environment through such activities as the posting of pin-ups, phrased properly, this prohibition should apply equally to suggestive screen-savers and the like; if unwelcome sexual advances are prohibited, there is no reason to believe that advances by e-mail would be excepted.

The possibility of possession and transmission of illegal content raises more serious issues for the employer. The Criminal Code of Canada prescribes prohibitions in respect of three principal classes of content: obscene material, libellous material and statements promoting hatred.
against an identifiable group. The question that is repeatedly asked is, what liability might an employer face if employees visit Internet sites displaying such materials and download them in the workplace?

 [...] 

2.4. Electronic Forgery. Electronic forgery is defined as misrepresenting your identity in any way while using electronic communications systems (e.g., by using another's e-mail account without permission, by so-called IP spoofing, or by modifying another's messages without permission). For example, messages written by others should be forwarded "as-is" and with no changes, except to the extent that you clearly indicate where you have edited the original message (for example, by using brackets [ ] to flag edited text).

Electronic forgery is not allowed for any purposes. For e-mail messages, you may not take any action to misrepresent the identity of the person responsible for the message. You may send e-mail messages using another person's account, but only with prior express approval from the account owner, and only where the text of the message indicates that you are the author.

For newsgroup postings, you may not misrepresent the identity of the sender, but you may (as may sometimes be appropriate) make postings on an anonymous basis. (Keep in mind that true anonymity may be quite hard to obtain, and that most such attempts at least leave an audit trail that identifies the Company as the source of the posting.)

2.5 Intellectual Property. The Internet offers a universe of information, useful in conducting and furthering business operations. You must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and inventions. Do not copy, use, or transfer others' materials without appropriate authorization. Be aware that downloaded software and other copyrighted material may be subject to licensing obligations or restrictions. In cases where it is possible that the software might be used by Company engineers in product development or might be incorporated into commercial products, it is critical that these licensing obligations be well-understood and strictly observed. Even when software is labelled "freeware" or "shareware" there may be retained licensing restrictions that prohibit or limit the usage or commercialization of such items.

You should also note that patent rights may exist independently of any other intellectual property rights and that this may be owned by the author of the software or even by an unrelated third party. For example, innovative algorithms or new applications may be subject to patenting, and appropriate precautions must be taken before incorporating such inventions into software to be sold or licensed.

If you have any questions in this regard, contact someone in the Company's legal department.
Commentary:

Copyright protection in Canada is exclusively a creature of statute. The Copyright Act confers exclusive rights to do or authorize certain acts upon copyright owners and deems the performance of those acts by anyone other than the copyright owner to be infringements of copyright. Among those rights are the right:

(a) to produce or reproduce the work or any substantial part thereof in any material form whatever;
(b) to perform the work or any substantial part thereof in public;
(c) in the case of a literary, dramatic or musical work, to make any record, perforated roll, cinematograph film or other contrivance by means of which the work may be mechanically performed or delivered;
(d) in the case of any literary, dramatic, musical or artistic work, to reproduce, adapt and publicly present the work as a cinematographic work;
(e) in respect of any record, perforated roll or other contrivance by means of which sounds may be mechanically reproduced, the sole right in respect of the contrivance or any substantial part thereof;
(f) to communicate the work to the public by telecommunication;
and
(g) to authorize any of the foregoing acts.

[...]

2.6 Transmitting Confidential Information. Confidential information (whether owned by the Company, its customers, its vendors, or other persons) is not to be disclosed to unauthorized persons without prior authorization. The question of "authorization" will be a function of the type and ownership of the confidential information (e.g., different authority may be required for disclosure of Company-owned information than for customer-owned information). Also, "authorization" for disclosure may be limited to certain specific individuals within the organization (e.g., on a "need-to-know" basis).

In some cases, posting or e-mailing confidential information that relates to new products or services can constitute a "publication" and prevent the Company from applying for patents or later treating the information as a "trade secret". These consequences can follow even from postings or distributions that are not to the general public.

Generally, the common-sense prohibition of casual disclosures means that confidential information should not be contained in e-mail sent to outsiders or posted to newsgroups, and should not be placed on Company communications tools that are available to third parties (e.g., unsecure notebook computers that are accessible to non-Company personnel). You should post such
information on "web pages" only when you are certain that the web page is not accessible from locations outside the Company firewall. Also, you should not set your Company e-mail account to forward automatically your e-mail to any non-Company account (e.g., to your America Online account).

Commentary:

*It is self-evident that employers must take steps to guard against the unauthorized disclosure of confidential information. The most significant risks are the practical ones: the loss of trade secrets and the loss of other proprietary information that competitors may be able to exploit. Legally, there is another risk which warrants note. The disclosure of information will result in a loss of its confidential character thereby precluding any future breach of confidence action. Such a claim requires the plaintiff to show that (a) the information had the necessary quality of confidence; (b) the information was communicated to the defendant in circumstances imparting an obligation of confidence; and (c) the defendant made unauthorized use of the information to the plaintiff's detriment. Thus, if a defendant can show that the information it has allegedly misused was, at some point, disclosed in e-mails or postings by employees of the plaintiff without regard to the information's confidential character, there is a significant risk that the plaintiff's action will fail.*

2.7 Encryption. The use of encryption tools is also governed by Company security standards and policies. In general, authorized encryption tools should be employed to protect Company confidential information on unsecured computers (e.g., notebook computers), and may be used by the various business units to encrypt information traveling by unsecured means (e.g., CD-ROM distribution or Internet transmission).

Only authorized encryption tools (software and hardware) may be used in connection with any Company communications tools. Except with the prior written consent of the appropriate IT manager, all such tools must implement key-recovery or key-escrow techniques to permit the Company to access and recover all encrypted information (e.g., in the case of the absence of the employee who performed the encryption).

