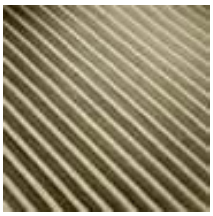
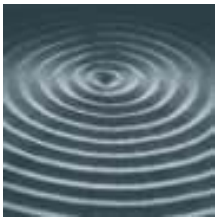


2500, 20 Queen St. West
Toronto, ON M5H 3S1
Canada
Tel. 416.595.8500
Fax.416.595.8695
www.millerthomson.com



MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents

TORONTO VANCOUVER WHITEHORSE CALGARY EDMONTON WATERLOO-WELLINGTON MARKHAM MONTRÉAL

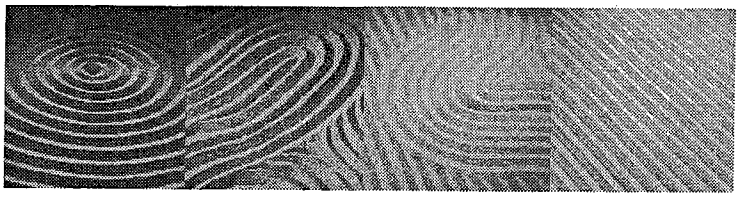
From Cyber-Slacking to Cyber-Stalking: Dealing With Internet Abuse in the Workplace

Stuart E. Rudner and
Laura Cassiani

November 26, 2004

MILLER THOMSON LLP

Barristers & Solicitors, Patent & Trade-Mark Agents



FROM CYBER-SLACKING TO CYBER-STALKING:

DEALING WITH INTERNET ABUSE

IN THE WORKPLACE

Stuart E. Rudner
and
Laura Cassiani (student-at-law)
Miller Thomson LLP
416.595.8500
www.millerthomson.ca

FIFTH ANNUAL

EMPLOYMENT LAW SUMMIT

NOVEMBER 26, 2004

CONTENTS

INTRODUCTION

Three years ago a Canadian teenager made headlines across North America when a computer virus he implanted on the internet to detect downloaders of child pornography nabbed a California Superior Court judge. The judge had been downloading images of child pornography onto both his workplace and home computers. Interestingly, in that same year, a judge in the Ninth Circuit Court of Appeals in San Francisco had successfully protested when the government proposed to use a monitoring program to detect "unauthorized" internet activity by federal court employees, including judges.

Internet abuse by employees – in every profession, in every rank, and of every nature – is a serious problem for employers seeking at once to integrate the internet as a high efficiency business tool and at the same time manage its alluring, non-work related temptations. While the internet and email access have increased the speed of doing business and lowered its cost, they have also introduced a potential minefield that lurks behind every computer screen. As one author described it, "[m]any times, internet access is an open invitation to waste time."[1]

The types of inappropriate internet and email usage span a wide spectrum, from "cyber-slacking" to "cyber-stalking". In between, one can find online gaming and gambling, pornography (which covers its own spectrum from "merely" inappropriate to repugnant), chat rooms, hate sites, and copyright violations. Without adequate systems in place to monitor employee use of email and the internet, most employers will be completely unaware of the abuse taking place under their

[1] G. Taillon, "Controlling Internet Use in the Workplace" *The CPA Journal*, online: NYSSCPA <http://www.nysscpa.org/cpajournal/2004/704/perspectives/p16.htm>. [Date accessed: October 15, 2004].

watch and on their equipment. As Howard Levitt described in the *National Post*, such behaviour can be "silent and, superficially, undetectable."[2]

This paper will examine some of the common forms of internet and email abuse that employers should be aware of, what employers can do to effectively monitor internet use in the workplace, and what the courts and arbitrators have said about disciplining employees for abusing the internet and email. The paper is divided into the following topics:

1) Context – The Extent of the Problem

2) Types of Internet-Related Abuse

3) The Employer's Cyber-Protection: Effective Policies, Monitoring and Enforcement

4) Disciplining the Cyberslackers

CONTEXT – THE EXTENT OF THE PROBLEM

Use of email and the internet has increased exponentially in recent years. There is an American study which estimates that "approximately 40 million employees use email" and that this figure is likely to increase by nearly 20% every year."[3] One report estimates that by 2005, there will be 36 billion email messages sent each day[4]. These numbers also reflect the Canadian trend; for example, 62% in a national survey reported that they prefer to communicate via email rather than through any other method.[5]

Use of email and the internet has also exploded in the workplace. Many, if not most, workplaces provide monitors at desks or stations. Many also provide at least some employees with wireless devices such as notebook computers, palm pilots and blackberries. Three years ago, according to Statistics Canada, 57% of Canadian employees used a computer at their job[6]. The numbers are undoubtedly much higher now.

More and more North American employees have at least some degree of internet access at work. While the intention is obviously for employees to use this access for work purposes, the reality is often quite different. Some have estimated that as much as 25 to 40% of the time that employees

---

[2] Howard Levitt, "Why you need a policy on worker email: Misconduct not always obvious from observation" *The National Post* (24 November 2003) at FP10.

[3] Edward Hertenstein, "Electronic Monitoring in the Workplace: How Arbitrators Have Ruled" (1997) 52 Dispute Resolution Journal 36 at 37 [Hertenstein], cited in Janis Sarra, "Employee Use of E-Mail and the Internet: An Arbitrator's Perspective" in Kevin Whitaker, eds., *Labour Arbitration Yearbook 2001-2002* (Toronto: Lancaster House, 2002) 11 at 12. [Sarra].

[4] Sally Chan, "e-Risks: What to consider when creating your email risk management policies" (November 2002) 76 *CMA Management* at 45.

[5] Ipsos Reid, "The Canadian Internet Fact Guide" (January 2002).

[6] Statistics Canada, *Perspectives on Labour and Income*, 2001, online: www.statcan.ca, cited in J. Birrell & D. Aaron "Controlling Internet Use and Abuse: Stalking the Cyberslacker" (*Employee Terminations: All the Legal Information, Advice and Strategic Know-How You Require to Manage Dismissal*, November 19-20, 2001) Insight Information. [Birrell & Aaron].

spend on the internet at work is for personal use.[7] As will be discussed below, this "personal use" can be anything from online banking to hard-core pornography. Regardless of what the employees are doing, when they are not working, it is the employer that suffers. For example, an Ipsos Reid survey found that in Canada, 800 million working hours are wasted each year because employees are using the internet at work for personal reasons.[8]

The cost to employers of online abuse is as significant as, for example, absenteeism. A survey of small and medium-sized businesses in Great Britain found that 30% are losing more than a day's work (10 hours) per week due to non-work related internet and email use. According to the same survey, 61% of those employers lost up to 2 hours per work week.[9] For a specific example, when the Starr Report, which probed the controversy surrounding the possible impeachment of former U.S. President Bill Clinton, was released on the internet, 13.5 million employees accessed it, costing U.S. businesses a reported $500 million (U.S.) in lost productivity.[10]

The numbers are significant, and examples of workplace internet abuse are becoming all too common. Consider the following:

- A 2003 survey conducted in the U.K. found that approximately a third of employers had handled "up to five disciplinary cases" relating to internet abuse by employees that year[11];

- A 2002 survey conducted by the U.K.-based Personnel Magazine reported that 25% of responding companies had terminated employees for internet abuse. Most of these employees had been using their employer's internet to access pornography[12];

- According to a 2001 study by the American Management Association,[13] 15% of responding employers said they had dealt with some legal action due to employee misuse of email or the internet[14];

- In 2000, the results of an internal study of internet activity by employees in Canada's Department of Fisheries and Oceans revealed that at least 10% of employees' internet

---

[7] Cited in Gabriel Somjen and Michael Birch, "Privacy Issues in the Workplace: Use and Abuse of internet and E-Mail" (*Employee Terminations: All the Legal Information, Advice and Strategic Know-How You Require to Manage Dismissal*, October 29-30, 2001) Insight Information.

[8] *Ibid.*

[9] BBC News "Internet abuse costs big money" (1 November 2002), online: http://news.bbc.co.uk/1/hi/technology/2381123.stm [Date accessed: October 15, 2004].

[10] Cited in Nancy Flynn *The E-Policy Handbook: Designing and Implementing Effective E-Mail, internet, and Software Policies*, (New York: AMACOM, 2001). [Flynn].

[11] BBC News "Firms face up to internet abuse" (10 November 2003), online: http://news.bbc.co.uk/2/hi/business/3256753.stm [Date accessed: October 15, 2004].

[12] Cited in Peter Churchman, "Technology Abusing the Net – How to curb work surfers" *New Zealand Management* September 2003 at 46. [Churchman].

[13] AMA, *Workplace Monitoring & Surveillance: Policies and Practices* (2001), online: www.amanet.org/research.

[14] AMA, *Workplace Monitoring & Surveillance: Policies and Practices* (2001), online: www.amanet.org/research.

use during work hours was spent visiting non-work related sites. During one work week, employees visited sex and dating web sites an average of seven times a day[15];

- In 2001, sixty-six government employees of the Ministry of Natural Resources were disciplined after an internal investigation by the Ministry found that emails, some containing images of bestiality and violent acts against women, had been sent and received by employees. While only 66 employees were ultimately disciplined, the Ministry's investigation determined that 189 employees had sent and received emails of this nature[16];

- In 1999, a prominent daily New York newspaper terminated 23 employees and gave warning letters to another 20 for their internet abuse. Employees who were terminated had distributed "offensive" emails, some of which contained sex-related material, and the others had simply been the recipients of these emails but had not re-circulated them[17];

- Some studies have suggested that online pornography sites get more hits during the hours of the "normal" workday than any other time of the day[18];

- Studies suggest that workplace harassment is one of the most prevalent forms of email abuse.[19] The AMA found that more than a quarter of American Fortune 500 employers have had to deal with "sexual harassment claims arising from employee abuse of corporate email and internet systems."[20]

Internet abuse and misuse in the workplace can have a serious financial and legal impact on employers. It can impact on productivity levels and result in lost revenues and increased costs to the employer. If left unchecked, it can allow a permissive and toxic culture to develop which can ultimately lead to more egregious behaviour and also impede efforts to discipline employees.

Furthermore, internet and email abuse can expose the employer to liability for offences such as harassment and copyright infringement. Companies can also become entangled in criminal investigations where illegal material, such as child pornography, has been accessed. Improper use can also have a negative impact on a corporate reputation, such as where an employee uses

---

[15] Russell Albert and Karen McBean, "Employee Use of E-Mail and the internet: A Management Perspective" in Kevin Whitaker, eds., *Labour Arbitration Yearbook 2001-2002* (Toronto: Lancaster House, 2002) 33 at 34. [Albert and McBean].

[16] [2004] O.G.S.B.A. No. 97.

[17] *Ibid.*

[18] "Computer Use Policy, internet Use Policy, Information Use Policy – A Guide to Drafting Comprehensive and Effective Computer Policies" April 13, 1999, online: http://www.computer-policy.com, cited in Scott Williams and Lior Samfiru "Balancing Employer and Employee Rights in the Wired Workplace" (Privacy Laws and Effective Workplace Investigations, January 30-31, 2003) Insight Information. [Williams and Samfiru].

[19] Albert and McBean *supra* note 15 at 35.

[20] Cited in Churchman *supra* note 12.

her employer's email account – a publicly-owned, high-profile corporation – to handle her exotic dancer recruitment business.[21]

All of these issues can affect the bottom line in one way or another, whether it be due to a loss of productivity or due to a claim made against the company.

