Université de Montréal

Situated Information and Communication Moralities:

An Investigation into the Personal Use of the Internet in the Office Workplace

by Adrian Cloete

Département de communication
Faculté des arts et sciences

Thèse présentée
en vue de l'obtention du grade de Ph.D.
en Communication

April 2016

Résumé

Cette thèse remet en question la perception négative, dominante dans la littérature et largement répandue dans les organisations, de l'utilisation personnelle d'Internet au travail. Une étude de cas a été réalisée auprès d'environ 80 d'employés et superviseurs dans un bureau d'un département du gouvernement canadien. La thèse confirme que, non seulement ces employés de bureau transgressaient-ils régulièrement des règles explicites conçus pour cadrer l'utilisation des technologies d'information et de communication (TIC), ces comportements étaient largement tolérés au sein du département. L'analyse des pratiques et interactions quotidiennes a révélé une relation entre des gestionnaires et leur personnel basée sur une confiance réciproque, mais pas absolue. Il ressort une moralité située fondée sur la promotion du professionnalisme et le maintien de la productivité. Le relâchement de contraintes organisationnelles autour de l'utilisation de l'Internet à des fins personnelles est utilisé comme outil de gestion par les superviseurs et cette flexibilité accrue est bien accueillie par les employés pour des raisons à la fois pragmatiques et psychologiques. Une sondage, des entretiens approfondis avec un certain nombre d'employés et gestionnaires et l'observation participante ont révélé un désir de paraître professionnel malgré les activités non liées au travail; une perception généralisée de l'utilisation d'Internet comme compensation informelle pour temps et effort; et un sens partagé de confiance entre des salariés et leurs superviseurs, ce qui favorise la satisfaction au travail et productivité. Avec ces observations, on offre des éléments de réponse pour expliquer comment les employés de bureau négocient ce qui est acceptable en termes de leur utilisation d'Internet non liée au travail, et comment les gestionnaires justifient leur application subjective des règles à ce sujet. Finalement, la recherche montre que l'utilisation personnelle d'Internet au travail peut rapporter des bénéfices et ne devrait donc pas toujours être vu comme du "cyber-loafing" ou du "time banditry" comme la littérature l'a principalement représentée depuis que l'Internet est arrivé massivement sur les lieux du travail. La forme et la faisabilité de restrictions organisationnelles sur ces pratiques devront faire objet de réflexion dans le contexte de brouillage accru de frontières entre le travail et la vie personnelle des employés de bureau du 21e siècle.

Mots-clés : Internet, cyber-loafing, time banditry, moralité située, zone grise morale, identité professionnelle, contraintes organisationnelles, confiance, productivité, brouillage travail-vie privée, appropriation des TIC, communication organisationnelle

Abstract

This case-study investigation challenges the negative perception by organizations and researchers towards the personal use of the Internet in the workplace. While confirming that office employees in the field site were breaking explicit rules governing the use of information and communication technologies (ICT), this thesis provides evidence of informal relations between managers and their staff built on a tacit toleration of rule-violation. Their daily practices and interactions revealed a relationship that was shown to satisfy the conditions of a situated morality in promoting desired occupational identities and relaxing organizational constraints. Survey results, interview responses and observations of about 80 office workers and supervisors in a Canadian government department uncovered a desire to appear professional in spite of the non-work-related activity; Internet use as an informal compensation for time and effort; and a shared sense of trust to foster job satisfaction and productivity. Through these findings, answers are offered to explain how office workers negotiate what is acceptable in terms of non-work-related Internet use, and how supervisors justify their subjective enforcement of rules. Lastly, the research showed that personal Internet use in the workplace can yield positive outcomes and should not always be seen as "cyber-loafing" or "time banditry" as the literature has predominantly portrayed it since the Internet age entered the workplace. Lastly, this thesis raises questions as to the value of employee monitoring and organizational restrictions amid the increasing blurring of work and personal lives of 21st Century office workers.

Keywords: Internet, cyber-loafing, time banditry, situated morality, moral gray zone, professional identity, organizational constraint, trust, productivity, work-life blurring, ICT appropriation, organizational communication

Table of Contents

List of Tables

To my Mom and Dad, who sacrificed so much to give me, and many others, opportunities to study and learn in life.

Remerciements

After two decades and three universities, I have learned much about pursuing a doctorate.

First, your thesis advisor is absolutely critical to success. With the patience of Job and her indefatigable faith in me, Prof. Lorna Heaton has caringly and powerfully made my Ph.D. possible. After she so warmly welcomed me as an *étudiant libre* into her *Technologie et organisation* class in 2007, I regret that I burdened her with my inability to complete my thesis sooner, especially as her first doctoral student.

Secondly, you cannot complete any diploma or degree without the expertise and encouragement of faculty, colleagues and family.

Along with Lorna, both Prof. Pierre-Léonard Harvey and Prof. Serge Proulx kindly guided this anglophone through productive discourses and defenses. I am also grateful to Prof. André-A. Lafrance for bringing in the helpful critique of a very supportive external reviewer, Prof. François Lambotte of the Université Catholique de Louvain. And, as the university dean's representative, Prof. Victor Y. Haines III rounded out a kindly thought-provoking jury.

Senior federal bureaucrat and true public servant Peter Larose made a courageous decision in a risk-averse organization to grant me access to a research site of dedicated employees who provided their frank insights.

Michelle, my best friend and soul mate who is next to finish her doctorate, never gave up on me as I nearly perfected the art of procrastination. And, our darling Brontë who is set to earn her MD in 2017, served as a role model of a dedicated student who always works so hard to attain her academic and career goals.

Lastly, my parents and family provided the prayers and wishes to yield this "by-the-grace-of-God" thesis.

In a long document like a thesis, one often searches for words to cut, but I want to preserve the following verbatim messages because these sentiments embody my long path to graduation:

I wanted to say that you don't need to feel that you are alone in finishing the thesis. I'm here to help you – read drafts, comment on them, etc. I'm REALLY glad that you're planning on finishing. We can do this. – Lorna

When can we book tickets to our family reunion in Montreal to celebrate your graduation? – Keith, Louise, Merle and Anita (my encouraging siblings)

I love you…you are so smart and I know you can finish your thesis. I will help keep you focused. You can do it…you know you work your best under pressure. – Michelle (and Minuit)

Dad, you've got this! – Brontë

Introduction

People are going to work to *not* work.

For the past three decades, research and media reports have shown that employer-employee practices related to the personal use of the Internet in North American organizations are fraught with unresolved issues and unforeseen consequences. In spite of signed policies prohibiting specific actions and electronic monitoring, employees are regularly updating their social media personas, shopping or playing games online, bidding at Internet auctions, writing personal email messages, visiting pornographic sites, and downloading copyrighted music. In some instances, employees are losing their jobs over their personal Internet usage in the workplace.

For the purposes of this thesis, these practices will be referred to as personal Internet use or non-work-related computer use. They will be defined as the workday use of an organization's hardware and/or software resources to access the Internet for activities unrelated to the organization, often described pejoratively in the literature as "Cyber-slacking" and "Cyber-loafing" (Lim, 2002) or Time banditry (Martin et al, 2010, p. 26). In articulating the notion of cyber-loafing, Lim (2002) argued that information and communication technology (ICT) has revolutionalized taking breaks at work through its apparent invisibility, unlike face-to-face chats among colleagues about personal matters.

> Employees can now not only engage in loafing on the job; they can literally enjoy the best of both worlds by maintaining the guise of being hard at work in the real world while, in effect, travelling through cyberspace by surfing Web sites for personal interests and purposes…Cyber-loafers need not be absent from the office for inexplicably long periods of time, as long lunchers do. Cyber-loafers also need not

> worry as much about the visibility of their loafing compared to the restroom-minded or those who hang out by the watercoolers to chat. (Lim, 2002, p. 678)

In spite of any perceived cloak of invisibility adorning employees, North American companies devote huge resources to Internet filtering, reporting and surveillance tools to uncover Internet abuse and "cyber-slacking" employees (AMA, 2005). By 2001, three-quarters of all major U.S. firms were recording and/or reviewing the email messages, telephone calls, Internet connections, and computer files of their employees to fight against the personal use of ICTs. This percentage represented an almost 100% increase from the same survey conducted in 1997 (Nord et al, 2006). Typically, employers inform employees of the electronic surveillance through Acceptable Usage Policies (AUPs) designed to regulate access to the World Wide Web, but with little apparent success. In a dire prediction, Lim (2002) concludes that cyber-loafers may pose a greater "threat" to organizations relative to other types of loafers, in terms of productivity losses and costs incurred.

However, this thesis will posit that an inherently negative perspective, as part of the broader Organizational Misbehaviour and Counter-productive Work Behaviour domain, may have stifled an examination of the positive effects of this ICT workplace phenomenon. In fact, we will explore unintended consequences – both positive and negative – arising from employer-employee relationships as examined in pre-ICT workplaces, benefiting from the work of Donald Roy (1959), Alvin Gouldner (1954), Michel de Certeau (1984) and others, to help us understand the dynamics surrounding the personal use of the Internet in the workplace.

To deepen an understanding of employer-employee practices related to the personal use of the Internet in North American office workplaces, this thesis focuses on the emergence and sustainability of moral codes in an organizational context. Research into the notion of situated moralities in the workplace – expanding the concept of Anteby's (2008) "moral gray zones" beyond the context of industrial assembly lines – will prove most useful. Essential to understand authorized and unauthorized activities are various areas of organizational sociology, behavioural ethics, counter-productive work behavior, involving both informal and formal supervisor-employee dynamics – planned and unintended – as well as issues of control and surveillance in office workplaces dominated by ICTs.

To probe and analyze the relations between employers and employees surrounding the personal use of the Internet, a case-study approach was utilized in this investigation. The field site is a branch, or functional work unit, of a federal government department based in Gatineau, Québec. The managers and their staff of this branch served as the potential participants of an anonymous questionnaire followed by participant-observations and in-depth interviews. A document analysis of employee guidelines and policies related to personal Internet use in this work site was also undertaken.

This thesis begins with a Literature Review that seeks to provide an overview of several diverse and relevant bodies of literature, such as organizational sociology and behavioural ethics, featuring issues of control, authority, rules, moral codes, psychological contracts and compliance, plus organizational misbehaviour and counter-productive work behaviour theory, and the domains of surveillance and privacy as they relate to the workplace. The Problematisation is presented in Chapter two where the problem is identified, leading to the central research questions and followed by a description of the conceptual framework used to carry out the research. The third chapter describes this investigation's ethnographically inspired methodology, as outlined above. Chapter four presents and describes the results of the survey, interviews and observations, followed by the analysis of results in the final chapter.

The thesis ends with conclusions outlining the contribution of this investigation, its limitations, plus ideas for future research.

Chapter 1: Literature Review

1.1 Introduction

Tensions around of authority and control have always been present in organizations through the actions, rules, ethics and resulting relationships among employers and employees in the workplace. Organizational misbehaviour literature probes reactions of obedience and resistance among employees, largely viewing workplace actions and relationships from an individual perspective, with some of the ethics and resistance literature seeing the situation in a social context. When it has been explored, the personal use of Internet in the workplace – often in defiance of organizational rules – is a new terrain for manifesting these tensions. The dominant perspective in the last three decades has been to view this phenomenon as a theft of company resources and time; however, if we cast a spotlight from previous studies of supervisor-employee relationships – with a tighter focus on unintended consequences – we can see the benefits of personal Internet use in another light.

Several diverse bodies of literature are useful for this investigation into the dynamics surrounding the personal use of the Internet in the workplace. Arising questions and issues have been considered from different perspectives, such as organizational sociology and behavioural ethics – specifically surrounding issues of control, authority, rules, moral codes, psychological contracts and compliance – to organizational misbehaviour and counter-productive work behaviour theory. Lastly, we segue into domains of surveillance and privacy and their impact on the relations between an employee and her employer.

We will begin by exploring traditional approaches to organizational control, ethics and misbehaviour in the workplace. In Part two, we look at the unintended consequences – both positive and negative – arising from relationships between employer and employees, featuring Gouldner's couplings, May's "Effort Bargain", de Certeau's acts of resistance, and Lyon's research into modern-day surveillance. Lastly, we will take directions from the traditional, largely industrial organizational approaches on a path to better understand the use of the Internet by first acknowledging the phenomenon of cyber-loafing but then stopping to experience Roy's "Banana Time" and other positive outcomes.