Please remember that possession and use of encryption tools may be subject to complex laws or outright local prohibitions. Also, the export and import of computers carrying such tools may be subject to local regulation.

2.8. Unsolicited E-mail. If you are using the Company system to send e-mail to potential customers to attract new business, please contact the legal department prior to sending any message to a third party in which no prior business relationship exists. Various regulations exist regarding unsolicited e-mail and vary depending on where you message is being sent.

2.9. Consequences of Misuse. Misuse of any Company communications tool or violations of these guidelines may result in disciplinary action up to and including termination from the Company.
Commentary:

It is valuable to include an express provision allowing for discipline or dismissal in the event of breaches of the electronic communications policy. Where the employer merely prescribes a policy and fails to provide the consequences for any violation it may be difficult to rely upon such a violation as grounds for disciplinary action, particularly dismissal. A breach of the employer's directives would constitute misconduct, but whether that misconduct was serious enough to constitute cause for dismissal at common law would remain a matter to be determined by the court or an arbitrator. In essence, the employer is required to show that the violation of the policy represents a fundamental breach of the employment contract entitling the employer to treat the contract as at an end. This exceptionally high standard does not have to be met where an employer seeks to exercise a contractual power of dismissal; the employer need only show that the contractual preconditions for the exercise of the power have been met. Where a breach of the policy authorizes termination, the employer need only show that the employee breached the policy.

While the foregoing is generally accurate, it is likely that in a case where the employee argues that the dismissal was wrongful, the court will assess the reasonableness of the policy and the employer's actions. If an employer were to respond to a minor violation with summary dismissal and without offering the employee an opportunity to explain his or her actions, the court might well conclude that the contract confers no such power upon the employer. The court might interpret the provision as empowering the employer to dismiss the employee only for acts that can be shown to seriously adversely affect the employer's business.

Again, as discussed above, to maximize the efficacy of a provision such as that in Section 2.9 it is necessary to ensure that it is not only brought to the attention of all employees, but that it becomes a term of the employment contract. To achieve this objective, it is perhaps preferable that employees be required to return a signed acknowledgement of the policy. It is also necessary that the employer enforce the policy: if an employer merely pronounces a policy but then tolerates breaches thereof, the policy may lose its effectiveness and the employer may not be able to invoke the policy as grounds for discipline or dismissal.

SECTION 3. LIMITS OF PRIVACY

3.0. Retention and Security of Messages. E-mail and voice-mail messages, and computer-stored items all are Company property and business records, and may have legal and operational effect identical to that of traditional, hardcopy documents (e.g., they are "discoverable" in litigation, and can be used in evidence). Accordingly, all e-mail messages should be treated as though they may
later be viewed by others (while confidential information may be contained in such messages, these messages should be created with the same care you would use in creating hardcopy documents).

Remember that no electronic communications facility is completely secure. This means that information stored on or carried over Company communications tools may be the subject of accidental or intentional interception, misdelivery, attack, or authorized Company review.

When stored on computers, e-mail messages and other files typically are subject to routine back-up procedures. This means that copies of these files may be retained for long periods of time (in accordance with back-up recycling and document retention procedures). Also, keep in mind that many site-wide backup systems do not guarantee privacy of backup copies (e.g., system administrators may have access).

3.1 A Limited Expectation of Privacy. The Company respects the personal privacy of its employees. However, because communications tools are provided for the Company's business purposes, employee rights of privacy in this context are quite limited. Employees and others should have no expectation that any information transmitted over Company facilities or stored on Company-owned computers is or will remain private. These systems are owned and/or controlled by the Company and are accessible at all times by the Company for maintenance, upgrades, or any other business or legal purposes. Employees who use Company communications tools should be aware that our firewall (and other security tools) creates an audit log detailing every request for access in either direction by each user. Also, in the course of their duties, system operators and managers may monitor employee use of the Internet or review the contents of stored or transmitted data.

The Company permits personal use of all these communications tools on the express understanding that it reserves the right (for its business purposes or as may be required by law) to review employee use of, and to inspect all material created by or stored on, these communications tools. Use of these tools constitutes each employee's permission for the Company to monitor communications and to access files that are made on or with these communications tools.

Commentary:

Canadian case law has confirmed that e-mail messages and other communications in electronic form will be treated in the same way as their paper-based counterparts. Courts have treated e-mail messages as among the documents to be produced in discovery before trial without any suggestion that the technological differences called for different treatment under the applicable rules of civil procedure.

3.2. Company Access to Computers, Voice-mail and E-Mail Systems. Company management will not routinely examine employees' communications or files. However, such examination generally may be expected to occur in the following circumstances (that are not intended to be all-inclusive):

- ensuring that Company systems are not being used to transmit discriminatory or offensive messages, or in connection with the infringement or violation of any other person's rights;
- determining the presence of illegal material or unlicensed software;
• counteracting theft or espionage;
• ensuring that communications tools are not being used for inappropriate purposes;
• responding to legal proceedings that call for producing electronically-stored evidence;
• locating, accessing, and retrieving information in an employee's absence;
• investigating indications of impropriety; and
• to manage, operate and resolve issues associated with the ownership and operation of the system.

All such examination is subject to prior review and approval by senior management of the associated operating company.

SECTION 4. QUESTIONS/CHANGES TO POLICIES

Questions about this policy may be directed to personnel in the IT and/or the legal departments. The Company intends generally to observe these policies but also reserves the right to change them at any time without prior notice. The Company will make reasonable efforts to provide notice of such changes by postings to the appropriate web page, <http://www.it.ABCco.com/poli>.

This Paper contains statements of general principles and does not constitute legal advice or opinion. Readers are advised to consult with a lawyer for specific analysis and advice in relation to any particular matter. E&OE.