TYPES OF INTERNET-RELATED ABUSE

Although the case law and arbitral jurisprudence has dealt predominantly with employees accessing pornographic web sites, it is clear that the workforce is not limiting its online appetite to this type of activity. The high-speed nature and global breadth of the internet and email make it all the more critical for employers to be aware of all forms of non-work related online activity. If you are not aware of them, you cannot adapt your policies to reference them, and you cannot monitor them.

The results of a survey conducted in 2000 by Vault.com are illustrative of the wide range of use and abuse that is taking place. The employees surveyed indicated that they surf the internet at work for the following non-work related purposes:

- 72.1% to read the news
- 45.2% to make travel arrangements
- 40.1% to make purchases
- 36.8% to look for other jobs
- 36.6% for "special interests" (hobbies, etc.)
- 33.5% to check stocks
- 27.5% to make social plans
- 25.7% to instant message
- 13.3% to download music
- 10.6% to play games
- 9.1% to "chat" (i.e., chat rooms)

---

[21] See *Ontario Power Generation Inc. and Power Workers' Union* (2004), 125 L.A.C. (4th) 286. (*Ontario Power Generation*). In that case, Arbitrator Swan noted the following:

> The exotic dancer business is not, however, just any private business. It is, on all of the evidence before me, a perfectly legal business, involving the regular immigration process to issue employment visas for work that, at least in general, is permitted by law. But again, rightly or wrongly, there can be no doubt that a substantial body of public opinion would find this particular business distasteful, and its conduct from the offices of a publicly owned corporation intolerable.

- 4.0% to access pornography[22]

Despite the fact that this was a self-reporting survey, it is nonetheless indicative of the extensive list of temptations looming in cyberspace to compete with actual work for your employees' attention. And it does not even include two forms of abuse that have been the subject of reported discipline: the downloading of copyrighted material and the use of email to harass others

While most cases deal with employees abusing the internet or email systems while at their place of work, it should also be recognized that many employees can now access, and abuse, the internet using company equipment while away from the office. Employees that telecommute, and work at home using corporate computers and networks, are a prime example. So too are employees that use company notebook computers, blackberries and Pocket PCs, all of which have the capability to access the internet and send and receive email messages.

To a certain extent, this was recognized by the arbitrator in the case of *British Columbia v. B.C.G.E.U. (Maddison Grievance).*[23] In that case, the grievor had been given a one day suspension after the employer discovered that the employee had been accessing "offensive" sites using the computer that was provided by the employer, although he had done so in the comfort of his own home using a company-provided laptop computer.

Excessive Personal Use – How much is too much?

Most employers permit their employees to use the internet at work for personal reasons, at least to some extent. These employers have undoubtedly accepted the reality that Canadians rely on the internet to help them manage the daily minutia of their personal lives, such as paying bills, ordering groceries, making travel arrangements, purchasing gifts, and communicating with family, especially as they devote more time to work outside of the home.

Given people's significant reliance on the internet, it is unlikely that a zero-tolerance approach to personal use at work will be a wise, or realistic, business choice for most employers. In this regard, the internet is no different than the telephone. It is unlikely that a trier of fact would find a zero-tolerance policy to be reasonable; it is widely accepted the employees will use the telephone occasionally for personal matters, without repercussion. Email and the internet should be treated in the same manner. As D. Rogers states:

> Some employers may be tempted to limit liability and curb employee misuse of computers, e-mail and the Internet by prohibiting personal use altogether. Although such a strategy may have superficial appeal as a straightforward solution, employers will find it unworkable in most circumstances.
>
> Most employees would reasonably expect that during a productive workday, a limited amount of time spent on inoffensive personal use of e-mail and the Internet would be acceptable. Indeed, many employees look forward to taking such time during their break periods, a practice which need not have any adverse effect on their employers.

---

[22] Fall 2000, "Results of Vault.com Survey of internet Use in the Workplace" Vault.com, online: http://www.vault.com/surveys/internetuse2000/results2000.jsp?results=12&image=employee [Date accessed: October 15, 2004].

[23] [1998] B.C.C.A.A.A. No. 535.

> The imposition of a "zero personal use" policy would offend the sensibilities of loyal and conscientious workers. One would expect that such a policy could contribute to a workplace environment of resentment, and that the resulting decline in morale could very well cause productivity to suffer.
>
> In addition to employee disapproval, employers seeking to prohibit all personal use of computers, e-mail and the Internet would also face serious policing and enforcement problems. In order to ensure compliance with such a strict policy, an employer would likely be forced to invest a prohibitive amount of time and money in monitoring its employees. Furthermore, the required level of monitoring would almost certainly be so intrusive as to be intolerable.[24]

Arguably, employers who allow some form of personal use during work hours may be creating a more productive workplace, as employees will have fewer reasons to take the time to physically leave the office to tend to their personal errands, such as standing in line at a bank. An example of corporate recognition of this dynamic can be found in the internet policies in place in the case of *Owens-Corning Canada Inc. and C.E.P., Local 728 (Gorgichuk)*,[25] which provided the following:

> As with other corporate assets, the Internet and e-mail are to be used for business purposes. However, many of us work extended hours, both at home and in the office or travel extensively. We need to balance our work lives with our personal and social lives. The Internet can help us stay connected with family and friends, and contribute to improved quality of life. We expect you to use it responsibly, such that this use does not interfere with business use of the service and the performance of our jobs.

However, whether and to what extent to allow personal access to the internet, as Albert et al. suggest, is ultimately a business decision.[26] An employer will have to consider a number of factors before deciding how much personal use to allow employees while they are "on the clock". Such considerations could include the nature of the workplace, any built-in physical constraints, the availability of computer terminals and networks, the type of work being done, health and safety issues and, ultimately, cost. The goal is to allow some use without losing significant productivity or exposing the company to vicarious liability for inappropriate activity.

A review of the case law makes it clear that personal use does not have to include accessing or distributing "inappropriate" material in order to warrant discipline. "Cyber-slacking" is a modern variation of an age-old problem: employees who spend their time doing anything but working. In some ways, technology has made this even easier, as employees don't even have to leave their desks to find non-work related ways to entertain themselves. The question, of course, is how much is too much?

Consider the case of *Mount Royal College and Mount Royal Support Staff Assn. (Horan Grievance)*,[27] where the grievor was dismissed due to excessive use of the employer's resources

---

[24] Derek L. Rogers "Terminations Due to Improper Use of Technology: Whose Business is it Anyway?" (*Employee Terminations: All the Legal Information, Advice and Strategic Know-How you Require to Manage Dismissals*, April 11-12, 2002) Insight Information.

[25] (2002), 113 L.A.C. (4th) 97. (*Owens-Corning*).

[26] Albert and McBean *supra* note 15.

[27] [1998] A.G.A.A. No.12. (*Mount Royal College*).

and equipment, including email and the internet, for the purpose of furthering her part-time dog breeding business. The grievor was the library secretary and had been employed at the College for 14 years prior to her dismissal. She admitted to using her work email for personal matters; however she said that it was "common" for employees to do so. On one particular day the grievor had received 69 emails; many of them, Arbitrator Ponak concluded, were of a personal nature. The arbitrator found that the use of her employer-provided email, amongst other resources, was not culpable "in and of itself" since the employer's policies "were ambiguous and inconsistently applied." However, the problem was the "amount of time the Grievor spent using the equipment during her regular work hours."[28] Despite the fact that the employer had not raised any concerns about the grievor's work performance and that her performance appraisals were "positive", Arbitrator Ponak stated the following in upholding the grievor's dismissal:

> It is true that there were no specific concerns demonstrated about the quality of the work assigned to her. In fact, the Grievor's recent performance appraisals were positive. This is not the issue, however. An employer has a right to expect employees to focus their attention during working hours on activities that benefit the employer. It is reasonable for [an] employer to instruct employees to refrain from devoting substantial work time to personal matters. The College's direction to the Grievor was explicit – do not perform personal work on College time. Because the Grievor disobeyed this order, I can only speculate on how much more productive and valuable her services would have been to the College had she devoted the time spent on personal matters to work on behalf of the College. Clearly, she had an obligation to the College in this regard and clearly this was an obligation that she knowingly did not fulfill. Thus, the fact that the Grievor adequately performed work assigned to her cannot shield her from the consequences of deliberately engaging in personal work once assigned tasks were completed.[29]

The grievor in this case had been previously warned to stop using work time to tend to her personal business. In upholding the dismissal the arbitrator also noted the grievor's problem with tardiness and her misuse of other equipment including the telephone.

In the end, this case was decided on the same basis as any other employment case dealing with employees that are not devoting working time to their jobs. Operating a personal business while at work is certainly ill-advised, whether one is using email, the telephone, or simply doing the books while at work.

Another example is *Re Ontario Power Generation Inc. and Power Workers' Union*,[30] where the grievor had been using her company email address to engage in correspondence with exotic dancer agents and clubs in the Czech Republic. The grievor was dismissed after it was found that she had been using the employer's email and internet systems, amongst other equipment,[31] in a side-business recruiting female exotic dancers from the Czech Republic. She also "occasionally" used the employer's email system in her activities with the non-profit Autism

---

[28] *Ibid.* at para.67.

[29] *Ibid.* at para.81.

[30] *Ontario Power Generation supra* note 20.

[31] The grievor used her employer's telephone for her side-business a total of about 15 hours in a one-year period. As Arbitrator Swan noted: "It is not clear what the subject of these calls might have been, but the sheer volume is, in all of the circumstances, quite striking."

Society of Ontario and to conduct other personal investment business like reply to offers to rent her family's condominium properties.

Her use was at first occasional. Later on, "to avoid further friction" with her husband over her participation in both her volunteer work with the Society and her recruitment of foreign exotic dancers, the grievor began to use her workplace email address exclusively for these purposes. Arbitrator Swan also noted that her email contained "a substantial amount of the sort of material which one finds, regardless of the dire warnings issued by management, on almost any corporate email system. There were jokes received and forwarded, and similar non-business material received or passed on."

Despite the mitigating factors in this case, which included 12 years seniority, no prior disciplinary record, the high regard of her supervisors, and an extremely difficult family situation including a child with special needs (for which the employer had accommodated her allowing her to work one-half day per week at home, "at a time of her choosing to suit her schedule") and the breakdown of her marriage, Arbitrator Swan found that the "degree of breach of trust" was "significant and that the employer had made an overwhelming case for dismissal." In so doing, Arbitrator Swan noted the importance of the fact that the grievor held a position of trust:

> There can be no doubt that the grievor was in a position of particular trust beyond that normally accorded to someone at her level of responsibility. She worked for a manager who was regularly out of the office for extensive periods, and she worked for a large number of individuals who were regularly assigned in the field; some of them, in fact, seem to have been permanently at field sites.
>
> The grievor was therefore required to work alone, and she was trusted to do so. She was given every latitude in setting her own break and lunch times, and the evidence is that she was only required to ensure that she put in the requisite total number of hours per day.

Arbitrator Swan also noted the fact that the employer had accommodated her special circumstances and allowed to let her work at home one-half day per week:

> That permission meant that she was not merely supervised, but was completely away from the Employer's premises, so that even her attendance could not be verified directly. From her home, she had access to the Employer's computer system, so this special situation of trust extended to the Employer's assets as well.

Arbitrator Swan found that the grievor was aware that using the employer's email and assets to carry on her side-business was "absolutely prohibited", and that she exercised great care to make it unlikely her email use would be detected. Furthermore, it was noted that she was "less than forthright" throughout the employer's investigation and misled the employer and the union as well as to her conduct.