1.2 Control and Rule-breaking in Organizations

In Charles Dickens' classic tale, *A Christmas Carol*, readers feel great pity for Bob Cratchit, the beleaguered clerk who receives insufficient wages to feed his family a proper Christmas dinner and who barely obtains permission from Ebenezer Scrooge to enjoy the festive occasion. Yet, Cratchit remains loyally under the control of his employer for fear of landing in the debtors' prisons or treadmills of England in the mid-1800s. Back then, the control that employers yielded over employees was clear: obey your boss, or lose your job and be relegated to the legions of impoverished victims of the Industrial Revolution. In the last century, however, far less drastic options have emerged for employees, along with complex duties, thereby forcing organizations to develop strategies and tactics to maintain a more sophisticated type of control in the workplace.

In *The Control Revolution*, James R. Beniger (1986) defines control as the "purposive influence toward a predetermined goal" (p. 7). And, from a career management perspective, Gene W. Dalton (1971) lauds A.S. Tannenbaum's 1962 explanation: "The coordination and order created out of the diverse interests and potentially diffuse behaviours of members is largely a function of control.” (p. 3) Understanding ways to influence, or control, employees towards predetermined goals within an organization has evolved from industrial to post-industrial to Internet workplaces.

Organizational studies theorist Richard C. Edwards has summarized three broad strategies that have evolved from the modern organization's struggle with controlling the activities of its members, or employees (Edwards, 1981).

1. **Simple control:** the direct, authoritarian, and personal control of work and workers by the company's owner or hired bosses, as seen in Dickens’ Bob Cratchit character mentioned earlier.
2. **Technological control:** this control emerges from the physical technological infrastructure of a company, such as the assembly line found in traditional manufacturing.
3. **Bureaucratic control:** this type of control is derived from the hierarchically based social relations of the organization and its systemic rational-legal rules, best articulated by Max Weber and his “iron cage” analogy.

Since Gouldner’s analysis of relations among bosses and workers in a mine will prove insightful later, his views on Weber are relevant here. As Hallett and Ventresca (2006) point out, Gouldner associated Weber’s “iron cage” with his own “Punishment-centred bureaucracy”. However, he rejected Weber’s description of bureaucracy as a formal structure of oppressive conformity and the legitimacy of authority simply on the grounds that it evoked consent (Hallett and Ventresca, 2006). Lastly, while acknowledging that his own “punishment-centred” model is least likely to incorporate interactions in support of legitimacy in the eyes of employees, Gouldner pointed to two other models in his taxonomy – “Mock bureaucracy" and "Representative bureaucracies" – that can create implicitly and explicitly productive relations between workers and managers (Hallett and Ventresca, 2006).

Clegg and Edwards (1981) have articulated the evolution and application of the three summarized types of control: Simple, Technological, and Bureaucratic. "(However), the development of these systems of control has been uneven across different sectors of the economy," Clegg (1981) observes. Barker successfully posited a fourth approach in his 1993 work, *Concertive Control in Self-Managing Teams*. "This form, called concertive control, grows out of a substantial consensus about values, high-level coordination, and a degree of self-management by members or workers in an organization." (Barker, 1993, p. 408) In a post-bureaucratic organization – no longer structured as a rule-based hierarchy – an employee works with a team of peers who are all equally responsible for managing their own work behaviors (Barker, 1993).

Barker's Concertive control of these self-directing, self-managing teams is helpful to this investigation by addressing the employee relationships in counter-productive behaviour. He observes:

> Under bureaucratic control, employees might ensure that they came to work on time because the employee handbook prescribed it and the supervisor had the legal right to demand it, but in the concertive system, employees might come to work on time because their peers now have the authority to demand the workers' willing compliance. (Barker, 1993, p. 412)

John Van Maanen's 1977 concept of "organizational socialization" explains how organizations may use veteran employees to exert and sustain control over new employees. Long-time employees can contribute to an organizational culture that is maintained as a way of coping with an environment. Therefore, a knowledgable and productive employee is the organization's channel to ensure continued operations with incoming employees.

> Put bluntly, new members must be taught to see the organizational world as do their more experienced colleagues if the traditions of the organization are to survive. The manner in which this teaching/learning occurs is referred to here as the organizational socialization process. (Van Maanen & Schein, 1979, p. 3)

While Van Maanen's concept explains socialization of new employees, it does not provide insight into how long-term employees socialize themselves to changes in the organizational environment, such as the new availability of ICT resources. Elements of response many be found in Van Maanen's later work. In *Occupational Communities: Culture and Control in Organizations,* Van Maanen and Stephen R. Barley (1984) defined an occupational community "as a group of people who consider themselves to be engaged in the same sort of work; whose identity is drawn from the work; who share a set of values, norms, and perspectives that apply to but extend beyond the work-related matters; and whose social relationships meld work and leisure." (p. 287) These occupational communities create and sustain relatively unique work cultures consisting of:

- task rituals;
- standards for proper and improper behaviour;
- work codes surrounding relatively routine practices; and
- compelling accounts attesting to the logic and value of rituals and standards.
  (Van Maanen & Barley, 1984)

The tools of these communities include codified rules examined in the next section.

1.2.1 Codes of Ethics

Corporate codes of ethics are written policies that set out expectations for business-related activities and behaviour within an organization, often embodying a collective set of ethical values (Schwartz, 1998). These codes serve as a top-down contract between the employer and the employee. Despite the prevalence of policies and codes in large organizations, there is relatively little empirical evidence available regarding their effectiveness on perceptions and behaviour among employees (Callan, 1992; Cleek & Leonard, 1998; Murphy, 1995; Weeks & Nantel, 1992 in Van Zolingen & Honders, 2010, p. 385).

Indeed, the dissemination of a document featuring lists of permitted and forbidden behaviours – manifested in a corporate code, policy or similar document – appears insufficient for comprehensive compliance. In the purview of our investigation, Lim (2002) argues that acceptable use policies (AUPs) for ICTs can serve to reduce cyber-loafing. However, Schwartz (1998) contends that any written document is only a small component of the overall explicit and implicit "ethics program" of an organization that seeks to encourage ethical behaviour. A workplace ethics program is defined as a coherent system of documents, activities and cultural norms designed to foster compliance with organizational policies. *Explicit components* of this program include: codes of ethics, policy manuals, employee training materials, employee orientation programs, ethics seminars, management speeches, management ethics decisions, board of director decisions and committee activities, internal control systems, and ethics staff activities. *Implicit components* include: corporate culture, incentive systems, valued behaviours, promotion policies, performance measurement systems, and management behaviour. (Schwartz, 1998)

Therefore, a norms-based approach to convey acceptable behaviour appears equally, if not more important. To be effective, an ethics policy has to be reflected in behaviour. “Discrepancy between the policy and the behaviour (‘the talk and the walk’) corrodes the ethical tone of an organization.” (Balch & Armstrong, 2010, p. 294) However, research also shows that a combined contract and norms-based strategy is insufficient to guarantee ethical behaviour in the workplace. Other conditions, stemming from the individual, the action, and the organization, have been identified as important.

For example, a variety of individual factors, such as gender, dispositions, and attitudes, has been linked to the ethical reasoning process (Bergman et al., 2002; Franke et al., 1997; Trevino & Youngblood, 1990 in Valentine et al, 2010). As well, an employee’s “positive job response” – defined as job satisfaction and intention to stay in the organization – has been found to influence his/her level of ethical job performance (Valentine et al, 2010). Also, research shows that an ethical issue’s perceived seriousness or its ‘‘moral intensity’’ impacts ethical reasoning (Barnett & Valentine, 2004; Jones, 1991 in Valentine et al, 2010). Lastly, a firm’s ethical climate, or culture, and the ethical leadership of top managers will influence employees’ ethical decisions regardless of a contract or norms-based approach (Trevino et al., 1998; Victor & Cullen, 1988 in Valentine et al, 2010).

Research into psychological contracts in the workplace has been deepened by Greenbaum, Folger and Ford (2011) who found that “employees may respond unfavorably to organizational unethical behaviours, even if employees are not affected by the behaviours, because the organization failed to uphold the perceived promise of abiding by moral obligations." (p. 199) Indeed, a *moral contract* arises to focus on behaviour that violates principles of morality. One example provided by Greenbaum et al (2011) occurs when an employee believes that his organization should not violate environmental standards, even if the action won't affect the employee, because the action would violate "a principle of morality". (p. 215) However, this type of analysis does not acknowledge instances where both parties share the same moral compass, specifically, perceiving that breaking organizational rules are acceptable.

Fichtner and Strader (2014) reviewed 22 studies involving Non-work-related computing (NWRC) issues in relation to job dimensions and work outcomes. Several of the areas of common ground among the studies pointed to a situated morality. For example, "the more opportunity an employee has to spend time on the Internet at work, the higher his or her perception that NWRC activities are acceptable" and "social norms of co-workers and friends affect an individual's NWRC behaviors. If co-workers and friends engage in NWRC behaviour, an employee is more likely to do so as well." (Fichtner & Strader, 2014, p. 74) As we have seen, there are many factors that must come together to fully guarantee that employees adopt an ethical approach to all their decisions and actions.

> Ethical organizations are ethical not because they say they are or because it has been mandated but because it is the very essence of who they are. Ethics is part of every policy, procedure, and practice. It is a way of being for every member of the organization. It is at the heart of their culture. (Sloan & Gavin, 2010, p. 59)

1.2.2 Organizational Misbehaviour

Looking at this issue from another perspective, one may ask, what is happening when employees do not take the right, or ethical, action? To deepen an understanding of current employer-employee practices related to the personal use of the Internet in North American office workplaces, it is valuable to explore the domains of *Organizational misbehaviour* (OMB) and *Counter-productive work behaviour* (CWB). OMB generally encompasses low-intensity behaviour, such as taking excessive breaks, spreading false rumours and withholding effort, to more serious behaviours such as sabotage, verbal abuse, and physical assault (Namasivayam & Lin, 2005). CWB is somewhat synonymous, ranging from work avoidance or misuse of resources to more severe behaviours such as physical aggression and violence, substance abuse, absenteeism, theft, destruction of property (Dilchert et al, 2007).

In their oft-cited topology, Robinson and Bennett (1995) articulated four types of employee wrongdoing in organizations:

1. **Property deviance**: when employees acquire or damage property belonging to the organization;
2. **Production deviance**: employee behaviours that violate organizationally established norms of quality and quantity;
3. **Political deviance**: behaviours that cause other individuals to be at a political or personal disadvantage;
4. **Personal aggression**: behaviours that are hostile or personally aggressive against other persons.

When employees deviate from stated or widely accepted rules and conventions in the workplace, these transgressions are described as OMB and CWB. Although many terms are found in CWB literature, such as workplace deviance, organizational misbehaviour, they all describe actions that are "negative for the functioning of the organization and intentional". (MacLane & Walmsley, 2010, p. 62)

Vardi more precisely defines OMB as "any intentional action by members of organizations that defies and violates (a) shared organizational norms and expectations, and/or

(b) core societal values, mores and standards of proper conduct." (Vardi, 2001, p. 325) Others describe these types of actions as "deviant workplace behaviours" (Goldman, 1992; Robinson & Bennett, 1995; Robinson & Greenberg, 1998), "unconventional practices at work" (Analoui & Kakabadse, 1992), "non-compliant behaviour" (Puffer, 1987) or in general "antisocial behaviour" (Giacalone & Greenberg, 1997) (all in Vardi, 2001, p. 325). Vardi (2001) further notes that some organizational misbehaviours are not necessarily dysfunctional or designed to cause damage.

The use of ICTs in the workplace for an employee's personal interests has become predominantly framed within this OMB and CWB literature (Lim 2002) and falls under "production deviance" (Robinson & Bennett, 1995).

1.2.3 Rule-Breaking

So, what leads to organizational misbehaviours or counter-productive work behaviours? And, more specifically, for the purposes of this research, why are *some* written rules respected by employees while *others are not*? Lehman and Ramanujam (2009) focused on selective compliance with external rules, such as formal laws and regulations. Selectivity may be especially influenced by the perceived benefits of internal rule violations as solutions to attain organizational outcomes (Lehman & Ramanujam, 2009).