Perhaps one of the most egregious examples of "excessive use" was illustrated in the case of *Syndicat Canadien des Communications, de l'energie et du papier, section local 522 c. CAE Electronic Itee (grief de Petruzzi)*.[32] In that case, Arbitrator Tremblay concluded that the grievor

[32] [2000] D.A.T.C. No. 15.

had committed time theft and upheld his termination. The employer launched an investigation after a co-worker noted that the grievor spent an inordinate amount of time online, even though using the internet was not a part of his job responsibilities. The employer found that during a four and a half month span when the grievor had claimed about 480 hours of overtime, he had also been spending a truly tremendous amount of time online. Specifically, during that four and a half month period, the grievor had spent about 300 hours on the internet, accessing mostly pornographic material. In upholding the termination, the arbitrator noted that the grievor was aware of the employer's internet policy and had acknowledged these policies by signing them.[33] The actual content that he had accessed was irrelevant; it was the amount of time wasted, along with the corresponding overtime claim, that justified disciplinary action.

In contrast to these decisions, Arbitrator Bruce in *Hadfield v. New Brunswick Electric Power Commission*[34] found that the grievor in that case had not reached the point of "excessive use" of the employer's online resources. The employee had previously been disciplined for using email and the internet for personal reasons. He had acknowledged that on that previous occasion he had misappropriated the employer's time and resources and entered into a "last chance agreement" by which he undertook to cease using the employer's resources for personal use. The employer based the grievor's subsequent termination on, amongst other things, the fact that the grievor had sent about 30 personal emails over the course of a 3 month period and that he continued to receive emails of a personal nature, including some from charitable organizations for which he worked.

In determining that his discharge was too severe in the circumstances, Arbitrator Bruce analyzed the emails that had been received in detail, in the context of the nature of email more generally:

> By far the large majority (of the emails) were to two of his daughters who at the time were away from home. These e-mails when seen in context were very brief and simply involved a series of correspondence over a very few topics. Some e-mails the Grievor received were ones where he would not necessarily have thought to advise the individuals not to use his office e-mail address. For instance, the Grievor received an e-mail...from a niece in England and another e-mail...which consisted of jokes that came from a work friend who would have not been advised not to contact him at work because there may be occasions when he would be receiving information of a work nature from him. There was also a series of e-mails from Sarah Kennedy, the Executive Director of the New Brunswick Choral Federation. Any replies from the Grievor to her were extremely brief and would not have involved any substantial amount of time. It is obvious, however, that the Grievor did not immediately advise her to use his home e-mail address for any future correspondence which he should have done. Another e-mail that came in...simply was in relation to a request that had gone out prior to June 1998 and, therefore, cannot be seen as something which the Grievor initiated subsequent to the disciplinary action in June of 1998.[35]
>
> The availability of e-mail is a fairly recent development and there was no suggestion in the Employer's evidence that the limited use of the e-mail referred to in evidence

---

[33] Cited in Terry Roane and N. Blaise MacDonald "When Privacy Interests Clash with Surveillance and Testing in the Workplace" (*Labour Relations, Atlantic Region*, September 2003) Insight Information. [Roane and MacDonald].

[34] [1999] N.B.L.A.A. No. 16.

[35] *Ibid.* at para.17.

> involved any measurable costs to the Employer apart from the work time the Grievor would have utilized in composing and sending the e-mail messages. There appears to be some similarity in terms of cost to the Employer of an employe[e] using a telephone for local calls and e-mails. The issue again is not a question of theft of company property but more directly one of whether the use of these facilities is appropriate during working hours. This is not to suggest that employees should be free to use the Employer's e-mail facilities during non-working hours for personal matters. If the Employer has made it clear to all employees that this facility is never to be utilized for personal matters then any such usage would have to be viewed in the same way as one would regard a direction from the Employer never to utilize local telephone service at work. There is no evidence that the Employer in the present case had issued a directive to employees never to utilize e-mail facilities for personal reasons. One obvious difficulty with using office e-mail addresses is that the initiation of one e-mail often provides an easy and inviting way for an individual to reply using the office e-mail address. With the ability to forward the same e-mail to numerous people this invites the possibility of numerous replies.[36]

The grievor was reinstated without loss of seniority but without retroactive pay. In coming to this conclusion, Arbitrator Bruce took note that:

1. the grievor's personal usage did not amount to "a significant amount of time during working hours";

2. "the large majority of the emails were to his children and not to volunteer community groups";

3. the grievor had made significant efforts and improvements to curb his personal usage, including contacting people to tell them to cease communicating via his work email; and

4. the grievor had "indicated his willingness to resign from any positions he holds with various volunteer groups to further ensure he does not use working hours to do volunteer work for these groups."[37]

In *Milsom v. Corporate Computers Inc.*,[38] an Alberta court found that the employer did not have just cause to dismiss the employee on the basis of excessive personal use of the employer's email nor on the basis of poor levels of performance. The employee in that case had been employed for six years as a commissioned salesperson. He was originally dismissed for poor performance, but after his dismissal the employer found that he also had a high volume of personal email usage. The employer's internal review found that in one year, the employee had sent out 18 personal emails daily. In holding that a warning would have been the appropriate discipline in this case, the court stated that it "was not satisfied...that this amount of email traffic constituted a serious distraction". The court went on to state the following:

---

[36] *Ibid.* at para.19.

[37] *Ibid.* at para.27.

[38] [2003] A.J. No.516 (Alta. Q.B.).

> Without evidence concerning (the employee's) habits relating to coffee or lunch breaks, it is [im]possible to account for this level of e-mail traffic as having taken place during (his) legitimate breaks from work.[39]
>
> At most, however, this level of e-mail traffic might have caused some distraction from (his) peak performance (for the employer). Attending to this level of personal messaging might have decreased (his) work performance, but it did not stop (his) work performance....poor performance is rarely a basis for summary dismissal.[40]

In *Manchulenko v. Hunterline Trucking Ltd.*,[41] the court also found that dismissal was not an appropriate response to the employee's personal use of the internet and email at work. The employer began to provide internet and email access in the spring of 2000, and soon after had begun to notice abuses of the system by employees, including the transmission of emails with large graphic files attached which "congested and slowed the network and e-mail system."[42] By the following year, the entire email system crashed and was down for a week as attempts were made to re-activate it. After this incident, the employer sent out a warning that, amongst other things, employees were to be "held accountable for non-work related activities during regular hours."[43] Subsequently, according to the employer, it found a "significant number of non-work related emails which included jokes, nudity, hardcore pornographic videos; and various other disturbing pornographic material"[44] on the employee's computer.

In holding that the employee's internet and email use was not excessive in the circumstances, the court noted that "[t]he evidence does not appear to document whether the (employee) was involved with the material....before, during, or after regular business hours."[45] The court further stated:

> The evidence appears to support (the employee's) argument that the offensive e-mail and graphic materials...were received by (the employee) without apparent solicitation on his part. The (employee's) evidence is that he was unaware of the photographic content of a message until he opened it. In some instances when he became aware of the content he forwarded the material only to his brother.[46]
>
> The (employee) was foolish and careless regarding his personal use of the company computer system. I have no doubt he could, and should, have stopped his friends or relatives sending him the offensive material at his workplace. He abused the privilege of limited personal use. The evidence however does not indicate there was any excessive amount of the material involved; that any significant amount of time was wasted; or any problem to the system occurred. In particular there was no evidence of any distribution of this material to anyone except the (employee's) evidence he forwarded some

---

[39] *Ibid.* at para.49.

[40] *Ibid.* at para.50.

[41] [2002] B.C.J. No.1472.

[42] *Ibid.* at para.43.

[43] *Ibid.* at para.49.

[44] *Ibid.* at para.41.

[45] *Ibid.* at para.50.

[46] *Ibid.* at para.51.

> to his brother in law. In particular and most importantly there was no involvement with other workplace employees or business customers.[47]
>
> ...
>
> The (employee) was certainly deserving of rebuke and censure as the matter had previously been dealt with in respect of errant employees, however in context it was not an appropriate incident upon which to found a dismissal for cause.[48]

Among other things, this case highlights the importance of appropriate language in policies and communications to employees regarding internet and email use. By specifically using the words "during regular hours", the employer may have hindered its efforts to restrict inappropriate activity and prevent further risk to the integrity of its network and online systems.

Pornography – The not so bad, the bad, and the really bad

Seemingly the most common form of internet abuse, pornography certainly dominates the headlines when it comes to employees' inappropriate use of technology. While no hard and fast rules exist, like in most areas of employee discipline, reference to previously decided cases is often instructive.

Where pornography is concerned, decision-makers have consistently distinguished between more offensive material (e.g., child pornography) and less offensive material (e.g., semi-nude images) when determining the appropriate discipline. As Arbitrator Petryshen stated in *Ontario (Ministry of Natural Resources) and Ontario Public Service Employees Union*:[49]

> When determining the seriousness of an offence of the sort engaged in by the grievors, the arbitral jurisprudence clearly indicates that it is appropriate and necessary to consider the degree of offensiveness of the material. Rather than put all inappropriate material, irrespective of how offensive it is, in the same category, arbitrators take into account the nature of the inappropriate material when determining the seriousness of the conduct at issue. Although some of the Union's submissions appeared to suggest otherwise, this approach has considerable merit. For example, the distribution of child pornography by e-mail at work and the distribution of pictures of naked women are both inappropriate, but it is obvious that the distribution of the former material is considerably more serious than the latter, and generally would warrant a more severe disciplinary response.

In that case, sixty-six government employees were disciplined to varying degrees, including six who were terminated, for "inappropriate use of the employer's email". The dismissals were ultimately held to be without just cause, although reasons, and any penalty to be imposed in place of termination, are still pending.[50] The employees had been distributing emails containing images of bestiality, violent and denigrating acts against women, and pictures of nude obese and elderly women to both co-workers and persons outside the workplace. In determining the degree

---

[47] *Ibid.* at para.52.

[48] *Ibid.* at para.54.

[49] (2003), 115 L.A.C. (4th) 120. (*Ontario (Ministry of Natural Resources)*).

[50] [2004] O.G.S.B.A. No. 97.

of offensiveness of the material, Arbitrator Petryshen held that whether or not other employees complain about the material, and whether or not the grievor or employees did not subjectively find the material offensive is irrelevant in terms of assessing the seriousness of the offence. As the Arbitrator made clear, "[t]he failure of anyone to complain did not influence the arbitrator's view of the seriousness of the conduct."

Most pornography cases involve the discipline of those distributing the materials, or storing large quantities on their computers. However, Arbitrator Petryshen explicitly stated that "the mere receipt and deletion of inappropriate material" can be the subject of discipline. He found that

> The grievors, and others, explicitly in some instances and certainly implicitly, invited the receipt of inappropriate material. The situation in this case is not one where an employee receives pornographic material by e-mail, deletes it and then advises the sender not to send such material again. Once the invitation is made, the recipient has no control over what material is sent and how offensive it is.

Furthermore, the Arbitrator noted that the fact that the grievors also sent these images to persons outside the workplace created "the potential for considerable embarrassment for themselves and the Employer."

By way of contrast, in *Dupont Canada Inc. v. Communication, Energy and Paperworkers Union of Canada, Local 28-O (Panter Grievance)*,[51] the employer's monitoring system found 24 pictures of "sunshine girls" – semi-clad women in pin-up style poses which are published daily by some tabloid newspapers) – which the grievor had transferred from one personal web-based email account to another via his employer's internet connection. In dealing with these images, Arbitrator Roach disagreed with the employer's assertion that these images were "pornographic". As he stated:

> Although the nature of the pictures are offensive to a segment of society and may be offensive to some fellow employees...without attempting to attach a label to these pictures it [is] suffice to say that for the purpose of this arbitration they are not as labelled by the Employer...."pornographic, sexually explicit pictures", as these words are commonly understood by the population at large. This does not mean that the Employer cannot prohibit the viewing of this material at the workplace so as to provide a better climate for fostering self respect of all of its employees. However, it must be emphasized that the ground upon which the Employer relied on...to terminate the Grievor's employment was that he interacted...with inappropriate material, namely "pornographic, sexually explicit pictures." These are serious [allegations] constituting per se violation of the Employer[']s policy...[52]

This is a good example of a situation where a properly-worded policy might have assisted the employer. Without such a policy, the behaviour in question was not sufficient to justify the discipline which the company sought to impose.