Martin et al (2013) have articulated two key dimensions of organizational rule-violation as both patterned and interactionally mediated, namely:

1. Rule-breaking may be permitted or contested by those charged with enforcement. Incidents become routine where violations are unofficially allowed; where they are not allowed – officially or unofficially – employer-employee conflict arises, understandably.

2. Rules can be broken by individuals acting alone, by workgroups, or sanctioned by management as "unofficial policy".

For the first type of rules that are broken, Martin et al argue (2013) that employees may even be unaware they are violating company rules. "Rules are not always clearly defined; it is probable that routine rule violations are justified by the way in which actors interpret them. In other words, rule ambiguity creates the opportunity for organizational actors to ignore the rule." (p. 553) Given the widespread and regular dissemination of Internet use policies, the second type of rule-breaking is more apt where rule-breaking is not an individual choice, but a collectively organized choice based on the expectations of the broader group (Martin et al, 2013, p. 556).

Lim's observation of an "imbalance in the employment relationship" (2002, p. 687) serves to raise the issue of control and compliance in the workplace surrounding the use of the Internet. Clegg's focus on rules sheds some light on the dynamics because it is clear that well-defined rules prohibiting the personal use of the Internet are being broken. Clegg (1981) explains that "layers of rules exist in a dynamic relationship with each other." (p. 551-552) Employees are clearly ignoring the "layer of rules" or control created to regulate workplace Internet usage while, at the same time, they are complying with the other layers that regulate office hours, parking spaces, discrimination policies, and smoking. As well, Clegg's (1981) elaboration of Weber's model of bureaucracy may not be precise enough for the level of analysis needed to understand employee behaviour, specifically counter-productive behaviour. Critical Organizational Studies largely views workplace dynamics in terms of power, the labour process, and institutions; individuals are not as important because something larger is controlling everything. Clegg (1981) contends that power stems from the ownership and control of the key resources of production, namely means and method. In today's office workplace, there is power at the macro-level, i.e. company managers could turn off their Internet servers; however, the control is not comprehensively effective at the individual level as employees continue to shop online and download pornography during work hours. For this investigation – with its focus on particular situations, behaviours, actions and moralities – a systemic power perspective will not be taken.

1.2.4 Unintended Consequences of Rules

Emerging from initiatives aimed at control is the well-documented and manifold thread of unintended consequences – both positive and negative. For example, in their 1971 compilation, *Motivation and Control in Organizations*, Dalton *et al* describe scientific management with its established methods of performance standards and incentives for employees who met those standards under the control of the manager. They documented many unanticipated consequences of control, giving birth to their notion of "collusive resistance" (Dalton, 1971).

> Often when they (managers) least expect it, they encounter restriction of output or departmental in-fighting. On one hand, they find what seems to be apathy, and indifference; yet on the other hand, they keep discovering remarkably ingenious methods developed by their subordinates for beating the system. (Dalton, 1971, p. 1)

Dalton (1971) argues that resistance – both social and psychological in nature – leads to further controls, and the cycle of unintended consequences continues. "Merton, Selznick, and Gouldner all noted that efforts to control the activities of members of the organization have both intended and unintended consequences and that these consequences tended to lead managers toward further use of controls." (Dalton, 1971, (p. 5) Specifically related to the Internet, Garrett and Danziger (2008) suggest that some types of online activities are an employee's hostile response to perceived workplace grievances. Indeed, this is just one of the many areas of unintended consequences. More are examined in the next section when we explore workplace relationships as well as the impact of increased surveillance. However, the potential consequences of a rise of a subversive revolt should be acknowledged briefly here. For example, is there a "subversive way of life" developing among office workers in reaction to an over-regulated post-modern society? "I transgress; therefore, I am alive", explained Professor Pierre-Léonard Harvey (Lecture, Dec. 3, 2008) in articulating an emerging reaction to the over-control of uses of new technologies. "The social context is more important than the organizational context" in this area, he added. Clearly, organizations are not worlds in and of themselves, and larger societal trends also enter into play. While one can debate the more dominant force, social and organizational contexts are clearly interdependent.

1.3 Dynamics of Employer-Employee Relations

Recognized as a pillar of organizational sociology, Gouldner's (1954) "Patterns of Industrial Bureaucracy" documented four stages of couplings or relationships among workers and manager in a 1950s gypsum mine:

1. A pre-bureaucratic "Indulgency pattern" that characterized the relationship between workers and their long-time manager;
2. A "Punishment-centered bureaucracy" imposed by a new manager with expectations for bureaucratic efficiencies and increase productivity;
3. A "Mock bureaucracy" that grew out of the resulting conflict revealed a power struggle and generated a loose coupling;

4. A "Representative bureaucracy" based on cooperation and a more tightly coupled form based on shared interests between workers and the manager.

Of particular relevance to the personal use of the Internet in the workplace – specifically the compliance with workplace rules – are the Indulgency pattern and the Mock bureaucracy. The Indulgency patterns among the miners developed from and were "enmeshed in a network of kinship relations" (Gouldner, 1954, p. 65). While this familial network does not apply to today's office workers, the workplace dynamic around the personal use of the Internet could feature leniency, a flexible application of rules, and second chances, so gypsum miners may help us understand the non-compliance of Internet policies.

Gouldner (1954) explains his Mock bureaucracy as a work pattern in which bureaucratic rules are in place but are largely ignored or inoperative. "As an instance of loose coupling, the Mock bureaucracy involved an implicit agreement where the workers let the management save face and have their rules as long as they looked the other way as the workers went about their daily lives." (Hallett & Ventresca, 2006, p. 6) The example given by Gouldner was the no-smoking policy, akin to the rules related to parking spaces and Internet use in today's modern workplace.

> A chief example (of the Mock bureaucracy) involved the "no smoking" rules. These rules were formalized, but for the most part, the workers considered them "dead letters," and so did the management. The mine was filled with signs that proclaimed the rules and punishments, but these rules were not enforced, except when an insurance or fire inspector came to the mine. Both the new management and the workers agreed to this arrangement, and when it was breached, punishment occurred not through the formal warning notices but through informal interactions. (Hallett and Ventresca, 2006, p. 6)

Gouldner’s Indulgency pattern provides an organizational culture that offers an informal legitimacy and widely accepted behaviours where workers adhered to a set of informal rights and expectations. This type of organizational culture heralded unintended and implicit benefits for both workers and management, such as legitimacy, autonomy, trust and job satisfaction. Commenting on Gouldner’s case study, Hallett and Ventresca (2006) remark that the Indulgency pattern fostered a positive relationship between a specific manager and workers. “Where (the former manager) Old Doug trusted that the workers would get their jobs done, (the new manager) Peele put them on watch.” (p. 6) But, with the arrival of the new boss and the change to a different bureaucratic relationship, the “new emphasis on supervision violated the norms of equality that characterized the indulgency pattern” (p. 7).

Gouldner’s approach also introduces us to unintended perceptions and rationalizations of compensation, specifically a “reverse efficiency wage” on two levels: Firstly, the gypsum miners saw the Indulgency pattern’s leniency as an unofficial perk to compensate for the hazards of the work. “This was especially the case in the sub-surface mine, where the workers believed that the dangerous nature of the job gave them the right to take occasional liberties, especially in regards to absenteeism.” (Hallett and Ventresca, 2006, p. 7) Secondly, Gouldner noted the perception among some workers that their positive relationship with their former boss constituted part of their overall compensation; specifically, they could be satisfied with low wages as long as they were content with their treatment, in the words of one worker: "I like it here. They don't push you around. A man's got his work to do and they leave him alone. You know that's one of the reasons they pay so low around here. The pay is like a balance for the working conditions. It sort of balances things." (Gouldner, 1954, p. 32)

However, when the Indulgency pattern was broken, Gouldner’s miners stopped going beyond the call of basic duties, and the unintended impact on productivity was profound.

> Although punishment-centered bureaucracy could regulate basic behaviors, it could not regulate feelings and attitudes. The workers would not break any rules, but they would not put forward any extra effort or enthusiasm to make the product of their labor better. They would punch in and out of work exactly on time, but they would not volunteer for extra hours when gypsum orders were high. This kind of basic "activity" without sincere "participation" undermined the very productivity that the management sought to increase. (Hallett and Ventresca, 2006, p. 7)

In summary, Gouldner (1954) showed that employees supported informal rights and expectations in an environment where mock bureaucratic rules were mainly ignored. And, he contrasted this stage to the subsequent stage that would emerge and replace it:

> The imposition of a tight coupling between the logic of bureaucracy and everyday practices began to squeeze the life out of the indulgency pattern. The actions of the new management and Peele's efforts to create a tight coupling generated a particular form of bureaucracy that Gouldner (1954) labels "punishment-centered bureaucracy." In this tightly coupled pattern, formal rules are enforced for their own sake, regardless of their utility, and deviations are met with punishment. (Hallett and Ventresca, 2006, p. 6)

A thread in one of Gouldner's conclusions – specifically, that the tacit resistance of the workers sabotaged the legitimacy of their new boss – continued in May's (1999) look at resistance and unintended consequences in his revisiting of Roy's (1959) seminal research. Through a participant-observation of New York garment factory workers, Roy described a group of machine operators who kept boredom at bay through routine behaviours during break times. They basically made a game out of their monotonous duties through simple conversations, jokes and pranks along themes of "peach time", "window time", "pickup time" and “banana time". In "From Banana Time to Just-In-Time: Power and Resistance at Work", May (1999) identifies two factors for continual smooth relations in the workplace:

1. Employers mobilise strategies to extract the maximum effort from employees in the name of productivity.
2. Employees seek to balance the occupational and social costs associated with these strategies through the securing of sufficient remuneration for their effort. (May, 1999, p. 768)

May (1999) argues that both control and consent are necessary to secure this “Effort bargain” often with employers and employees occupying new “discretionary spaces” and with “episodes of resistance”. There is only so much control that employees can handle before they start to resist as May points out, with support from previous findings by Hodson, Graham and Mars.

> Hodson’s study also saw workers as highly creative in preserving ‘their autonomy in the face of excessive or inappropriate demands’ (Hodson 1991:55–6). […] Joking, fiddling, making out, sabotage and escape have become just some of the survival tactics that have been documented at work (Graham 1995; Mars 1982). (May, 1999, p. 769)

Notions of resistance and survival tactics are also seen in de Certeau as examined in the Problematisation chapter. De Certeau’s (1984) “tactics” are daily and brief gestures of rebellion against management without any positive goal intended for the organization. Specifically related to the topic of this investigation, in his 2002 study of cyber-loafing among office employees in Singapore, Lim found employees would intentionally break company rules to use the workplace computer for personal reasons as a means of retaliation against their organization. “Employees who are disgruntled because they perceive that there is an imbalance in the employment relationship as a result of unjust treatment would be inclined to reinstate a sense of justice into the relationship through cyber-loafing." (Lim, 2002, p. 687)

May concludes that:

> Strategies cannot be assumed to produce particular effects according to their intended logics, but often co-exist with the result that they produce conflicting effects, or have unintended outcomes…This has the potential to create spaces within unintended outcomes. It is within these spaces that practices and identities emerge at odds with the strategies that seek to stabilise and intensify the effort bargain (May and Buck 1998; Pile and Keith 1997). (May, 1999, p. 776)

Indeed, unintended and unforeseen outcomes related to surveillance are explored in the next section.

1.3.1 Surveillance and Control

In addition to the use of authority, implicit and explicit rules, as well as teams, we can also view control as pursued through surveillance and compliance by accomplishing two objectives:

1. Determine what employees are doing through surveillance; and
2. Obtain their compliance to do what they are hired to do.

Compliance was previously explored in this chapter along with rules and authority; however, the concept of Surveillance, with its own suite of unintended consequences, now warrants some attention. To begin, as a helpful backdrop, is Dalton's warning of the "control paradox":

> In many circumstances, the more managers attempt to obtain and exercise control over the behavior of others in the organization, the less control they have. Furthermore, often the less control they have, the more pressure they feel to exert greater control, which in turn often decreases the amount of control they have. (Dalton, 1971, p. 5)

Is there an elusive uncontrollability to the understanding and use of control within organizations? If so, can it be tamed to rein in post-modern employees who no longer work in fear of their Scrooge-like bosses but who seek to use the organization's access to the Internet for personal tasks while at work? The literature appears divided, especially when monitoring is introduced.