When it comes to pornography in the workplace, at least one arbitrator has rejected the argument that where the employees are consenting adults the employer should not be concerned with the activity. As Arbitrator Sims stated in *Telus Mobility v. T.W.U. (Lee Grievance)*: "The employee

---

[51] [2001] O.L.A.A. No. 676. [*Dupont (Panter)*].

[52] *Ibid.* at para.20.

is perfectly free to circulate such material with other consenting adults away from work, but I do not find that line of defence persuasive in the workplace, on company time and equipment and particularly in the face of an express warning."[53]

In *British Columbia (Public Service Employee Relations Commission) and B.C.G.E.U. (Johnstone),*[54] the employer suspended an employee due to the employee's breach of a policy that prohibited accessing pornographic sites while at work. The employee had no prior disciplinary record. In substituting the suspension with a letter of reprimand, the arbitrator noted, amongst other reasons, that the grievor had merely accessed an online directory of sex-related web sites but did not enter or view any of these offending sites.

These cases must be contrasted with the case of *Seneca College v. Ontario Public Service Employees Union,*[55] in which a college professor with 18 years tenure and no prior disciplinary record was convicted of possessing child pornography. The employer launched a formal investigation of the professor after two students who had been working in the computer lab at the College noticed that the professor had images of naked children in sexual poses on a computer screen in the lab. The employer ultimately found that the professor had been using the employer's equipment and facilities to access, download and store images of child pornography. In holding that discharge was not excessive, Arbitrator Carter for the majority stated the following:

> Even more telling is the fact that many of these violations also involved a breach of the Criminal Code of Canada. The grievor's conduct, in our view, irreparably damaged the bond of trust that is essential between the College and one of its employees. No amount of contrition or good intentions after the event can repair this damage. An institution such as the College must trust its members to honour the institutional norms of conduct that it establishes. The grievor consistently violated that trust over a sustained period of time. In our view, it is not unreasonable of the College to expect that members of the faculty, who serve as a role model to students, should be particularly scrupulous in honouring the norms of the institution. In this case any mitigating circumstances do not outweigh the grievor's consistent and systematic violation of these norms for a period of over two years. For these reasons it is our conclusion that the employer has established just cause for the termination of the grievor's employment and that this grievance should be dismissed.[56]

In *Dupont Canada Inc. and C.E.P., Local 28-o (Maitland Site),*[57] the employer had discovered that the grievor was using a female co-worker's computer to access the internet and download pornographic files. The grievor had by-passed the log-in requirement and evaded immediate detection; however, the employer later discovered it was in fact the grievor who had been engaging in the clandestine online activity. The grievor had access to his own computer but deliberately chose to mask his behaviour by using the computer of a co-worker. Computer disks obtained from the grievor's locker were found contain the following images including nude

---

[53] (2001), 102 L.A.C. (4th) 239.

[54] Unreported, August 9, 1999 (Hope), cited in Albert and McBean *supra* note 15 at 38.

[55] [2002] O.L.A.A. No. 415 (*Seneca College*).

[56] *Ibid.* at para. 22.

[57] (2000), 92 L.A.C. (4th) 261 [*Dupont (Maitland)*].

women explicitly exposing their genitals; group sexual activity, females performing oral sex on men, and nude men ejaculating into and onto women's faces. It should be noted that the grievor had also been terminated for a number of other "extremely serious", including denying his use of his co-worker's computer.

The majority of the Board concluded that the grievor's termination was justified, despite the fact that "there is some form of inconsistent enforcement of the penalties regarding the improper use of the Internet". They recognized that the "rules regarding the use of computers, while not models of clarity, clearly were known by the Grievor who admitted he breached these." [58]

Hate Sites

The number of hate sites – those including racist sentiments and promotion of violence against particular groups – has also seen a tremendous increase in recent years. According to a 1999 report of the Senate's Subcommittee on Communications, it was estimated that the number of internet sites devoted to hate was around 800. According to Justice Minister Irwin Cotler, however, in 2004, there has been an "explosion" of these hate sites on the internet and the number has clearly and significantly increased.[59] In a recent newspaper article, Cotler was quoted as estimating the number of hate sites to have risen to 5,000 today.[60] Although there do not appear to be many cases dealing with employees accessing "hate sites" at the workplace, that could have more to do with detection issues than a lack of hits to those sites. In any event, an analysis of this type of behaviour would parallel the analysis that one should engage in when considering employees that access and/or distribute pornography.

Chat Rooms & Instant Messaging

A by-product of the "information highway" has been the proliferation of new and intriguing forms of online communication. In addition to email, chat rooms and instant messaging are also creeping into the everyday internet usage and parlance. It has been reported that "almost half of all North American corporations already use messaging – a number projected to grow to 90% in barely two years."[61] Thirty-one per cent of employees in 840 American companies use instant messaging at the office, with 78% of these employees downloading "free" instant messaging software from the internet.[62] Of the employees who have access to instant messaging at work, 58% use it for personal chats.[63]

Instant messaging and the like can have a great value for employers; they can replace needless and lengthy telephone calls and perhaps save money on long-distance costs. However, they can just as surely and easily become open and prone to abuse. In the case of instant messaging, for instance, there is a constant stream of back-and-forth communication – something akin to a

---

[58] *Ibid.* at para.7.

[59] Elizabeth Thompson "Ottawa set to toughen hate crimes legislation" *The National Post* (12 October 2004).

[60] *Ibid.*

[61] Clive Thompson "Hey." Wassup? "Nothin." Instant messaging is here, and the workplace will never be the same" *Report on Business Magazine* (January 2001) at 27-28, citing an estimate by The Gartner Group. [Clive].

[62] The 2004 Workplace E-Mail and Instant Messaging Survey, online http://www.amanet.org /books/catalog/0814472532_Survey.htm [Date accessed: October 6, 2004].

[63] *Ibid.*

telephone conversation but far more time-consuming due to the fact that it can involve a large group of people and continue almost endlessly and without the verbal distractions to officemates. A worker could conceivably log into a chat room upon arrival at work and not log out until she leaves the building. In the meantime, she could be spending vast amounts of time, and dedicating much of his focus and attention, to the online discussions. As one writer puts it, "[m]essaging is a sort of elegant midpoint between the phone call and email; fast, yes, but still with the quasi-literary quality of all text."[64]

In the case of *Canadian Union of Public Employees, Local 37 and Calgary (City) (Graham),*[65] the grievor was employed in the city's waterworks unit where, among other things, the city's drinking water safety levels are tested. The employer's internet policy permitted personal use of the internet "for occasional personal obligations without criticism." Specifically, the policy provided the following:

> When employees are working at any work site, they may (as determined by departmental management) use City telecommunication and personal computing resources for occasional personal obligations without criticism. If at any time the use increases, or the consumption of resources becomes more material it is incumbent on the employee to advise their Manager or Department Head. If this higher level of usage is acceptable, a formal arrangement should be made between the employee and the supervisor. The accommodation and the formal arrangements will vary depending on the nature of the work requirements, but will not interfere with the employee's normal duties or require material consumption of City resources.
>
> Where the personal use becomes excessive it will be treated as misuse of City's resources which is a serious offence. Offenders will face disciplinary action up to and including dismissal.[66]

The grievor, a senior operator with 23 years of service, was suspended and ultimately dismissed after he failed to respond to alarms on more than one occasion. These alarms are set off to notify employees in the unit that chlorine levels in the water have dropped below acceptable levels, putting the city's water supply at risk for higher levels of bacteria and increasing the potential for health risks to the community. One of the alarms lasted for two hours without the grievor making any attempt to respond or to inform his immediate supervisor. It was later discovered that the grievor had been in an online chat room that day for two hours and fifty minutes and that "[t]he personal nature of the messages posted to and from the [g]rievor make clear that the [g]rievor was not attending to his responsibilities at all."

Compounding the seriousness of the grievor's behaviour was the nature of the position, which the arbitrator noted at length, and the fact that the grievor had initially denied responsibility for his actions. In upholding his termination, the Board stated:

> By his actions he has shown himself to be untrustworthy, to lack the credibility and honesty of a person entrusted with caring for the health and safety of the City's drinking water.

---

[64] Clive *supra* note 61.

[65] [2003] A.G.A.A. No.30. (*Calgary (City)*).

[66] *Ibid.* at para.35.

> As an employee of 23 years, [the grievor] knew better. He knew the City internet policy and his foreman had spoken on 3 separate occasions about the need to respect the City's policy. Knowing this [the grievor] made a decision and abused the policy.[67]

While it was not clear whether the grievor in the *Calgary* case was accessing "inappropriate" chat rooms or making "inappropriate" statements in these chat rooms, it is clear that his personal use interfered with his job and compromised the reputation and integrity of his employer's business goals and expectations. This is sufficient reason for dismissal.

So far, there are few other reported instances of discipline for chat room or instant messaging use. However, like internet use generally, it can be deserving of discipline for many reasons. It can fall within the inappropriate or offensive category of behaviour, due to sexual, violent or hate-filled conduct, or it can be "innocent" usage that is only problematic due to the fact that it is taking the employee's focus and attention away from her job responsibilities. A recent survey of 840 employers in the United States, however, showed that only 20% had implemented a policy with respect to instant messaging use and content; the same survey found that 79% of the same employers had implemented a written email policy.[68] In other words, most companies have not yet considered or addressed the issue of instant messaging.

Online Gaming and Gambling Sites

Most computers come pre-programmed with a selection of games which do not require online connectivity, such as solitaire. While these games are entertaining and undoubtedly distracting, the availability of online games, including gambling, is far more dangerous from an employer's point of view. The sheer number of online games, readily available for play at any time, should be of concern. The ability to interact with others while playing is tempting indeed, as is the ability to gamble without leaving one's desk.

According to one software company, in just one year, from 1999 to 2000, the number of sites dedicated to online "gambling" has increased by 209% (from 6,992 sites in 1999 to more than 21,651 sites in 2000).[69] Again, employees abusing their employer's online connection and computer resources to access games is costly; according to one internet-forensic firm, businesses and governments lose about $52-billion a year in lost productivity due to employee use of online games.[70]

In the case of *Wytenburg v. Business Express Airlines Inc.*,[71] the employer dismissed Mr. Wytenburg after it was alleged that he had unplugged a fax machine in the employer's operation

---

[67] *Ibid.* at paras.88, 89.

[68] "2004 Survey on Workplace E-Mail and IM Reveals Unmanaged Risks", AMA, online: http://www.amanet.org /books/catalog/0814472532_Survey.htm [Date accessed: October 6, 2004].

[69] "Online Gambling a Losing Battled in the Workplace", online: www.gamblingmagazine.com/articles/23/23-263.htm [Date accessed: October 15, 2004].