Panopticism, as articulated by David Lyon (2006), can help us analyze control in the workplace in relation to ICT uses and surveillance. Early surveillance theorists seized upon George Orwell and his *1984* dystopic novel of a totalitarian government that watches its people to such an extent that even the deepest fears of each citizen are known by "Big Brother". We still see remnants of this view in the popular press and in the work of researchers in disciplines outside sociology, such as Human Resources and Law. For example, Los (2006) appears to maintain this Orwellian view in her exploration of the "totalitarian potential of the late modern forms of regulation and surveillance." (p. 69) Her neo-Luddite view is strong: "I am focusing on the conditions and areas of vulnerability that could either facilitate a deliberate imposition of a totalitarian domination or have unintentional totalitarian effects." (p. 69) However, Lyon has been recognized for the "shift from the Orwellian vision of a dystopic society of total surveillance towards explanations based on Foucault's notion of disciplinary society." (Penfold, 2002, p. 222)

In 1791, social reformer Jeremy Bentham introduced the architectural design of a "panopticon" for the ideal penitentiary. Hier, Walby and Greenberg (2006) explain this design concisely:

> The idea of a panoptic prison consisted of an inspection tower surrounded by a semicircular structure that housed inmates in separate cells. Each cell was to be made

> available to the uni-directional gaze of the inspectors, and the utility of panoptic supervision was based on assumptions of uncertainty. It was believed that, because prisoners would not be aware of when inspectors were watching, a state of uncertainty induced by the visible – but unverifiable – expression of power ensured the normalization of discipline and self-control. (p. 231)

Almost 200 years later, Michel Foucault's *Surveiller et punir* work – translated into *Discipline and Punish: The Birth of the Prison* (1977) – revisited Bentham's work and extended the panopticon principles "as a model for understanding the operation of power in contemporary society" (Haggerty, 2006, p. 25). However, Lyon argues that the "panopticon" is no longer a viable theoretical construct to help us understand surveillance issues.

> Without careful theorizing, the growth of contemporary surveillance will be seen only in relatively shallow and superficial ways in media accounts and policy reports that depend only on descriptive and statistical data…For much of its work, as this volume attests, surveillance theory for the twenty-first century is obliged to look beyond the panopticon. (Lyon, 2006, p. 18)

Complicating matters, in recent decades, we have seen the emergence of an "electronic panopticon" in the analysis of ICTs and their use as tools of surveillance at home, at work, and in our communities. The electronic monitoring of people and actions through data, also known as "dataveillance", is now part of the same surveillance family as Closed Circuit Television (CCTV) and other traditional forms of monitoring, aimed at protecting a company's "physical" property or increasing productivity. Mazmanian et al's (2006) research into Blackberry use also touched on the notion of surveillance commonly used by employers to counter the personal Internet usage among employees. "For these users, the Blackberry is not experienced as an electronic leash or panopticon," observed Mazmanian (2006, p.3).

Indeed, one of the problems with the Panopticon framework is that the arena of surveillance has grown beyond penitentiaries and correctional services to include smartphones and manifold forms of other tools and applications, such as:

- Workplace surveillance
- Closed Circuit Television
- Reality TV shows, such as “Big Brother”
- eCommerce surveillance of web surfing, such as “cookies”
- Citycams in cities to deter criminal behaviour
- Citycams in public places to promote tourism
- Home webcams and web blogs
- Military applications of surveillance technology for warfare
- Anti-terrorism measures, such as data-profiling, databases, and biometrics
- Telemedicine
- Global systems for infectious disease control
- Monitoring of animal-borne microbes that can infect humans
- Surveillance in parenting

Bentham began with the ultimate venue for surveillance – the prison – to develop the panopticon. However, a casual observer can quickly see that the notion of inmates being watched by unseen guards in a central tower does not have much in common with many forms of surveillance, as listed above. As well, according to both Bentham and Foucault, the purpose of surveillance is “efficiency and economy of power”, but now it is serving many other purposes (Haggerty, 2006). “The panoptic model has been over-extended to domains where it seems ill-suited, and important attributes of surveillance that cannot be neatly subsumed under the “panoptic’ rubric have been neglected.” (Haggerty, 2006, p. 23) Independently articulated in "Supplementing the Panoptic Paradigm: Surveillance, Moral Governance and CCTV”*,* Hier, Walby and Greenberg (2006) similarly conclude "ethnographic research in CCTV control rooms has called into question the extent to which the panoptic paradigm can be applied uncritically and in a totalizing manner." (p. 231)

With specific goals, workplace surveillance initiatives often evolve in anticipated ways (Haggerty, 2006). In fact, many researchers have uncovered unintended consequences, including increased stress, reduced commitment, and decreased work performance (Tabak and Smith, 2005; Brown, 1996; Fairweather, 1999). Furthermore, in direct contradiction to one of the primary rationales for the use of electronic surveillance, Tabak and Smith (2005) found that some organizations do not even see an increased level of productivity. Indeed, Miller and Weckert (2000) raise the possibility that monitoring could cause a breakdown in trust, which could lead to a less efficient workforce.

> One of these questions is the relationship between monitoring and trust in the workplace. It would appear that monitoring is a sign of distrust, and perhaps employees who know that they are being monitored, and hence not trusted, will become less trustworthy, in which case they will require more monitoring. Superficially at least, it appears that monitoring could precipitate a breakdown in trust, which in the longer term would probably lead to a less efficient workforce. (Miller & Weckert, 2000, p. 263-264)

Going even further, Mary F. Cook in her Management Review article, "What's Ahead in Human Resources?" (1988) blamed the rise in employee theft and drug abuse – the traditional counter-productive behaviours along with alcoholism – for the increase in workplace surveillance. Miller and Weckert (2000) cite a myriad of studies that show employees who are monitored with computers suffer more health, stress and morale problems than non-monitored employees.

1.3.2 ICT Monitoring and Privacy in the Workplace

Where surveillance is used to exert control, the issue of privacy emerges. As far back as 1988, the issue of computer monitoring of workers caught the attention of U.S. politicians, such as California representative Don Edwards, who remarked, “We are becoming a surveillance society. Every day we see new abuses of the dignity of workers. People should not be forced to surrender their right to privacy when they go to work.” (as quoted in Cook, 1988, p. 42) But what are the expectations and effects of privacy in the workplace? In “Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development”, Tabak and Smith (2005) note:

> Privacy is especially problematic since it pits two central interests against one another: the individual’s right to be “left alone” and society’s (or the organization’s) right to know about those actions which are likely to cause it harm. For individuals, privacy is a necessary condition of self-determination (Rogerson, 1998). It is nearly impossible for employees to do their jobs in the manner they think is best if every conversation they have, every action they take or every moment of their day is recorded and observed by someone else. (p.185)

Miller and Weckert (2000) in “Privacy, the workplace and the Internet” have no problem with employers who prohibit Internet access for personal use. They then ask rhetorically: “Is it an unjustified invasion of privacy for employers to monitor their employees’ activity on the WWW, to check on the sites visited?” And their answer is a qualified ‘No’. “From a privacy perspective, there is no problem with restricting access to certain sites by the use of software. Monitoring sites visited, however, is not such an acceptable way of restricting access. Monitoring someone's use of the Internet in this way is a bit like monitoring library use.” (Miller & Weckert, 2000, p. 7)

And, the invasion of a basic right to privacy is more egregious when people are unaware that such surveillance is taking place, contend Tabak and Smith (2005). In "Monitoring for Pornography and Sexual Harassment" by Panko and Beh (2002), the balance between an employee's privacy concerns and an employer's right to monitor is best struck with signed consent. "Certainly this right is most clearly supported when the employer promulgates clear policies and regulations and the employee gives prior consent to monitoring because to do so reduces the employee's expectations of privacy on the workplace computer." (Panko & Beh, 2002, p. 85) However, the signed policies represent another problem, according to Nouwt et al (2005):

> Because employees reduce their reasonable expectations of workplace privacy by giving consent to an employer's search and monitoring policies, employers nowadays demand such consent as a standard business practice. As a result, consent to search and monitor is becoming implicitly acknowledged in the employment relationship. Adopting such a standard business procedure into regulation can diminish privacy expectations. (p. 341)

Further, Nouwt et al (2005) believe that the examination of workplace privacy must be shifted away from the task, that is, "…regulating workplace privacy is often focused on physical artifacts or techniques as the primary object of regulation, instead of the social relationship between the employer and his employees." (p. 341)

However, the always-on nature of electronic surveillance of computer activity, or dataveillance, presents a paradigm shift. "If a manager were to rifle through an employee's desk, it would cause an uproar. And yet, managers can easily go to a computer terminal and call up documents an employee is working on," remarks Cook (1988, p. 42) in "What's Ahead in Human Resources?"

On an emotional level, Brown (2000) raises an alarm for the impact on an employee's "inner self" caused by the invasion of privacy of electronic surveillance.

> Given the totality and depth of penetration of information gathering, one may reasonably ask, what does this mean for concepts of self?...Sociologists have concurred in the centrality of work in the defining of self and the derivation of meaning in life for the worker...how loss of privacy creates feelings of vulnerability, violation and shame at the exposure.
>
> Given the transparency of the worker's life to employer inquiries, one can legitimately raise the question if the level of employer inquiry now impinges on the inner self of workers. (Brown, 2000, p. 62)

In another adverse consequence, Greenberg and Barling (1999) found that aggression against a supervisor was predicted by two perceived workplace factors – procedural justice and workplace surveillance. As employees search for a better way to stay in control, there is much at stake. William S. Brown (2000) in "Ontological security, existential anxiety and workplace privacy" remarks:

> As technology develops at an ever-increasing rate, we must step back from it and question its impact upon the quality of human existence. Moreso than ever before, we must re-examine the direction technology is taking in the workplace, and the price it is exacting from our workers. (p. 5)

Lastly, since electronic surveillance renders the Internet usage of employees visible, another dynamic must be acknowledged. The "watched" can also be an actor in the surveillance – or, in this case, dataveillance – referring to workplace monitoring and calls centres, and other forms of surveillance where employees know they are being watched via ICTs.

In Koskela's (2006) "*The Other Side of Surveillance: Webcams, Power and Agency",* she notes, "Exposing oneself can be connected to identify formation...It is quite apparent from these sites that the person on the cam wants to be known." (p. 172) And she observes a distinction from other types of surveillance. "What seems to be essential to identify formation – and different from the surveillance contexts of being seen – is that the home webcam owners have agency in their project." (p. 172). Haggerty (2006) concurs: "The targets of surveillance as depicted in Foucault's *Discipline and Punish* are largely passive. What little agency they display is directed inward upon themselves in the form of an almost inevitable process of acquiescent 'soul training'." (p. 34)

1.4 Cyber-loafs or Cyber-benefits?

Both innocuous and malicious usage have long-led organizations to allocate huge IT resources for the electronic surveillance of their employees to confront issues such as legal liability, declining productivity, and misuse of company resources (AMA, 2005). As part of the 25th anniversary of the creation of the World Wide Web in 2014, Purcell and Rainie of the Pew Research Center found that US employers continue to change their practices regarding their employees' use of the Internet.

> Just under half of those surveyed say their employer blocks access to certain websites (46%) and has rules about what employees can say or post online (46%). The latter figure has more than doubled since Pew Research began asking about company rules about employees' online presentation in 2006. (Purcell & Rainie, 2014, p. 3)

In Lim's seminal 2002 research, she specifically positioned the personal use of the Internet at work on the Organizational Misbehaviour stage by observing, "the advent of technology has also opened up new avenues and opportunities for individuals to misbehave." (p. 675) Based on a study of almost 200 working adults in Singapore, Lim proceeded to define the term "cyber-loafing" as the act of employees using their companies' Internet access for personal purposes during work hours (2002, p. 675). Furthermore, Lim (2002) embraced Robinson and Bennett's topology by categorizing cyber-loafing as "production deviance". By 2006, the approach of Yulihasri et al had confirmed that the personal use of the Internet in the workplace had clearly fallen into the OMB domain with an all-encompassing judgement that *it was bad*.