[70] www.bajai.com; cited in J. Birrell and D. Aaron. According to one software company, in just one year, from 1999 to 2000, the number of sites dedicated to online "gambling" has increased by 209 % (from 6,992 sites in 1999 to more than 21,651 sites in 2000). ("Online Gambling a Losing Battled in the Workplace", www.gamblingmagazine.com/articles/23/23-263.htm) [date accessed: October 15, 2004]

[71] [2002] C.L.A.D. No.157.

centre so that he could hook up the cable to the telephone plug in order to access and play games on the internet. The employer operated an airline, and the employee was responsible for distributing reports about the field conditions that periodically came through the operations centre. The reports detailed any changes to weather conditions that could affect runways, and assisted pilots in "making a decision as to whether or not to land". They are issued when conditions on the runway change in a meaningful way. On this particular night, there had been an unexpected winter storm in the area. Because the employee had disconnected the line to the fax, the report was not received. Acknowledging that the employee "had worked in the airline industry in one or more capacities for almost two years, and it would be hard to imagine that he would not have known of the important safety significance of current knowledge of runway conditions", the arbitrator upheld the employee's termination. Adjudicator Nadjiwan went on to state:

> ...the conduct of the Complainant in disconnecting the fax machine constituted a misuse of company property, created a serious public safety risk, and also constituted an attempt to mislead the employer. It is somewhat rare that a single event is sufficient to warrant the immediate termination of an employee. However, in the context of this industry and this case, I find that this incident does rise to that level. While the safety risk of unplugging the fax machine is not direct or immediate, I must consider that this Complainant was willing to take that risk so that he could use the internet to play games. In addition, the situation is further exacerbated by Complainant's continued denial of the incident which does not provide any assurance that the Complainant is likely to change his conduct in this regard in the future.[72]

While this case is particularly extreme, in that it involved a potential safety risk, most cases involving online gaming will deal with the garden variety cyber-abuser and they will be decided in the same fashion as other online abuse cases.

Downloading Copyrighted Material

The online community has made it relatively easy to access and download copyrighted material, either intentionally or without knowing of the copyright issue. The issues regarding music and movies, and services such as Napster, are merely the tip of the iceberg. With the increasing availability of copyrighted material, including music, movies, games and other software applications, pirating while at work, using the company's equipment, can pose a serious concern for employers. This is particularly true because companies often have faster internet connections than their employees' home connection; it can therefore be quite tempting to employees to download large files at work. However, as one American surveyor reports, it can cost about $1 million (U.S.) to defend a web-related patent infringement case.[73]

At least one arbitrator has held that the downloading of material which violates copyright or criminal law is probably the most troublesome issue for employers in their attempt to regulate internet usage at work. In *Krain v. Toronto-Dominion Bank*,[74] the dismissed employee had been employed by the bank for about ten years at the time of his termination. Particularly surprising was the fact that the grievor was an Information Technology Analyst. He had viewed and

---

[72] *Ibid.* at para.57.

[73] Flynn *supra* note 10.

[74] [2002] C.L.A.D. No. 406. (*Krain*).

downloaded pornography online, and had also pirated copyrighted applications and games on to his work computer and used those games and applications while at work and at home.

The bank had an extensive internet policy in place which allowed for occasional personal use of the internet for web browsing but which explicitly prohibited the viewing and downloading of offensive and copyrightable materials. The policy went on to provide further elaboration on what constituted "offensive or inappropriate material" under the policy. Despite Mr. Krain's otherwise unblemished ten year record, and the fact that he was genuinely remorseful, Arbitrator Luborsky refused to overturn his dismissal. As the Arbitrator held:

> His use of the Internet to download unlicensed software applications and games was particularly troublesome. Common sense and the Complainant's knowledge as an IT Analyst would have alerted him to the Bank's legitimate security concerns about the importation of unapproved computer programs into its systems, as well as possible civil liability for the illegal use of such programs, which would be reasonably understood by any employee in the Complainant's position to be conduct incompatible with the Bank's necessary institutional reputation for integrity and trust. In many respects, this may be more serious than the private viewing of images of adult nudity and explicit adult sexual conduct, which while inappropriate in the workplace is not illegal per se, whereas the possession and use of unlicensed software exposes the Bank to potential civil liability for copyright infringement.[75]

The decision in *Krain* must be contrasted with the decision of Adjudicator Liang in *Minaker v. Toronto-Dominion Bank.*[76] In *Minaker*, the dismissed employee was also in the employer's information technology services department. In fact, the employee had worked on a team of employees who had worked towards the installation of special software to prevent bank employees from downloading files from unauthorized internet sites through web browsers. The evidence showed, and the employee admitted, that the employee had bypassed this software program and downloaded software, videos and games from the internet. The evidence also showed that once downloaded, the employee did not generally use the material and software for personal or business use and in most cases, the evidence showed that the employee deleted the material without using it.

In distinguishing the instant case from that of *Krain*, and in determining that the employer did not have just cause to dismiss the employee, Adjudicator Liang held the following:

> ...I am not convinced that the complainant's wrongdoing was so serious as to permanently destroy the bond of trust between him and the Bank. There is no doubt that he committed some serious errors in judgment, in choosing to download files from the Internet through other than sanctioned channels. In so doing, he placed the Bank's computer systems at risk from computer viruses. ...Although it is not clear that there is any specific policy on this, the presence of the blocking software speaks for itself, and would have been known to employees to communicate the Bank's disapproval of importing software through unsanctioned channels. There is no evidence, however,

---

[75] *Ibid.* at para.18.

[76] [2003] C.L.A.D. No. 39. (*Minaker*).

> that the complainant's activities had any effect on the Bank's systems, either at the time he performed the downloading or afterwards.[77]

While it was acknowledged that the employer has a legitimate concern with respect to the pirating of unlicenced software and the potential to be exposed to liability, Adjudicator Liang stated that "the evidence is less than clear that the complainant's activities could be characterized" as pirating. Liang based this partly on the fact that the employer's information systems security employees who testified at the hearing did not consider "the mere downloading of commercial software applications as pirating."[78] It was also significant that the employee in this case had not downloaded the unlicenced software applications for work or personal purposes and had proceeded to delete material downloaded when it became clear to him that the software was subject to a license. Liang accepted the evidence that "absent descriptive titles on the files being imported, it is only at the completion of a download that it becomes apparent whether or not a software application is commercial (and therefore requires a license.)"[79]

In distinguishing the case from *Krain*, Liang observed that what "tipped the balance" in favour of termination in that case was the fact that the employee there admitted to using pirated software applications for work and for personal reasons.[80] In concluding, Liang stated:

> In sum, I find that the complainant was reckless in his behavior, in downloading material through unsanctioned channels, which bypassed the Bank's blocking programs. Further, although I accept that some of this activity was aimed at exploring the range of applications that might have been of potential use to the complainant in his work for the Bank, much of it was for personal interest.[81]

Adjudicator Liang would have reinstated the employee subject to a suspension; however, the employee did not want to be reinstated and so nine months of notice were ordered to be paid to the employee.

Although the law has not been fully explored, it is clear that the illegal pirating of software and other materials should be a significant concern to employers. It is interesting that the two cases above involved IT workers; on the one hand, they have the knowledge and ability to bypass protective systems. On the other hand, they should understand the consequences of their actions, and the potential for being caught, better than most employees. In any event, employers should take steps to protect themselves from liability for this type of behaviour.

Harassment

Harassment is certainly and unfortunately not a new phenomena in the workplace. The jurisprudence regarding sexual and other forms of harassment has set out how such matters are to be dealt with, including situations where there is a poisoned work atmosphere. However, advances in technology have made it easier for employees, and people in general, to carry out such nefarious activities, often in ways that are difficult to detect. As noted earlier, harassment

---

[77] *Ibid.* at para.28.

[78] *Ibid.* at para.30.

[79] *Ibid.* at para.23.

[80] *Ibid.* at para.35.

[81] *Ibid.* at para.32.

of co-workers is one of the most prevalent forms of email abuse and it can be quite costly to employers. The Chevron Corporation in the U.S., for example, paid a $2.2 million (U.S.) settlement to some of its female employees because it did not prevent the transmission of pornographic emails by male employees.[82] Employers must take action when they become aware of any such activity. Furthermore, they should explicitly refer to such activity in their policies, and make it clear that it will not be tolerated. A failure to do so can lead to substantial liability.

In *DiVito et. al v. MacDonald Dettwiler*[83], two employees were dismissed from their jobs after circulating to other employees an email containing a derogatory sexual description of an overweight female co-worker. The email was not originally created by the dismissed employees; however, one of them had stored the email for a year before re-circulating the email to other co-workers. Another co-worker who received the email had printed a copy and posted it on one of the office bulletin boards. The employee was confronted about the email by a supervisor; after this confrontation, the female co-worker who had been depicted in the email found a copy of the email in her in-basket.

Drost J., in distinguishing the instant case from a similar case, stated that "...there was nothing humorous about the contents of the e-mail. It exploited Ms. X's physical problem as well as her sensitivity. It was personal and it humiliated her. The fact that it was delivered to other employees and then posted on a company bulletin board, turned the matter into a form of public harassment."[84] In upholding their dismissal, Drost J. noted:

> ...I am not persuaded that the conduct of the plaintiffs, so far as their involvement in the distribution of the e-mail message is concerned, is alone sufficient grounds for their summary dismissal. I am of the view that, standing alone, that conduct warranted a severe reprimand, but nothing more.
>
> However, such conduct, when combined with the plaintiffs' subsequent dishonesty during the investigation, does, in my opinion, clearly [amount] to just cause for dismissal.[85]

Consider also the more recent case of *Westcoast Energy Inc. and C.E.P., Local 686B (Bourdon)*[86], where the grievor had anonymously sent emails containing "inappropriate" material on four occasions to a female co-worker. The grievor sent the emails under the name "Big Stick" and had used a web-based email provider rather than the employer's email system. One of the emails contained the following:

> Hi Baby!!!
> I am Back
> I sure Miss You...You have been on my mind a lot...Kisssss
> I have been so Hot for you while I was at home, thinking thinking thinking of you.
> Love
> C.

---

[82] Cited in Williams and Samfiru *supra* note 17.

[83] [1996] B.C.J. No.1436 (B.C. S.C.).

[84] *Ibid.* at para.29.

[85] *Ibid.* at paras.34-35.

[86] (1999), 84 L.A.C. (4th) 185.

In another, the grievor wrote:

> You are so sweet, I could lick you all day long...mmmmmmmm
> What a wonderful person you are...
> I miss You

In finding that the grievor engaged in sexual harassment, Arbitrator Albertini quoted extensively from the case of *Re Canada Post Corp. and C.U.P.W.*,[87] where Arbitrator Swan stated:

> While the categories of prohibited sexual harassment may not yet be closed, it is generally regarded that the offensive conduct is of two types. One form of sexual harassment is coercive in nature; the harasser attempts to use leverage gained from an employment relationship to elicit sexual favours, or to press sexual demands. While this kind of sexual harassment is normally committed by a superior, the offence can also be committed by a fellow employee who has no particular advantage of rank, but who uses the proximity and opportunity provided by a shared work place to press sexual requests which are unwelcome.
>
> . . .
>
> The second form of sexual harassment is harassment aimed not at an employee's sexuality, but at the employee's gender itself. This may be harassment because the employee is of a particular gender, or harassment amounting to degradation of persons of that gender. There is really no difference between harassment of this kind and harassment on the basis of any other of the prohibited grounds of discrimination; when one employee sets out to make another employee's life miserable because of some characteristic of that employee which also constitutes a prohibited ground of discrimination, that can reasonably be perceived as undermining that person's right to equality in the work place. Indeed, harassment may justify discipline even where the basis for the harassment is not a prohibited ground; if employees have a right to be protected from physical assaults by their fellow employees, they have an equivalent right to be protected from a course of verbal injury, whether that verbal injury has a basis which is a prohibited ground of discrimination, or has some other basis, or even has no basis at all.