> The problem of pervasive personal web usage in the workplace has become an issue to be tackled in the ever-growing interconnected world of today…The extensive use leads to work inefficiencies which, in turn, lead to lower productivity, and it gets translated into lower performance…This has become a prevalent problem that needs to be tackled to reduce the negative impact on productivity. (Yulihasri et al, 2006, p. 2-5)

In formulating the notion of "time banditry", Martin et al (2010) directly linked the CWB domain to the use, or misuse, of ICTs. "Time banditry, a variant of counter-productive work behaviour, is defined as the propensity of employees to engage in non-work related activities during work time…they are using paid organizational time for personal reasons." (p. 26) Martin et al (2010) also argued that time bandits are not a monolithic group of employees; rather, there are at least four types of bandits.

a. Weasels: the Engaged-Productive bandits
b. Mercenaries: the Unengaged-Productive bandit
c. Sandbaggers: the Engaged-Unproductive bandits

d. Parasites: the Unengaged-Unproductive bandits (p. 31)

Terms with clearly negative connotations have emerged, such as:

- *Cyber-slacking*: highly interactive behaviours which include online gambling, stock trading, online romance, chat, or visiting pornographic websites;
- *Cyber-loafing*: a more restricted set of less interactive non-work-related online behaviours, such as recreational Internet surfing, and personal email use.
  (Weatherbee, 2010)

Distinctions among the behaviours have been made based on the degree of ‘social-ness’, their utility, or their degree of interactivity (Johnson & Kulpa, 2007 in Weatherbee, 2010, p. 36). Still other researchers have separated the behaviours as a function of their potential for harm, for example:

- *Counter-productive Computer Use:* involves behaviours that may expose an organization to risk or liability as a function of the misuse of a firm's Internet access (e.g., illegal software downloading, distribution of pornography, exposing the firm's systems to viruses, or ‘malware’ through surfing).
- *Non-Productive Computer Use:* consists of behaviours which are assessed as posing essentially little or no risk to a firm's systems.
  (Mastrangelo et al, 2006 in Weatherbee, 2010, p. 37)

However, according to Weatherbee (2010), the examination of ICTs in the workplace is still evolving and under-studied in the OMB domain.

> While there is almost universal acknowledgement that the misuse of technologies at work should be considered ‘bad behaviour’, or behaviour that an organization would prefer not to have practiced by its employee, there is as yet no consensus at the broader conceptual level. (Weatherbee, 2010, p. 38)

Weatherbee blames the lack of consensus on the varied multi-disciplinarian approaches – focused on individual types or forms of behaviour, varying from technical, managerial, organizational, and psychological perspectives – resulting in “a broad and inconsistent use of terminology, definitions, and labels”. (Weatherbee, 2010, p. 36-38)

Despite the inconsistency, whatever label is used time banditry, cyber-slacking or cyber-loafing – the premise is the same: these activities of surfing and checking personal email “constitute an unproductive use of time in that they detract employees from carrying out and completing their main job duties.” (Lim, 2002, p. 677) Early analysis into this phenomenon, beginning in the late 1990s, often explained the behavioural towards the personal Internet use at work in terms of employee disaffection (Lim, 2002).

> Cyber-loafers can inadvertently end up chalking up a lot of time spent surfing the Internet, moving from one Web site to another simply with a click of the mouse. Also, cyber-loafers in their virtual travels may – unwittingly or otherwise – visit sites which expose the organizations to legal liabilities and to the dangers pose by computer viruses. (Lim, 2002, p. 678)

Van Gamberg et al (2014) identified three key ways for human resources managers to control the online behaviour of employees: policy and procedures in the workplace; monitoring and surveillance; and discipline and dismissal. Acceptable Usage Policies (AUPs) are designed to regulate access to the Internet in cases where it is not blocked. To increase compliance with corporate rules and policies, companies often invest in Internet filtering, reporting and surveillance tools to uncover egregious Internet abuse and “cyber-slacking” employees (AMA, 2005). In their 2013 study, Wang et al studied two methods of control – Internet use policies and electronic monitoring – among Chinese public servants working for provincial and municipal government agencies and found that both methods can “significantly lower employees' cyber-loafing intentions". Henle et al (2009) questioned the anecdotal evidence that organizations use to decide how to curtail employee use of company Internet and email systems for non-work purposes through electronic use. Instead they sought to provide empirical evidence and reporting results from two experiments and a field study that found that zero tolerance, progressive discipline, and appeal processes were related to higher perceptions of policy fairness while periodic monitoring was related to less cyber-loafing (Henle et al, 2009). However, this increasing workplace monitoring is resulting in unforeseen consequences of stress, lower productivity and job satisfaction among employees (Alder, 1998; Miller & Weckert, 2000).

Lastly, it has been shown that if employees do not perceive personal ICT usage as unethical or wrong, then organizational policies prohibiting their use – and even leading to discipline and dismissal – are limited in their value. In her 2002 study of office workers in Singapore, Lim concedes there may be a disconnect between the perception of what is "right" and "wrong".

> Employees can easily convince themselves that, by cyber-loafing, their misbehaviour is not unacceptable since they have accrued sufficient credits previously, through the time and effort which put into completing their work. Cyber-loafing is simply a means of 'cashing in' these accumulated credits and is viewed as a fair entitlement. In this manner, employees will find it all too easy to cyber-loaf while at work. (Lim, 2002, p. 689)

In the second and third decades of this ICT phenomenon, research continued to presuppose that cyber-loafing was bad for an organization by focusing on understanding the predictors (Garrett & Danziger, 2008), or employee behaviours (Vitak et al, 2011) or on ways to reduce its frequency (Wang et al, 2013). Thus, not only are these activities continually deemed inherently counter-productive, they are placed into a category that would limit or prevent an examination of a possible positive contribution to the workplace. Would the same be said of chatting about personal topics with colleagues at the water cooler or over the cube walls, as these non-technology based activities are also seemingly unrelated to job duties? And, if workplace disaffection factors, such as stress and dissatisfaction, have no significant influence on the extent of web surfing or personal email use (Garrett & Danziger, 2008), it may be time to focus more on the positive outcomes or benefits, such as stress *reduction* and job *satisfaction*.

1.4.1 Benefits of Personal Internet Use at Work

There is general research on the positive impact on productivity of taking breaks at work to chat with others – both face-to-face and virtually. A notable historical example is traced to English author Charles Dickens who, apparently, would work on his craft from 9am-2pm before taking long walks. "That sort of downtime, when you're not thinking directly about what you're trying to learn, or figure out, or write about – that downtime is a time of subconscious processing." (Oakley, 2014) As well, Levithin (2014) contends that by dividing their workdays into project periods – including segments for online social networking – people can become more productive and creative.

And, in his much-cited study of a New York garment factory in the late 1950s, Roy (1959) found that informal but ritualized breaks among employees could foster job satisfaction by decreasing boredom amid monotonous tasks. More than a half-century later, research conducted among white-collar workers in New Zealand found that some loafing yields positive benefits, such as increasing employees' level of job satisfaction. (Duhita &

Daellenbach, 2015) And, when given unfettered Internet access, employees working in medium-size organizations in Lebanon developed an increased level of job satisfaction and a decreased level of cyber-slacking (Messarra, Karkoulian, & McCarthy, 2011). Coker's 2013 study found that workplace Internet leisure browsing (WILB) restored the attentiveness of employees more than other types of breaks. Coker concludes that managers should not necessarily treat WILB as "cyber-loafing", pointing to positive benefits within reasonable limits. This research supported Askew's (2012) findings that cyber-loafing might not have a strong influence on task performance, except when done frequently and in long durations. Furthermore, a 2014 Pew Research Center study of among a sample of 1,066 adult Internet users found that only 7% of working online adults felt their productivity has dropped because of the Internet, email and cell phones, while 46% felt more productive. Asked about a variety of effects of the technology, the mainly office-based, Internet-using workers reported that the Internet, email and cell phones:

- expanded the number of people outside of their company with whom they communicated (according to 51% of respondents);
- allowed them more flexibility in the hours they work (39%); and
- increased the amount of hours they work (35%).

In proposing situations in which the employee should be allowed to "cyber-loaf" without being disciplined, Ivarsson & Larsson (2011) conclude that "Today's workplaces are populated by engaged employees who work at a fast pace and need recovery, well-deserved micro-pauses, and breaks from demanding work." (p. 63) They also found that it was the fault of the organization for the employee's online behaviours. "Some Internet surfing is actually a consequence of organisations' inability to come up with decent work tasks to fill the whole day.” (Ivarsson, L., & Larsson, P., 2011, p. 63)

Regardless of one’s view on the positive impact of allowing employees to use an organization’s Internet access for personal use, Bucciol et al (2013) found that prohibiting it has negative consequences. When employees were told not to use the Internet for personal use, the temptation required so much willpower to resist that their productivity decreased. “The result is not surprising, considering that it's well-established in social psychology that using willpower to delay gratification can detrimentally impact performance on subsequent tasks due to the additional energy exertion.” (Zyga, 2013, p. 2) Lastly, positive benefits should warrant examination if only because of some research shows that high-performing employees are even more likely to violate Internet use policies.

> Indeed, given our findings that the highest status workers are most active personal Internet users, it seems worth analyzing further whether keeping such valued employees satisfied and loyal to the organization by not enforcing overly restrictive preventative measures on personal Internet use might actually benefit the organization overall. (Garrett and Danziger, 2008, p. 953)

Chapter 2: Problematisation

Over the past three decades, research and media reports have shown that employer-employee practices related to the personal use of the Internet in North American organizations are fraught with unresolved issues and unforeseen consequences. Employees are regularly updating their social media personas, shopping or playing games online, bidding at Internet auctions, writing personal email messages, visiting pornographic sites, and downloading copyrighted music. These actions are defined in this investigation as the workday use of an organization's hardware and/or software resources to access the Internet for activities unrelated to the organization.

As we saw in the literature review chapter, this behavior has been couched traditionally in negative terms. True, personal Internet use can pose a problem for organizations due to potential computer viruses, productivity loss and legal liability – such as harassment stemming from the sharing of offensive online material – as well as a general loss of control over employee behaviour. Counter-productive Work Behaviour literature has primarily adopted a *"This is bad and we need to fix it"* approach, deeming this type of Internet usage as organizational misbehaviour. In positing that "cyber-loafing" must be stopped, Lim (2002) concludes that managers need to "take the necessary steps…to keep cyber-loafing, and other deviant behaviours to a minimum level within their own organizations." (p. 689) In addition to the human and material costs associated with this phenomenon in the business world, Lim (2002) argues that the ICT has revolutionized work-breaks through their apparent invisibility when they are taken using computers at an employee workstation.

Despite any perceived cloak of invisibility adorning employees, North American companies continue to devote huge resources to Internet filtering, reporting and surveillance tools to uncover Internet abuse and "cyber-slacking" employees (AMA, 2005). Employers typically inform employees of the electronic surveillance through Acceptable Usage Policies (AUPs) designed to regulate access to the World Wide Web to confront issues such as legal liability, declining productivity, and misuse of company resources (AMA, 2005). However, despite knowing they are being watched and even after signing policies prohibiting specific actions, employees continue to violate Internet-related rules while complying with other workplace rules, such as where to park or smoke. And, there appears to be no resolution in sight as this phenomenon approaches its fourth decade. By 2001, three-quarters of all major U.S. firms were recording and/or reviewing the email messages, telephone calls, Internet connections, and computer files of their employees to fight against the personal use of ICTs (AMA, 2005). As part of the 25th anniversary of the creation of the World Wide Web, the Pew Research Center (2014) found that US employers continue to block access to certain websites and expect employees to follow rules about what they can say or post online.

Yet, the continued treatment seems too simple a reflex without a regard for the unintended consequences – both positive and negative. For example, workplace monitoring to curb personal Internet use at work has been shown to lead to increased stress, lower job satisfaction and – counter to its primary intent – lower productivity among employees (Alder, 1998; Miller & Weckert, 2000). And, on the directly positive side, there is evidence that the personal use of the Internet at work can herald the benefits observed with other informal work practices as articulated by Roy (1959), such as *ad hoc* breaks providing time for a valuable subconscious focus on work-related challenges (Oakley, 2014), increased job satisfaction.