Despite setting aside the grievor's termination in this "borderline" case, Arbitrator Albertini nevertheless called the conduct a "serious offense", and went on to state:

> To send anyone an anonymous inappropriate email message is contrary to the most basic concept of decency in addition to being a cowardly act." The arbitrator noted that the grievor was a 24-year employee with no previous disciplinary record, that he had suffered economic loss due to being suspended ultimately pending the grievance and that "[m]ore importantly, he has and will continue to suffer the shame of sending pornographic material anonymously and the further embarrassment of knowing his family and friends are now aware of his tendency to use pornographic web sites.

---

[87] (1987), 27 L.A.C. (3d) 27.

While these cases were not particularly egregious, it is easy to see how harassment can become more threatening, and lead to full-scale stalking. The technology is there to make this relatively easy to do, and also to do relatively anonymously. An employer that allows such behaviour to take place within the confines of its workplace, on its equipment, could easily be exposed to liability, not to mention a serious blow to their reputation.

Based on the above, the types of internet and email abuse can be divided into the following categories (with some overlap between them):

1. behaviour that is innocuous but time-wasting (surfing, online chatting, games, etc.)

2. behaviour that is inappropriate in relation to other workers (pornography, hate sites, harassment, etc.)

3. illegal behaviour (child pornography, serious harassment, pirating software, etc.)

Each should be addressed in any policy, and should be monitored as closely as possible. Each presents its own challenges to employers, and each, left unchecked, can cost an employer significantly.

THE EMPLOYER'S CYBER-PROTECTION: EFFECTIVE POLICIES, MONITORING AND ENFORCEMENT

Having reviewed the plethora of online dangers, the next question to be addressed is how an employer can protect itself from the cyber-abusers in its midst.

It is clear from the case law and arbitral jurisprudence that it is critical for employers to create, maintain and enforce policies relating to the use of the online resources in the workplace. These policies should be communicated to employees regularly, updated as required to accommodate the changing workplace and technology, and, ideally, endorsed or acknowledged by the employees. The policies should be as detailed as possible, so that subjective terms such as "reasonable" or "inappropriate" are not left undefined and open to judicial or arbitral interpretation. Failing to abide by these recommendations can open an employer up to all sorts of abuses, and handcuff them when it comes to disciplining offenders.

It should also be borne in mind that a toothless policy alone may be little better than no policy at all. A perfectly-drafted policy will be meaningless if it is printed, filed, and left to gather dust. Employees must be made aware of the policy, and clearly told that violations will be cause for discipline. Failure to enforce existing policies can restrict future efforts to discipline violators. Although in some aspects of life, the excuse that "everybody else is doing it" may not carry much weight, it can in the context of workplace discipline. Unfortunately, a recent survey of IT security professionals revealed that employers are "failing to ensure that staff understood corporate security policies, potentially leaving them exposed to legal action or embarrassment when staff abuse internet access."[88]

---

[88] B. Goodwin "Survey shows internet abuse is rife" *Computer Weekly* (27 January 2004) at 4.

In most cases, a policy that is not enforced will not be sufficient to ground a dismissal for internet abuse. In fact, decision-makers have been loath to impose discipline where the employer has essentially allowed internet misconduct to go unchecked and unpunished, allowing a "permissive culture" to permeate the workplace. In this sense, the issue is just like any other workplace rule: it must be publicized and enforced. Otherwise, condonation issues arise that can restrict employers in their efforts to discipline offending workers.

In *Consumers Gas v. Communications, Energy and Paperworkers Union (Primiani Grievance)*,[89] the grievor, a senior clerk, was terminated for receiving and distributing inappropriate emails including pornographic material. The employer first became aware that there was a group of employees distributing inappropriate emails at work when its computer system crashed. It discovered that the cause of the crash was a manager's attempt to send a large email containing two pornographic videos, one depicting acts of bestiality and the other depicting a woman using a Coke can for sexual purposes, to other employees and to people outside of the workplace. The employer had an internet policy in place which permitted some personal use of the internet and email systems; however, it was doing nothing to ensure that the policy was complied with. The employer just "expected that the employees would live up to their code of conduct and its core values."[90] As Arbitrator Kirkwood held:

> ...the company has to share some responsibility for what occurred. Although the company did not monitor (the email) system, that...should not be held against the company in extreme circumstances. However, the failure to give guidelines to its managers and to its employees and thereby turning a blind eye, gave rise to the permissive culture that existed at the company. Even when it came to light that in January 1998, an employee was downloading pornography from the internet, the company did not recommunicate the existing policy to its employees or issue any directive on the use and abuse of the system, the company instead chose to wait until such time as the company had rewritten the policy. By not monitoring or directing its employees, a permissive culture developed within a small group in the context of the overall number, of managers and employees.[91]

In the end, due in part to "the lack of monitoring by the company and lack of direction of the company's workforce, and the penalties given to others" within the company who had engaged in similar abusive activities, the grievor's termination was substituted with a one month suspension.

Another example is the case of *MacLean v. New Brunswick (Department of Public Safety)*.[92] In this case, the grievor, who worked as a correctional officer in a male maximum security institution, was discharged for, among other things, inappropriate use of the employer's computers. The grievor had been creating and maintaining electronic files of offensive material, including primarily pornographic images of women and deformed genitalia. The evidence showed that it was common practice for employees to receive pornographic material and that "nearly all employees received such...material."[93] Furthermore, it was "not uncommon for an

---

[89] [1999] O.L.A.A. No. 649. (*Consumers Gas*).

[90] *Ibid.* at para.11.

[91] *Ibid.* at para.72.

[92] [2004] N.B.L.A.A. No.11.

[93] *Ibid.* at para.24

employee to see this material on the screen of another employee's computer during working hours, particularly during the night shift."[94]

The Arbitrator found that the grievor's dismissal was excessive in the circumstances and replaced the dismissal with a five month unpaid suspension and a condition that the grievor continue to receive counselling for a period of time as recommended by his counsellor. The arbitrator cited the following reasons for overturning the dismissal:

- Although the email policy was available to employees, there had not been any significant distribution or discussion of it by management with employees...which would have clarified the seriousness of the activity.[95]

- Although employees might normally have been expected to appreciate that this was not an appropriate use of the government computers, the culture of the workplace appears to have generated an acceptance of such material as commonplace.[96]

- ...the Sexual Harassment Policy and Email Policy were not well publicized amongst employees at the workplace. It is appreciated that employees should not need to be reminded of the inappropriateness of workplace harassment or the inappropriate use of the email system. At the same time, familiarity with these policies and with the sexual harassment policy, in particular, would have better equipped the Grievor and the other employees to understand the implications of their conduct and the need to respect any communication as to it being unwelcome.[97]

- Finally, it must be appreciated that the workplace culture did not discourage the exchange of such emails or suggest that they were seen as offensive by fellow employees. To some extent this may be a question of conditioning or, as suggested by one of the witnesses, an escape mechanism from some of the less savoury aspects of their daily work life. ...this does not condone the activity but may help to explain it.[98]

The employer's awareness of the impugned activity is an important factor. If the offending conduct is common but the employer is unaware, it will be difficult to argue that there was condonation unless the employer can be seen as having been wilfully blind. In *Ontario (Ministry of Natural Resources)*, Arbitrator Petryshen held that:

> The fact that a significant number of employees engaged in e-mail abuse, by itself, does not necessarily assist the grievors. Unless it can be shown that the Employer was in some way responsible for the culture or was aware of the problem but turned a blind eye to it, the grievors and the employees who were disciplined will not be able to avoid complete responsibility for their conduct.

Employers will encounter difficulty where they have knowingly allowed inappropriate conduct to take place, unpunished, for some time and then "suddenly" seek to impose discipline.

At the same time, however, arbitrators have not allowed employees to evade discipline in cases where common sense and better judgment should have prevailed. However, the employer's

---

[94] *Ibid.*

[95] *Ibid.* at para.28.

[96] *Ibid.*

[97] *Ibid.* at para.55.

[98] *Ibid.*

failure to adopt, disseminate and enforce appropriate policies might mean that an employee will be disciplined instead of terminated. In *Primiani*, for instance, Arbitrator Kirkwood held that while the employer's internet policy "was not well known", this "lack of knowledge of the policy" could not completely absolve the grievor. The Arbitrator held that "[c]ommon sense should have prevailed, and suggested to the grievor that the (email) system and the computer's storage system is not for her own extensive use and that the transmission and storage of sexual material would not be acceptable to the business."[99] A one month suspension was imposed in place of the termination that was grieved.

In *Ontario (Ministry of Natural Resources)*, the arbitrator held that while "[g]enerally, an employer should advise employees about what behaviour will result in discipline and how severe the discipline might be. ...But there is some conduct which any employee should recognize as unacceptable even without a rule or some other notice from the Employer." In that case, it will be recalled, 66 employees were disciplined for circulating inappropriate emails, some containing images of bestiality and violence against women.

This "common sense" or "should have known better" approach has also been successfully advanced in cases where there is no particular rule or policy covering the behaviour in question. For example, in *Telus Mobility and Telecommunications Workers Union*,[100] employees had used the employer's email system to transmit "seriously" pornographic material even though they had been expressly warned that such behaviour could result in discipline. In dealing with the issue of whether the employer needed a specific rule in order to justify discipline in these cases, Arbitrator Sims stated:

> I find that the conduct established in this case is of such a nature that no specific rule is needed in order to justify discipline. ... It should be self-evident to any employee that using the employer's e-mail facilities to send seriously pornographic material to other employees or elsewhere is unacceptable conduct.
>
> ...
>
> ...the materials in this case are...into the realm where no thinking employee would be under the impression they would be acceptable to the Employer. The grievor's receiving, storing and forwarding this material is, without any rule, just cause for discipline.

The more offensive or serious the behaviour, the more likely that a trier of fact will find that the employee should have known that it was inappropriate, regardless of the existence or lack of a policy on that point.

Despite this line of cases, it is nevertheless prudent to have a detailed and consistently enforced policy. It is also important to be completely clear when it comes to spelling out the prohibitions, restrictions and consequences of violation. In *Greater Toronto Airports Authority*, the arbitrator encouraged the employer to reconsider the language of its earlier internet policy. The policy provided in part as follows:

> GTAA computers are to be used solely for business purposes.

---

[99] *Ibid.* at para.71

[100] (2001), 102 L.A.C. (4th) 239.

> Internet access from dedicated machines should be limited to business-related purpose.
>
> No material should be downloaded from the internet or any other source that may constitute a criminal offense (*sic*) under the Criminal Code of Canada.

Arbitrator Murray advised the employer as follows: "Difficult though it may be, the employer needs to consider distinguishing between what might be described as permitted sites and classes of sites that are prohibited (that is those that may be offensive to other employees if accidentally accessed after another employee had accessed them...)."

It is virtually impossible to provide a comprehensive and uniform approach to creating internet and email policies for every workplace. However, these are some guidelines that have been gleaned from the jurisprudence and academic literature to date:[101]

- Use clear and unambiguous language;
- Avoid ambiguous words such as "reasonable" where possible - be specific;
- "The policy should state that the computers, systems and all technology, whether software or otherwise are the property of the employer. The policy should state that the employer owns all the files on the system and all communications received, sent or stored by that systems..."[102];
- Specify the nature of the web sites and types of online activity that are strictly prohibited (e.g., no pornography, hate sites, chat rooms, instant messaging, no distributing emails containing large attachments, no downloading copyrighted material)[103];
- Specify whether personal use of online resources can be engaged in and to what extent;
- State whether employees can use the resources after hours, or during work hours;
- Spell out enforcement mechanisms. If email and online activity is to be monitored, make this clear so that employees are aware that their email is not private and their internet and email usage is being monitored. "Surreptitious monitoring has no deterrent effect, and may raise allegations of unfairness, entrapment or invasion of privacy"[104];
- Communicate the policy. Make sure employees are aware of the policy, and any changes to the policy. Post it in the workplace, append it to the employee training

---

[101] For sample policies see: *Treasury Board of Canada Secretariat: Policy on the Use of Electronic Networks (February 1998)*; Todd Humber "Developing an internet use policy is painless – and crucial" *Canadian HR Reporter, Guide to HR Technology* (4 November 2002).

[102] Roane and MacDonald *supra* note 32.

[103] See "Sample personal computer use policy" *Canadian HR Reporter* (4 November 2002).

[104] Albert and McBean *supra* note 15 at 42.

manual or to employment agreements, and provide training where appropriate. "It is preferable that a new copy of the policy be given to each employee at the annual review or alternatively that there is some other form of annual reminder that the policy is in place and will be enforced"[105];

- "Emphasize that employees have a responsibility to discourage friends and associates from sending them inappropriate email"[106];
- Update the policy where necessary to reflect new potential forms of abuse that are not addressed adequately in the policy;
- Ensure supervisors and managers are aware of the policy and how to monitor for breaches;
- Be clear about the consequences of breaching the policy. Warn employees that they may be disciplined up to and including termination;
- Respond immediately and thoroughly to abuses. Ensure that there are appropriate systems in place to detect abuses early;

Although it may seem obvious, it is critical for an employer to clearly set out what behaviour is unacceptable to the employer, and what will warrant discipline. For example:[107]

- Transmitting or releasing sensitive, confidential, proprietary or privileged information concerning the employer to anyone not permitted by the employer to receive it;
- Sending or soliciting communications containing material which is fraudulent, harassing, pornographic, profane, obscene, vulgar, intimidating or unlawful;
- Participating in controversial or inappropriate internet discussion groups such as pornographic, hate-based or terrorist discussion groups;
- Accessing or displaying any material that may be considered offensive in the employer's environment unless required for specific research;
- Downloading copyrighted content from web sites on the internet except for research purposes or non-commercial use which results in limited machine-readable or print copies;
- Interfering with, removing or bypassing any security features or devices designed to protect data, whether it is the employer's data or not, from viruses, unauthorized external access or other security risk;

---

[105] Roane and MacDonald *supra* note 33.

[106] Albert and McBean *supra* note 15 at 42.

[107] These unacceptable uses have been paraphrased from original. They can be found in the sample policy outlined in the Canadian HR Reporter *supra* note 101.

- Storing personal data of more than a minimal amount on computer resources.

Many employers, perhaps dissatisfied with reliance on the "honour system", are turning to technological aids in order to monitor the online activity of employees and protect the security of their systems. A recent survey of American workplaces found that two-thirds of American companies are controlling and monitoring employee computer use.[108] A 2001 study by the Privacy Foundation in Denver found that 14 million employees (1/3 of the U.S. online workforce) are monitored for their internet and email use by their employers.[109]

It is also reported that in some industries and professions, including telecommunications, insurance and banking, more than 80% of employees are subjected to monitoring.[110] Monitoring can include reading files stored on an employee's computer, as well as monitoring the web sites that are accessed. In addition, employers can block certain web sites using software generally designed to prevent children from accessing in appropriate sites. Employers can also provide email access without access to the internet, which would admittedly be a step back on the technological evolution chain for most workplaces.[111]

Regardless of the efforts made by employers, it is impossible prevent all abuse. Consider the case of *Calgary Regional Health Authority and H.S.A.A. (Dickinson Grievance)*,[112] where the employer had used disabling technology to disable a link through which internet access was obtained at work. The grievor, in spite of the employer's efforts, cracked the system and on several occasions was able to gain access to the web. He used that access to view pornographic material. Needless to say, if such an employee is caught, the sanctions should be even more severe than they would otherwise have been based upon the internet use itself.

Monitoring also raises issues of privacy, and employers must be cognizant of the these issues. It is difficult to discern a universal commonality among the arbitral and court decisions with respect to the privacy implications of monitoring employees' online activity. Recently enacted privacy protection legislation apply to varying degrees to employees in certain workplaces. In some jurisdictions, privacy codes deal specifically with the issue of employee monitoring, providing some practical guidance for dealing with these issues in the workplace.[113]

For instance, the U.K.'s *Employment Practices Data Protection Code*, provides that while the data protection legislation "does not prevent an employer from monitoring workers" and that in fact "[m]onitoring is a recognised component of the employment relationship", it must be done in compliance with data protection legislation. For example, the Code provides that the following

---

[108] 2001 AMA, "Workplace Testing and Monitoring", online: http://www.amanet.org/research/pdfs/WT&M=2c_a.pdf.

[109] L. Rosencrance "Study: Monitoring of employee email escalates" CNN.com, online: http://archives.cnn.com/2001/TECH/internet/07/09/employee.monitoring.idg/. [Date accessed: October 18, 2004].

[110] Hertenstein supra note 3, cited in Sarra supra note 3 at 12.

[111] It should also be noted that the *Criminal Code* makes it an offence to "willfully intercept private communications", including emails. However, this offence has not yet been applied to employers who monitor their employees emails while at work.

[112] [1999] A.G.A.A. No. 66.

[113] See the UK Privacy Commissioner, *Employment Practices Data Protection Code, Section 2: Monitoring Workers.*

principles should be observed with respect to the monitoring of electronic communications by employees:

- 3.3.8. Wherever possible avoid opening e-mails, especially ones that clearly show they are private or personal;

- 3.3.11. Inform workers of the extent to which information about their internet access and e-mails is retained in the system and for how long.

The issue of how privacy rights inter-relate with the employer's right to monitor its employees is a tricky one that is still in its infancy. It is difficult to say what the law is, or what it will become, as relatively recent legislation is interpreted. However, the jurisprudence to date suggests that the following factors will be considered by a trier of fact:

- The purpose(s) of the adopted measures;

- The existence of other methods to achieve the stated purpose(s);

- The relative efficiency of those other methods;

- Whether the loss of privacy was proportionate to the benefits.[114]

What does seem clear, however, is that employees who trust that workplace email and internet usage is private should reconsider and take into account the nature of these resources.[115] In the case of *Naylor Publications Co. (Canada) and Media Union of Manitoba, Local 191*,[116] for instance, Arbitrator Peltz addressed the issue of whether an employee could have any privacy entitlement in an email message that was written during working hours using the employer's online resources and systems. In that case, the employer's internet and email policies contained a provision that employees "should have no expectation of privacy for any Internet use via the company's facilities" and that the employer "expressly reserved the right to review, monitor and record data on its system without notice or permission." The arbitrator concluded that employees were well aware and warned of the employer's right to monitor.

The employer had been monitoring the grievor's email activities and found that she had written some disturbing emails during work hours, including references to the grievor "going postal" and "mused about...shooting people at work", although she never specifically mentioned any co-workers and the emails were sent only to people outside of the workplace. The following is an excerpt from one of the intercepted emails: "I swear to Christ I'm ready to take some people out. I'm so ready to bring a gun to work and just shoot people. I can see how people go postal." After

---

[114] A more detailed discussion of these issues is beyond the scope of this paper.

[115] See the oft-cited U.S. case of *Smyth v. The Pillsbury Company* 914 F. Supp. 97 (E.D. Penn. 1996), where although the employer had told employees that email communications at work would be "confidential and privileged" and that they would not intercept emails and later use them to discipline employees, the court nevertheless held that the employee had no reasonable expectation of privacy in his emails when the employer eventually did intercept and use his own emails to terminate him. The employee's emails contained death threats aimed at some co-workers.

[116] Unreported, April 7, 2003.

the employer discovered the emails, they contacted police and arranged for 24 hour security to guard the premises.

While Arbitrator Peltz acknowledged that "an argument might be raised about employee email generated on personal time", he also stated that "the bulk of the grievor's messages were sent on company time." In dealing with the privacy issues and stating that "the reality of email and the internet is that privacy can never be guaranteed," Arbitrator Peltz went on to hold the following:

> The Union in the present case analogized to writing a letter for venting purposes and leaving it in your desk, or taking your troubles home to a spouse or friend. However, e-mail users ought to know that when they put out sensitive or offensive material into cyberspace, they can never be sure where the message will ultimately come to rest. Today, if a person needs or desires a private conversation, she must carefully consider how to ensure true privacy. Expressing deeply personal thoughts over an employer's computer system is surely not a good choice. At times, notwithstanding the inconvenience, it may be preferable to wait until there is an opportunity for face to face communication.

Arbitrator Peltz ultimately held that while discipline was justified in this case, termination was too excessive and progressive discipline should have been engaged to deal with the employee. The grievor was reinstated without pay on the condition that she would be terminated if she continued to abuse the employer's email system.

In *Milsom*, discussed above, the court held that employees could have no expectation of privacy with respect to "emails received and sent in the workplace on the employer's time and equipment,"[117] even where there is no email policy in place. As the court held:

> 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-mails. 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.[118]

In *Camosun College v. Canadian Union of Public Employees, Local 2081 (Metcalfe Grievance),*[119] the grievor, a laboratory technologist with 12 years of service, had forwarded an email to a union chat room housed on the employer's computer system and was ultimately dismissed by the employer due to its contents. The employer became aware of the email after a chat room subscriber forwarded the message to the administration. The Union attempted to argue that the grievor was entitled to privacy with respect to his email. In disagreeing with the Union's position, Arbitrator Germaine concluded the following:

> The cupe-1 list was part of the College's system. In my view, that fact alone should persuade any reasonably informed e-mail user that messages on the list could be monitored by the College. But other features of e-mail are even more critical. Once forwarded to a distribution list, e-mail is in the hands of all of the subscribers to the list. Any one of the subscribers with the necessary hardware could print an e-mail message in hard copy. The originator of e-mail has no control over

---

[117] *Ibid.* at para.41.

[118] *Ibid.* at para.46.

[119] [1999] B.C.C.A.A.A. No. 940.

> the circulation of printed copies. More significantly, any subscriber could simply forward it to persons external to the list. Every subscriber would have the capacity to communicate a particular message to every one of the subscriber's e-mail correspondents, and they in turn to their correspondents. The potential for dissemination is limited only by the internet.[120]
>
> ...
>
> The nature of the medium therefore does not support a claim for confidentiality. Rather, it prevents any such claim.[121]

While the law in this area is in a state of some uncertainty, employers would be well-advised that if they do install monitoring devices, they should inform employees that their usage will be monitored and that information obtained from such monitoring can be used for disciplinary purposed.

DISCIPLINING THE CYBERSLACKER

Having discussed the ways in which employers can monitor their employees' use and abuse of technology, the next issue to address is what they can do when they find that employees are abusing the system. As discussed above, ignoring the problem and doing nothing can create a permissive environment which is easily entrenched but very difficult to remove. This message does appear to be getting through to most employers; an American study suggests that employers are increasingly disciplining for these workplace offences. Specifically with respect to violations of email policies, 25% of employers said they terminated an employee in 2004, compared to 22% in 2003 and only 17% in 2001.[122]

At the same time, employers are often mindful of the minefield that disciplining an employee can open up. When arbitrators and courts have considered cases of internet abuse, they have applied the traditional legal principles regarding the disciplining of employees, adapting them as needed to address new issues brought about by developing technology. Like any form of inappropriate behaviour, not all internet or email abuse will provide sufficient grounds for termination. Just cause is difficult to prove in any context, and internet or email abuse is no different. All of the usual discipline-related factors must be taken into account. The trier of fact will usually take a contextual approach to the matter, considering the history of the employment relationship, the seriousness of the offending behaviour and, of course, any other mitigating factors.