(Duhita & Daellenbach, 2015; Messarra, Karkoulian & McCarthy, 2011), and even potentially higher productivity (Pew 2014).

Also of relevance for this thesis are the benefits of relaxed organizational constraints that Gouldner (1954) observed as enhancing relations between gypsum miners and their bosses to help decipher the ethical norms of office workers amid their Internet violations and the tacit tolerance of unauthorized practices by their managers. However, it should be noted that the miners often enjoyed prior familial and social connections with their co-workers and bosses while office workers usually embark on their relationships once together in the workplace.

2.1 Research Problem/Question

Fundamentally implicated in this relatively recent but sustained ICT phenomenon is the issue that, if employees do not perceive their actions as unethical or wrong, then organizational practices and policies prohibiting their use are limited in value, if not worthless. Has Internet use shifted the moral "compass"? Where is the "harm"? It is important to gain an understanding of what is taking place: why, in which contexts, and how this largely unintended use of ICT assets emerges and persists in the office workplace. Therefore, the following research questions served to guide this case-study investigation:

- How do office workers negotiate what is acceptable in terms of non-work related Internet use, often when it is prohibited?
- How do supervisors justify their subjective enforcement of rules governing the non-work-related Internet use among their employees?

For its theoretical and conceptual grounding, this thesis uses the concept of "Moral gray zones", examined in its connections among moral codes and situated moralities in the office workplace. Specifically, this investigation explores the emergence of a moral gray zone related to the personal use of the Internet at work. It strives to illustrate situated moralities as they emerge, develop and are sustained within an organization.

2.2 Conceptualization

In order to explore the above questions, this research will draw on the concept of Moral gray zones where supervisors and workers engage in forbidden practices, as articulated by Michel Anteby (2008) and, to a lesser extent, in Michel de Certeau's (1984) notions of "les perruques" and tactics to resist the panoptic eye.

2.2.1 Moral Codes and Situated Moralities in an Organizational Context

The ancient Greek philosophers struggled to identify "the good life" through ethics. Unlike the field of psychology where the pursuit is to understand *why* humans act the way we do, the study of ethics probes the inherently multi-faceted question of *how* we should, or ought to, act. Socrates likely conceded in frustration that the study of ethics or morality was an inexact science. Unlike arithmetic where 1 + 1 must equal 2, there can be many right answers in the pursuit of an ethical decision. Still, humans have persevered to define a list of right and wrong answers, or actions. In fact, the history of these lists or "codes" of ethics can be traced back thousands of years to The Code of Hammurabi dating around 1754 BC (Schwartz, 1998). And, whenever members of a society have been able to agree on a single "right answer" –

such as “the wrongness” of murder or material theft – these unethical actions have been prohibited in codified laws.

Similarly, the correct way that employees should, or ought to, act in the workplace has been articulated in codes of ethical conduct since the early 1900s when J. C. Penney introduced a set of guidelines for proper employee behaviour (Trevino & Weaver, 2003 in Kish-Gephart et al, 2010). Today, codified rules of conduct are common in organizations around the globe. And, their focus is often in the “boundary zone” of actions, as described by Balch & Armstrong (2010), where employees may be confused and need guidance on how to behave in the organization. “An action that is clearly out of bounds requires little ethical sophistication to judge. On the other hand, an action that is marginal – perhaps ethical, perhaps not – requires ethical imagination and sophistication to assess.” (Balch & Armstrong, 2010, p. 291)

Bandura’s (1999) articulation of Moral disengagement helps explain situationally induced processes that predispose people to behave unethically when they can:

- rationalize an action so that it is not viewed as being immoral;
- minimize their role in a situation;
- fail to see consequences from an action; or
- change the perception of the victims.

(Knoll et al, 2016)

Rather than focusing on the psychological moral disengagement notion as a personal characteristic, this thesis takes a more sociological tack. It examines the specificities of a particular situation – a single group of individuals involved in one type of behaviour, that is, Internet use. These are typical office workers with no history of disobeying other workplace rules and who consider themselves ethical people. This more sociological treatment is justified by Knoll et al who describe Mischel's (1977) idea of situational strength as an important component in the creation of situated moralities, even in their psychological analysis: "Weak situations, in contrast, lack strong signals for appropriate behavior; they give room for individual reasoning which, in turn, increases a) behavioral variability across actors, and b) permits individual differences to relate to other variables." (Knoll et al, 2016, p. 71) As further validation, Knoll et al (2016) conclude their analysis with a recommendation to understand personal and social factors together, contending that ethical behavior is a combination of what a person brings *and* the specific situation.

As further proof of the contextual interpretation of the rules, there are some behaviours that are not perceived as ethical, or right, by those on the outside of the situation. In fact, a unique ethical or moral framework can emerge and be sustained within organizations. Anteby (2008) isolates these areas as "Moralities that make sense and exist within given social contexts" (p. 132). For example, "theft" of company resources may be labelled as such only by people outside the organization because they do not understand the explicit and implicit codes of rules operating in the workplace. Vardi's work also supports this notion of moralities that are situated, or unique, to a specific workplace.

> Whether or not such behaviours (e.g., employee theft) are considered OMB [organizational misbehaviour] is determined relative to the core norms espoused by the organization in question as well as to the norms of conducts articulated by law (e.g., sexual harassment). Theoretically, OMB is a product of the interaction between factors at the individual level and factors at the organization level. Its motives, frequency and intensity thus vary and differ for different circumstances. (Vardi, 2001, p.326)

2.2.2 Moral Gray Zones

Anteby explains the situated moralities that he observed in a French airplane manufacturing factory in terms of a "Moral gray zone". It is a phrase that can be traced to Primo Levi (1989) and his analysis of the extreme ethical dilemmas faced by prisoners of Nazi concentration camps, described as a context that "possesses an incredibly complicated internal structure, and contains within itself enough to confuse our need to judge" (Levi, 1989, p. 27). Anteby wondered why managers looked the other way when employees engaged in some unauthorized activities. He contends that it was not because they were forgiving supervisors but, rather, they were deriving unofficial, important benefits from a workplace culture that tacitly encourages gray zones.

Anteby (2008) focused his research at his manufacturing field site on the creation by employees of "homers", also known as *perruques,* [French: "wigs"], as articulated by de Certeau who will be discussed later in this section. "Homers are artefacts produced for personal use by factory employees on company time, with company material and/or tools. The origin of the term is unclear but probably refers to the fact that these artefacts are brought home." (Silverthorne, 2005, p.1) The situated morality, or ethical perception, of homers had five universal tenets among workers and managers:

1. An employee's official assigned work must be completed first.
2. Employees must transform, not just use, the company's raw material.
3. Only scrap, not new material, can be taken.
4. The employee cannot receive any money from the finished product.
5. Employees must not spend their entire workday making a homer.

Anteby uses these homers as a focal point to develop his concept of Moral gray zones, defined as "areas in which workers and their supervisors together engage in practices that are officially forbidden, yet tolerated by the organization." (Anteby, 2008, p.139-140) For Anteby, two conditions are necessary for a moral gray zone to emerge:

1. The breaking of official company rules; and
2. The supervisors' explicit or tacit approval of the violations of these rules.

As we understand from the literature, Organizational misbehaviour (OMB) and Counter-productive work behaviour (CWB) occur within these moral gray zones. However, for Anteby (2008), a situated morality supports the emergence of these violations, bringing benefits to the entire organization through a relaxation of organizational constraints. And, the moral gray zone, as embodied in the practices related to homers, provides positive outcomes shared by both supervisors and workers. Specifically, the tolerance of the creation of homers:

- Secures greater flexibility from employees to meet work-related demands;
- Compensates employees for "doing well";
- Provides situated compensation (that is, incentives and perks) amid rigid collective labour agreements; and
- Promotes desired occupational identities.
  (Anteby, 2008)

In addition, Anteby (2008) contends that moral gray zones in organizations rely on trust between supervisors and their workers. These zones test middle management's ability to manage and to prevent abuses of mutual trust. A key assumption is that a manager will exercise proper judgment in allowing violations among employees. Finally, Anteby (2008) concludes that strong communities within occupations provide the unstated but necessary guidelines to ensure proper use and sustainability of moral gray zones.

Anteby's description of an informal relationship among supervisors and workers is reflective of Gouldner's "Indulgency pattern" from his 1950s research at a gypsum mine that featured an organizational culture with an informal legitimacy and widespread acceptance of unconventional behaviours (Hallett, 2003). Both situations heralded unintended and implicit benefits for both workers and management related to authority, autonomy, trust, and even harm mitigation amid the tacit violation of written rules.

Finally, in one of the few organizational studies to pick up on Anteby's Moral gray zones concept and then to show its relevance for the office workplace, Knoll et al (2016) contend that these situated moralities can help us better understand ethical behaviour in business organizations. However, they focused their lens on the leader's role in creating a moral gray zone in order to issue unethical instructions to followers. Knoll et al (2016) narrowly define their moral gray zones as "situations that are morally ambiguous and in which leaders and followers together engage in practices that are likely to harm others, yet might benefit the organization, the follower, or the leader" (p. 66-67).

2.2.3 ICT Strategies and Tactics

Michel De Certeau's concepts of "Strategies" and "Tactics" may also prove insightful for this investigation. De Certeau (1984) focuses on the devices, actions, and procedures that people use every day in order to subvert – for brief moments – those with the power of control and discipline. De Certeau presents strategies and tactics as distinct in source and goal. While a rational organization's implementation of strategies is associated with power, the employee performs a tactic to continue to work within the system. Strategies are planned and imposed with order as opposed to tactics that are not pre-planned and seize the moment and the particularities of a given situation (de Certeau, 1984). However, there is a logic to the use of the tactics by employees. Firstly, they are not just resistance to strategies, but are also another way, an « *art de faire* ». Secondly, the practice of resistance is situated in a *rapport de force* and optimizes the circumstances (de Certeau, 1984). While employers use strategies for control, such as electronic surveillance, employees can respond with pedestrian tactics to reclaim their own autonomy (de Certeau, 1984).

To describe tactics, de Certeau introduces us to "la perruque" [translation: "the wig"], defined as the worker's own efforts performed at the place of employment under the guise of work for the employer (de Certeau, 1984).

> It differs from absenteeism in that the worker is officially on the job. *La perruque* may be as simple a matter as a secretary's writing a love letter on 'company time' or as complex as a cabinetmaker's 'borrowing' a lathe to make a piece of furniture for his living room. (de Certeau, 1984, p. 25)
>
> Sur les lieux mêmes où règne la machine qu'il doit servir, il ruse pour le plaisir d'inventer des produits gratuits destinés seulement à signifier par son œuvre un savoir-faire propre et répondre à des solidarités ouvrières ou familiales. (de Certeau, 1983, p. 45)

The worker may find push the limits or "play the game" with a "tactic", an action defined "as insinuating itself within the space of the other, worming its way into the territory of that which it seeks to subvert, like a tiny virus infecting a vast computer program." (Weidemann, 2000, np.) However, this tactic insinuates itself not to destroy or take control. It claims no space for itself, relying rather on time: "It is always on the watch for opportunities that must be seized 'on the wing'" (de Certeau, p. xix, 1984). In addition, the beneficial outcomes from these acts of resistance are always discarded: "whatever it wins, it does not keep" (de Certeau, p. xix, 1984).

De Certeau's relevance to the personal use of the Internet could be viewed from the perspective of tactic of resistance in the face of organizational constraints. Lim (2002) found that office workers employees will intentionally break company rules to use the workplace computer for personal reasons as a means of retaliation against their organization. For Anteby's description of homers, a factory worker would use company time, equipment and materials to fashion a lamp, a toy or some decorative artefact to take home for personal use or as a gift. However, there appears to be a distinction based on material value. For de Certeau's *perruques*, only the employee's time is taken from the employer; nothing of material value is stolen. Arguably, the use of company machinery – be it a wood lathe or the Internet access – does have value. For an office worker, the personal use of the Internet involves the use, borrowing or theft – depending on one's perspective – of both tangible and intangible elements, specifically, the organization's network provision of the Internet access, the computer workstation, plus the time taken to surf the Web during paid working time – which a supervisor would argue does have value. Indeed, the use of the widely accepted term "time banditry" (Martin et al, 2010, p. 26) to describe this ICT phenomenon is testament to the value placed on this activity by an organization in that something – a digital but tangible asset – is being borrowed or lost in the workplace.

Along a trajectory that may link Anteby with de Certeau, Lieberman (2010) points to a "hydraulic effect" where employers deliberately allow employees to release frustrations by engaging in minor ethical wrongs rather than clamping down on such actions, which could ultimately drive workers to act out in more detrimental ways. Additionally, this non-damage-causing violation of rules may be seen as necessary, legitimate, and even desirable for such outcomes as learning and innovation (Levitt & March, 1988: ZoUo & Winter, 2003 in Lehman & Ramanujam, 2009). Lastly, de Certeau (1983) notes that in his *L'invention du quotidien* he did not seek as much to analyse different daily practices as to reconcile multiple logics and rationalities and seek the balance among them.

In conclusion, while primarily focusing on the moral and ethical aspects of moral gray zones, this thesis will also draw from de Certeau. While the moral gray zone concept may provide insights into why and how the personal and often unauthorized use of the Internet emerges and persists in the office workplace, de Certeau's concepts of strategies and tactics could be used to describe "the how", showing potential correlations between an employer's actions and an employee's reactions.

Chapter 3: Methodology

3.1 General Attitude and Orientation

Inspired by the fruitful ethnographic lens casts on workplace environments by Orlikowski, Suchman and Dyck – together with the informal employee relationships documented by Gouldner and Roy – a case-study approach was taken in this investigation. As Yin (1994) observes, case studies have become one of the most common ways to conduct qualitative inquiries.

This investigation into the personal use of the Internet in the workplace satisfies Yin's (1994) three optimal conditions to use a case-study method, namely:

- To answer questions like "how" or "why";
- When the investigator has little/no possibility to control the events; and
- A contemporary phenomenon exists in a real-life context.

In addition, as an employee in this field site, this researcher had access to many of the sources of evidence, as recommended by Yin (1994):

1) Documents, such as letters, agendas, progress reports
2) Archival records, such as service records, organizational charts, budgets
3) Interviews & surveys – typically open-ended, but also focused, structured
4) Direct observations – formal or casual; useful with multiple observers
5) Participant-observation – assuming a role in the situation and getting an inside view of the events
6) Physical artefacts

This researcher recognizes that the potential to theorize from a case-study approach is limited. Case studies can show a detailed view of an activity, but they cannot provide the foundation for a robust theory or even a generalization flowing from the data. Indeed, Stake (2000) argues that there is a risk in failing to fully understand important features of the case study when a researcher possesses a strong desire to generalize. Therefore, there is no ambition to construct a theory of the personal use of the Internet in the workplace from this research. A case-study approach cannot offer generalizations beyond the selected field site. However, a case-study approach *can* be valuable in discovering patterns that may prove relevant to other settings, as shown in the use of Anteby's study of a manufacturing plant in the theoretical framework of this investigation. In addition, the use of a case-study approach is appropriate if the focus is on a situated morality, specifically, the emergence of a moral gray zone in the office workplace.

Even though Cowtan (2000) cites disadvantages of cost and time, given the complex realities and inter-relationships of elements implicit in the research questions, a predominantly qualitative approach[1] was deemed most appropriate for this investigation. It provided the researcher with a role in synthesizing something new and determining what did not exist before.

> De cette manière, par l'analyse qualitative des données, la connaissance est une construction partagée, ancrée dans l'interaction chercheur/participants, interaction traversée par des valeurs qui ont un impact sur la connaissance produite et sur le processus de production. (Anadón et Savoie Zajc, 2009, p. 1)

---

[1] The online survey yielded some descriptive statistics to garner a portrait of actual Internet use and to determine the extent of the phenomenon.

Lastly, Wolcott describes varying proportions of qualitative insights emerging from three stages: Description, Analysis and Interpretation (Wolcott, 1994). An advantage for this researcher was to be able to make links to the theoretical concepts from other researchers, to observe nuances, and to connect the results to previous studies.

> Le troisième et dernier processus, celui de l'interprétation, en appelle à la créativité du chercheur. L'étroite relation ainsi que la compréhension en profondeur que la personne a développé face aux données aident le chercheur à passer à un niveau conceptuel pour leur donner sens. (Anadón et Savoie Zajc, 2009, p. 2)

Multiple methods were employed to ascertain and describe the reality and elements of the following central research questions, as explained in the previous chapter:

1. How do office workers negotiate what is acceptable in terms of non-work related Internet use, often when it is prohibited?
2. How do supervisors justify their subjective enforcement of rules governing the non-work-related Internet use among their employees?

This research sought to sketch a portrait of the complete situation, not just an oppositional one. Thus, a focus on the interpersonal relationships among workers, supervisors or managers, and employer or organization, rather that just worker/supervisor, was pursued. As well, this researcher also assumed that an individual's perspective is variable over time given the changing social dynamics and across various situations within the office workplace. This researcher also adopted an explicit, non-judgemental approach to examine the questions from various points of view, neither a uniquely management nor workers' perspective. Both the multiple sources of data, plus the non-judgmental approach, are supported by Alvesson and Karreman's (2000) observations:

> We read the account as a text (a story, not a truthful testimony of a personal conviction) and look at the claims and logic that it expresses. No assumptions are made regarding the constituting of subjectivity or expressions of meanings (intentions, beliefs, standpoints) outside of the situation of language use. From a discourse point of view, the interviewee may well talk and act in ways inconsistent with the account. (p. 1143)

In addition, this researcher followed Alvesson and Karreman's (2000) call to "critically evaluate the empirical material in terms of situated meaning versus meaning that is stable enough to allow transportation beyond the local context (e.g. an interview conversation)" (p. 1146). And, as Clifford (1983) notes, the researcher's experience within the site can "serve as a unifying source of authority in the field" (p. 128).

Lastly, a certain messy "bricolage" was recognized as part of this research with its multiple sources and intersecting methods, largely decided by a participant-observer. For example, while acknowledging the inherent risks of being the supervisor of some of the employees under observation, this researcher sought to also solicit the benefits, in keeping with the approach of Meunier et al (2013).

> L'intelligence du bricolage se manifeste plutôt dans le résultat particulier et individuel des décisions prises au cours d'une recherche. En ce sens, chaque chercheur met en forme un bricolage intellectuel à la mesure de ses projets, et celui-ci se révèle irréductible d'un projet à un autre. (Meunier, Lambotte et Choukah, 2013, p. 354)

This researcher joined the organization where the field site is situated as a middle manager in late 2008. A few years later, he was appointed to manage its first social media team focused on all types of social media use by employees. As part of his responsibilities, he led the development of the organization's first guidance document for employees on the personal, professional and institutional use of social media. He did not write the guidance; rather, he convened a team of representatives from the organization's policy centres of expertise, such as Legal services, Official Languages, Privacy, Information Security, Information Management, and Values and Ethics. This multi-year process yielded several editions of a Social Media Handbook for employees (see Annex 3b) that were promoted – in the preceding and same year of this investigation – across the organization to foster compliant use. While broadly complementary, the leadership of the Handbook dossier developed and progressed independently of this thesis.

Since this researcher was employed at the field site and was involved in files related to the research area, he took myriad measures to clearly transmit his role as researcher – not colleague – by carefully articulating this distinct role at all opportunities, as detailed throughout this chapter. This researcher was under no allusions that this process could be totally devoid of bias. For example, the selection of the field site was influenced and facilitated by the researcher's role in the site. In addition, the decisions of respondents to participate in both the online survey and the subsequent qualitative interviews were likely influenced by the pre-existing relationship with their colleague-turned-researcher. However, this researcher instituted a plethora of safeguards – explained in this chapter – to stand aloof. For example, the invitations to participate in the survey would have been far more efficiently delivered via organizational email systems using workplace distribution lists, and would have likely solicited a larger response rate. However, a hand-delivery of printed invitations was employed to avoid giving the perception of any organizational or management imperative. Still, some connections were impossible to untangle or avoid, such as a potential perception among an employee supervised by this researcher that s/he would receive a more favourable performance evaluation if s/he agreed to participate in this research project. However, this "messiness" of relations was acknowledged and reflected upon for both the limits it imposed on the research, as well as the observations and insights it could potentially generate, as Meunier, Lambotte and Choukah (2013) highlight.

> De plus, les relations qui émergent de leurs connexions doivent permettre de situer autant de moments de tension que d'accord, d'états de stabilité que d'instabilité, de mouvements d'improvisation que de calculs informant la réalité des chercheurs. Notre intérêt doit donc porter autant sur les articulations possibles entre ces diverses activités que sur le processus de passage d'une activité à une autre. (Meunier et al, 2013, p. 360)

3.2 Research Techniques

This thesis draws on manifold sources and data collection strategies. Recognizing that both quantitative and qualitative strategies have their respective limitations, a combination of the two strategies was utilized. This ethnographically inspired search for workplace patterns featured the following components: an anonymous questionnaire distributed among office-based employees and managers, followed by observation and interviews of a sub-set of the group, and document analysis. In developing the methodology, this researcher was attentive to the work of previous researchers, such as Alvesson, Karreman, Schwartz, Anteby and Dyck, allowing for the selection of relevant tools and techniques, plus the mitigation of known risks.

Firstly, it was hoped that a comprehensive examination of a myriad of available sources would enable us to palliate a common problem in organizational analysis as articulated by Alvesson and Karreman (2000): to move past specific empirical material – such as interview accounts, questionnaire responses, and documents – to uncover "discourses with a capital D – the stuff beyond the text functioning as a powerful ordering force" (p. 1127).

Secondly, Schwartz's 1998 study consisted of a descriptive exploration involving interviews with employees and managers, plus a normative evaluation of corporate codes of ethics and behaviours. Schwartz was able to explore the dynamics and interactions surrounding compliance and non-compliance by employees with organizational policies. He created and pursued five research questions surrounding corporate codes of ethics, including:

1. Do codes influence behaviour?
2. What are the reasons why codes are complied or not complied with?
3. How do codes influence behaviour?
4. What are the factors that lead to codes being effective in influencing behaviour? (Schwartz, 1998)

Based on the success of investigations by Schwartz into codes of ethics and other researchers probing prohibited behaviours in the workplace, this research ventured beyond the Acceptable Use Policies – signed by employees to restrict their use of personal use of company ICTs – to explore the entire workplace context. Indeed, in an examination of compliance with written codes of ethics, Schwartz (1998) acknowledges these types of documents as a *small component* of the overall explicit and implicit "ethics program" of an organization aimed at encouraging ethical behaviour.

Lastly, inspired by Anteby's (2008) exploration of homer-making, this researcher relied on interviews with employees, company records, legal cases and media reports, acceptable use policies, and national workplace surveys. However, unlike Anteby, this researcher was a member of the group studied, which opened up further possibilities and potential pitfalls, as discussed later.

Therefore, the following methodological approach was finalized and implemented:

1. **Anonymous Online Survey** among 75-100 respondents
   Goal: To obtain self-reported behaviour of Internet usage
2. **Participant-Observation** of the in-cubicle Internet usage of a small group of employees
   Goal: To qualitatively describe what people are actually doing
3. **Qualitative Interviews** of a sub-set of 5-10 employees who completed the online survey
   Goals: To clarify findings from the questionnaire
   To better understand the reasons the employees act as they do
   To qualitatively describe what people are actually doing
4. **Document analysis** of Acceptable use policies and other guidance documents
   Goal: To better understand the major instruments used by the employer

3.3 Description of Site and Respondents

Approval was granted to conduct research in a federal government department with its headquarters in Gatineau, Québec in Canada's national capital region. This department of 27,000 employees across Canada was then known as Human Resources and Skills Development Canada (HRSDC) and remains responsible for a "cradle-to-grave" suite of social and economic programs, policies and services offered to Canadians. The field site was the communications division, or branch, within this department. The division is known as Public Affairs and Stakeholder Relations Branch (PASRB), and its role is best articulated in its stated mission:

> Our mission is to promote and facilitate Canadians' awareness of Human Resources and Skills Development Canada (HRSDC) policies and programs that are relevant to

their lives, and to maintain an open and interactive relationship with stakeholders, other levels of government and Canadians. (Integrated Business Plan, 2012-2015, p. 1)

Employees of this branch serve "as the focal point for the flow of strategic and operational communications advice, products and services to the Department's ministers, deputy ministers and individual branches to advance government and departmental priorities." (Integrated Business Plan, 2012-2015, p. 1). Specifically, employees:

- translate policies and programs into communications products that can be easily understood and discussed by Canadians;
- develop communications strategies and implement plans to strategically position issues and effectively reach out to Canadians;
- support the engagement of stakeholders on key departmental issues to inform the research and policy development process;
- support the efforts of individual program areas to address their objectives through public affairs and stakeholder relations strategies and activities; and
- create a positive, inclusive and stable working environment for our employees, by optimizing their contribution to PASRB's objective on excellence in what it does and how it does it.