A review of the case law suggests that the following are the guiding factors courts and arbitrators have considered in determining the appropriate discipline with regards to internet/email abuse:

- The nature of the online activity (e.g., chat rooms, instant messaging);
- The nature of the material being viewed, accessed, distributed (e.g., offensive pornography, pirated material, chat room);

---

[120] *Ibid.* at para.21.

[121] *Ibid.* at para.24.

[122] 2004 Survey AMA.

- The nature of associated behaviour (e.g., hacking through built-in blocking devices or software, using other employees' equipment to avoid detection);
- The nature of the employer's workplace and type of industry (e.g., safety sensitive);
- The existence of a permissive workplace culture in which the employer has "turned a blind eye";
- Interference with productivity (e.g., excessive personal use);
- The timing of behaviour (e.g., during work hours, during breaks or outside work hours);
- The existence of a clear policy that is communicated and understood by employees;
- The nature of the employee's work responsibilities (e.g., supervisory, position of trust, self-supervising);
- Whether the material was being distributed both to co-workers or people outside the firm;
- Other mitigating and compassionate factors (e.g., whether it is the employee's first offence, length of service, prior disciplinary record);
- The appropriateness of the disciplinary response (e.g., progressive discipline);
- The likelihood of recurrence and the rehabilitative potential of the employee.

Decision-makers have been less inclined to substitute softer penalties when the offending employee holds a position of trust. This is in keeping with the well-established rule that employees in management or supervisory positions, or those engaged in work that requires a high degree of trust, are held to a higher standard of conduct. These include teachers,[123] union officials and managers.

For instance, in *Primiani*, discussed above, the arbitrator noted that the behaviour, although confined to a small group of employees, was particularly troubling as it involved managers. As Arbitrator Kirkwood stated:

> The evidence was very clear that there was a permissive atmosphere among certain managers and other bargaining unit employees. In the context of 3500 employees, it may not have been a large number, but it was within a group and it did involve managers.[124]

---

[123] See *Seneca College*; See also: *Re Chignecto-Central Regional School Board and Nova Scotia Teachers' Union* (2004), 126 L.A.C. (4th) 267; *Re Catholic District School Board of Eastern Ontario and Ontario English Catholic Teachers' Association* (2004), 123 L.A.C. (4th) 193.

[124] *Consumers Gas supra* note 89 at 73.

In the *Krain,*[125] case, the dismissed employee, who held the position of Information Technology Assistant, had downloaded pornographic material including images of "adult female and male nudity and hardcore sexual acts between adults, video presentations with such titles as "xxx bring'um young", "barely legal", "mm-freshmeat", etc., naked pictures of a grossly obese woman and one who was obviously elderly, and a graphic video of what appears to be sex between a woman and a dog, as well as pirated applications and games from the internet during working hours.

The bank had an extensive policy in place which allowed for occasional personal use of the internet for web browsing but which explicitly prohibited the viewing and downloading of offensive and copyrightable materials. The policy went on to define what constituted "offensive or inappropriate material" for the purpose of the policy. Despite the fact that the policy also stated that contravention of the policy was "subject to disciplinary action up to and including termination of employment for cause", Mr. Krain attempted to argue that he had never been "personally" warned that such behaviour could jeopardize his job. Arbitrator Luborsky was not persuaded by that argument:

> ... even if he was unaware of those policies, as a 10 year employee working in the Information Technology sector, one would reasonably expected that the Complainant would not require a "personal warning", nor even notice of a written rule to know that his time in the workplace and the Bank's computer and Internet facilities were not to be used to download and view pornographic/demeaning images, and unlicensed software applications and games.[126]

In this case, despite Mr. Krain's otherwise unblemished ten year record, and the fact that he was apparently genuinely remorseful, Arbitrator Luborsky refused to overturn his dismissal.

A similar approach was adopted in the case of *Greater Toronto Airports Authority.* In that case the grievor was employed in a supervisory capacity and had also been the union's local president for 8 years, up to the date of his termination. The union attempted to argue that the 1997 internet policy "did not register with" the grievor" because computers with internet access only became available in the workplace in 1998. The arbitrator did not accept the grievor's argument and stated that "...as a union official he needed to know the employer's rules so as to represent his members accused of violating same. If he knew them when performing as a union official he could hardly not know them when performing as an employee."

Similarly, in *Treasury Board (Solicitor General Canada – Correction Service) and Briar,*[127] correctional officers in a jail were disciplined after it was discovered that they had been using the employer's email system to send pornographic material including one email containing a video that was "exceptionally vile, revolting and depraved." Arbitrator Taylor considered the nature of the employer's work and the significance of the grievors' positions:

> It must be said that the Correctional Service is an employer which must continuously strive for public confidence and respect. The activities engaged in by the grievors can only detract from that objective.

---

[125] *Krain supra* note 74.

[126] *Ibid.* at para.17.

[127] (2003), 116 L.A.C. (4th) 418.

> In many respects, correctional officers must be seen as role models for inmates in the correctional system. Inmates are, among other things, reforming behaviour which is socially unacceptable. The type of activity engaged in by the grievors is not socially acceptable and is at odds with their positions as correctional officers.[128]

The arbitrator did not interfere with the discipline that was imposed by the employer, which involved unpaid suspensions ranging from five to seven days.

Addiction as a Defence?

In imposing discipline on online abusers, employers should also be aware that arbitrators have been willing to entertain the possibility that internet addiction, either independently or as a part of a larger psychological problem, may qualify as a disability in certain circumstances. If so, it would be deserving of reasonable accommodation under provincial human rights legislation. Interestingly, there are apparently web sites dedicated to dealing with "virtual addiction", some of which even provide self-diagnostic surveys.[129]

In the case of *Greater Toronto Airports Authority and the Public Service Alliance of Canada (Gorski)*[130], the grievor, the superintendent of airport statistics who had been employed with the employer for eighteen years, was discharged for abusing the internet at work. The grievor had accessed pornographic material using a communal department computer after his normal working shift. These sites were "mostly of young adult women in various stages of undress or exotic dress, some engaging in sexual activities of various sorts."[131] In trying to persuade Arbitrator Murray that the grievor was "an employee with a problem, not a problem employee", the union argued that the grievor's behaviour, and his compulsion for the internet, was a disease that should be reasonably accommodated by the employer. The arbitrator rejected the union's argument, and stated that "to the best of my knowledge compulsive viewing of internet sites (of whatever nature)" has not been accepted as a treatable disease 'meritorious of accommodation'". However, Arbitrator Murray did not foreclose the possibility that such a compulsion could be considered a disability: "[w]ere the union to have adduced evidence through qualified medical or psychiatric witnesses that it is such, the outcome of this case might have been different."

The dissenting opinion in the case of *Dupont (Maitland Site)*[132] is also interesting in this regard. In that case, the grievor was a controller with ten years of service. He was terminated after it was discovered that he had, in the hopes of evading detection, used another employee's computer to download pornographic material from the internet. While the majority opinion did not address the issue of addiction, Arbitrator More in dissent approached the matter from that perspective. He stated that:

> This grievor was clearly addicted to accessing pornographic material on the computer. Thus, the Board ought to have viewed this case from the perspective of a worker with an addiction.

---

[128] *Ibid.* at paras.68-69.

[129] See for example Virtual-Addiction.com and netaddiction.com.

[130] [2001] L.C.C. No. 3974 [*Greater Toronto Airport s Authority*].

[131] *Ibid.*

[132] *Dupont (Maitland Site) supra* note 57.

> An addiction, whether related to alcohol, drugs or other compulsive behaviour, produces a pattern of denial and activity designed to hide or camouflage the addictive behaviour. These symptoms were present in this case. The grievor chose to hide his addiction, using the office of another employee in an attempt to bypass the computer system user identification.

As part of his remedy, Arbitrator More would have ordered reinstatement conditional upon the grievor undergoing counselling for his addiction for a period of two years.

In the case of *Seneca College v. Ontario Public Service Employees Union*,[133] the grievor, a professor at the college, was convicted of possessing child pornography which he accessed using the employer's equipment and facilities. The union attempted unsuccessfully to argue that the grievor suffered from "a type of impulse control disorder that took the form of pathological attraction to internet pornography". The evidence adduced at the arbitration did not, however, support such an assertion. Although the grievor had been going through a period of turmoil in his personal life, there was no evidence that he engaged in the offending activity due to any medically recognized disability. The grievor was, however, diagnosed with clinical depression and became suicidal after the employer suspended him and before ultimately discharging him. As Arbitrator Carter held:

> The grievor through his own testimony indicated that his activity in searching out and viewing Internet pornography was both selective and controlled, suggesting that he could exercise self restraint if he chose to do so. Moreover, there is no medical evidence that the grievor was clinically depressed when he was engaging in this activity. While the grievor was unhappy about the social restraints that had been placed on his lifestyle by his parents and was seeking a form of escape from these restraints, these factors alone do not support a conclusion that the grievor was suffering from any medically recognizable mental disorder.[134]

The grievor in the case of *City of London and C.U.P.E., Local 101 (M.D.)*[135] was slightly more successful in arguing a case for addiction. In that case the grievor, who was a case worker in the Ontario Works division of the City, was terminated because of his increasingly insatiable appetite for viewing pornography from his workspace computer. The grievor, who worked with the employer for ten years prior to his dismissal and who had "never been disciplined prior...nor had he been criticized in any fashion for his work performance", admitted that at the outset he began to view the pornography "mostly during my lunch but occasionally during working hours. At the end, I'd log on first thing in the morning and it'd be minimized on my tool bar all day long."

At one point, the grievor had been spending from one to two hours every day while working viewing pornography online, which, as Arbitrator Marcotte noted, were "significant amounts of time." The grievor had a history of mental illness and the employer was aware that he had been diagnosed as a paranoid schizophrenic. The grievor was successful in arguing that he had an addiction to viewing certain sites and that his viewing of gay pornography online while at work was "causally related to his medical condition at the relevant times." In the end, the arbitrator found that the employer had just cause to discipline but that discharge was not an "appropriate disciplinary response in all the circumstances." The arbitrator substituted a 5-day suspension

---

[133] [2002] O.L.A.A. No. 415.

[134] *Seneca College supra* note 55 at para.16.

[135] (2001), 101 L.A.C. (4th) 411.

without pay, and reinstatement on the condition that the grievor continue to receive treatment for his mental condition, in place of the dismissal sought by the employer.

CONCLUSION

As technology continues to push forward, employers will increasingly find themselves dealing with new forms of employee misconduct. Some of the behaviour will "only" result in lost productivity. Others can lead to employer liability for things such as harassment, discrimination, and copyright violation. All of them expose the employer to a hit on their bottom line in one way or another.

It is critical for employers to be aware of the types of behaviour in which their employees might be engaging, and to use the preventative tools available to curb such behaviour. These tools are primarily strong written policies and technological aids to monitor and prevent abuse. It is vital that employers send a very clear message to their workforce that internet and email use will be monitored and inappropriate use of technology will not be tolerated.

In determining how to discipline online abusers, employers should be aware that decision-makers have applied the traditional regarding the discipline of employees. Ultimately, the punishment must be commensurate with the crime, taking into account all relevant contextual factors. Employees must be made aware that certain behaviour will have specified consequences; the behaviour and consequences should be spelled out as clearly as possible.

At the end of the day, technological advances will continue to increase the speed of business. Productivity will increase as more tasks are automated and information is made more readily accessible. However, these new technologies bring with them pitfalls which, left unchecked, can negate any productivity gains and expose employers to legal liability for the behaviour of their employees. As they seek to take advantage of new technology, employers must also be vigilant in protecting themselves from it.