(Integrated Business Plan, 2012-2015)

3.3.1 Profiles of Employees and Respondents

As of March 31, 2012, there were 270 employees of this branch across 5 locations in the national capital region, namely Ottawa, Ontario and Gatineau, Québec. The communications functional area within government typically attracts more women than men. And, more than one half of this branch's employees are under 50, with almost one third under

35, and the average number of years of service was 10 (Integrated Business Plan, 2012-2015). All respondents in this investigation were federal government employees, and most were currently or previously employed in this branch, specifically at its main location with the largest concentration of employees. They were generally reflective of the employee profile, as revealed below in the results from the demographic section of the anonymous online survey.

Gender

Response	Chart	Percentage	Count
Male		47%	35
Female		53%	40
	Total Responses		**75**

Age

Response	Chart	Percentage	Count
20-29		27%	20
30-39		37%	28
40-49		20%	15
50-59		13%	10
60 +		3%	2
		0%	0
	Total Responses		**75**

Time working in the federal government

Response	Chart	Percentage	Count
Less than 1 year		1%	1
2-4 years		35%	26
5-9 years		28%	21
10+ years		36%	27

	Total Responses	75

The linguistic requirement for almost all federal public servants working in the national capital region is some degree of fluency in Canada's official languages – English and French. In addition, some post-secondary education, such as a college or university degree, is required for all positions, even entry-level ones. The positions range from administrative assistants and junior communication officers to mid-level communication advisors up to middle managers and the executive cadre. Therefore, all members of this work site can be classified as office-based professionals.

3.3.2 Work Responsibilites and Internet Policies

The responsibilities of the employees in this field site revolve around strategic and operational communications planning and advice, issues management, stakeholder relations, public environment analyses, media services, ministerial and event services, internal communications, creative services and corporate Web governance. (Integrated Business Plan, 2012-2015). Like almost all federal departments, the workplace features a standard office building architecture with each employee designated an open-air cubicle, each equipped with computer hardware and software, a large monitor and keyboard. Members of the executive cadre in this field site consisted of 12 directors, 2 directors-generals and one assistant deputy minister, each working in a closed office.

At the time of this investigation, and due to the inherent public communications nature of their positions, employees in this branch had the most unfettered access to the Internet among all employees in the department. Their easy access to the Internet was provided for work-related tasks as a way to understand the communication needs and habits of the public with the goal to better communicate the work of the department and its ministers. Of particular relevance to this investigation, this branch committed to work with its sister Information Technology branch on “expanding and formalizing PASRB’s use of social media and collaboration tools as integrated parts of business” (Integrated Business Plan, 2012-2015, p. 6). The Internet was explicitly acknowledged as a productive tool. “Web 2.0 tools, such as wikis and blogs, together with social media channels, such as Twitter and YouTube, offer new personal opportunities to engage with others and to work together more efficiently in our official service to Canadians.” (Human Resources and Skills Development Canada Handbook for the Personal and Official Use of Social Media, 2012, p. 4) However, there was a growing awareness of not only the potential value, but also the risks of the Internet and social media for employees. Accordingly, the new handbook explicitly described its goal “to help all employees use social media effectively while minimizing its risks, such as:

- immediate transmission;
- loss of control of content;
- wide dissemination and broad audience;
- permanent nature of posts;
- vulnerability to alteration, misrepresentation;
- transparency of online identity (e.g. name, workplace); and
- disclosure of private or personal information”
  (HRSDC Handbook, 2012, p. 4).

Consistent with the suite of laws, policies, guidelines and protocols that govern the actions of federal public servants in all domains of their activities, employees in this field site were also informed of the limitations related to their use of the Internet. The *Guideline for*

External Use of Web 2.0 for public servants in the Canadian federal government (Annex 3c) was published and promoted in the year prior to this investigation. Of particular relevance to the respondents in this investigation, their new employee handbook explicitly defined personal use of the Internet "for purposes unrelated to work – at home or at work – on- or off-duty (that is, during or after the workday)" (HRSDC Handbook, 2012, p. 7). And, since the expectations of the behaviour of public servants extend beyond their time in the workplace, the employees in this department were also instructed:

> At **all times** when using social media for personal use – to minimize the risks previously outlined – public servants must:
>
> - ensure Public Service political neutrality and impartiality;
> - respect their Duty of Loyalty;
> - refrain from public criticism of the Government of Canada, HRSDC or its policies;
> - avoid statements that would appear to impair their ability to perform official duties;
> - respect confidentiality and privacy;
> - avoid causing harm to HRSDC, its reputation and programs;
> - respect the Values and Ethics Code for the Public Sector;
> - respect the HRSDC Code of Conduct and the HRSDC Policy on the Use of the Electronic Network; and, if applicable,
>   - respect the Guidelines of Conduct for Service Canada; and/or
>   - respect the Guidelines of Professional Conduct for the Labour Program (HRSDC Handbook, 2012, p. 7).

Yet, despite the myriad policies and publicized risks, Internet access was permitted largely unfettered for all employees in this field site. In fact, the business value of the Internet was promoted in the employee handbook:

> Official use is defined as using social media for internal and public-facing initiatives in support of:
>
> - departmental business, e.g. communication, employee engagement; and
> - individual purposes, i.e. employee participation for business purposes.
>
> Official use includes **internal** initiatives for workplace collaboration, employee engagement, research, and networking on internal platforms, such as the Knowledge Portal, SharePoint, GCpedia, GCconnex, and GCforums.
>
> It also includes **public-facing** initiatives, such as communications, outreach, engagement, service delivery, research and networking on third-party platforms such as Twitter, YouTube and Facebook. (HRSDC Handbook, p. 10)

In conclusion, employees were expected to use Internet access and social media to better comprehend the public environment related to the awareness of departmental issues within the public domain. Guidance was provided to urge prudence in the performance of their online tasks.

3.3.3 Work Culture of Policies and Results

In addition to working within an environment of policies and guidelines, the employees in this workplace fell under the federal government's Management Accountability Framework (MAF) that features an annual assessment of management practices and performance across the Government of Canada.

> The MAF is a key tool of oversight that is used by the Treasury Board of Canada Secretariat (TBS) to help ensure that federal departments and agencies are well managed, accountable and that resources are allocated to achieve results. (Treasury Board Secretariat, 2014, n.p.)

To feed into this framework, each department and its constituent branches develop detailed logic models showing how all their activities and resources are in support of various policy, program and service outcomes. Managers are then expected to guide each employee to complete a Performance and Learning Agreement (PLA) that articulates the connections between individual actions in pursuit of over-arching goals and priorities. These performance agreements detail work objectives and evidence, or indicators, for evaluation every year. Like many private-sector organizations, the focus within this organization is on attaining results utilizing the workplace resources and tools at hand. Through discussions focused on a standardized PLA form, managers complete a yearly evaluation of employees under their supervision.

Therefore, the environmental context is a results-focused approach towards the use of tools such as the Internet. Accordingly, for the employees in this field site, guidelines explicitly addressed the use of the Internet for personal purposes while on duty (that is, during the workday). In fact, this type of usage was the topic of the Handbook's first "Frequently Asked Questions for Personal Use", namely:

> **Question: Am I allowed to visit social media sites for private purposes, while at work?**
>
> **Answer:** Yes. The HRSDC Policy on the Use of the Electronic Network allows employees to use departmental computer networks for personal purposes provided that this activity:
>
> - is on personal time, i.e. breaks, lunch, the time before and after work;
> - is not for financial gain;
> - does not add to costs; and
> - does not interfere with the conduct of business.
>
> (HRSDC Handbook, 2012, p. 8)

3.4 Anonymous Online Survey

An anonymous survey (See Annex 1) in both English and French was offered to employees of this branch at its most populous location via a public-facing survey site using the Fluid Surveys platform. The survey was pre-tested among a small group of respondents, and tweaks were made to clarify skip patterns and content for a few questions. A response rate of 25%, or about 70 employees, was sought and obtained with a final total of 82 participants and 75 fully completed responses, between late 2012 into early 2013.

3.4.1 Administration of the Survey

About 200 post-card-sized invitations (See Annex 2) were developed in both official languages of this workplace. The invitations featured a brief description of the research, indicating that participation was voluntary and clarifying the role of this researcher – also a colleague. The invitation concluded with a URL to the online survey. The cards were distributed around 3pm, near the end of the workday, to mitigate completion of the survey during the workday and to give people more options to decide where and when to complete it, if they chose to do so. The cards were handed out in person to potential respondents at their workstations, in hallways, after meetings with this researcher on unrelated topics, or left on chairs in cubicles. No organizational resources, such as email systems or time during workplace meetings, were used to promote awareness or participation in the survey.

In the detailed Explanation and Consent form, participants were told of the voluntary and anonymous nature of their survey. Specifically, they were informed that "their answers will be treated confidentially and with anonymity". The survey allowed respondents to elaborate on their answers with free-form responses. These anonymous comments were then used in a verbatim form whenever they are quoted in the thesis.

3.4.2 Survey Design

The online survey sought to ascertain the magnitude of the personal use of the Internet in this workplace, to measure self-reported behaviour of Internet usage for both work-related and personal purposes, and to gauge awareness of practices and policies.

The first wave of questions was designed to measure perceived value of the Internet plus self-reported usage, e.g.

How helpful is the Internet to completing work-related tasks?
Very helpful
Somewhat helpful
Not helpful

How many times do you access the Internet?
For work-related purposes
For personal purposes

In the development phase, it was unclear whether respondents should be asked to assign a minute/hours to their use of the Internet for fear of affecting their initial responses. However, respondents were eventually asked, providing detailed answers in the final version.

Anteby (2008) posits that two conditions are necessary for a moral gray zone to emerge in an organization:

- The breaking of official company rules; and
- The supervisors' explicit or tacit approval of the violations of these rules.

Therefore, the following questions were designed to gauge awareness of the existing policies in the organization:

Are you aware of policies governing the use of the Internet at work?

Did you sign the Acceptable Use Policy for Internet usage at work?

Another line of questioning sought to understand the relationship of knowing between employee and supervisor, through these questions:

Do you believe your immediate supervisor is aware of your Internet usage?

Are you aware of the Internet usage of your colleagues?

Do you believe others in the organization are aware of Internet usage patterns among employees?

If you supervise employees, are you aware of their Internet usage?

If you supervise employees, are you aware of your co-workers' Internet usage

As well, these questions were designed to focus on the interpersonal relationships among worker, supervisor and organization, rather that just worker/supervisor.

Lastly, as adapted from Lim's 2002 study, the following types of Internet usage categories proved beneficial for the survey design:

While at work, how much time do you spend visiting the following types of Web sites:

- *Sports-related Web sites*
- *Investment-related Web sites*
- *Entertainment-related Web sites*
- *General news sites*
- *Non-job related Web sites*
- *Adult-oriented (sexually explicit) Web sites*

The option of social networking sites was added to reflect newer online channels. Lastly, this researcher challenged Lim's (2002) use of "ever" as employed in the following question:

While at work, do you ever:

- *Check non-work related email messages?*
- *Send non-work related emailed messages?*
- *Receive non-work related emailed messages?*
- *Download non-work related information, such as music or videos files?*
- *Shop online for personal goods?*

Instead, a choice of time periods was provided to gauge frequency of use.

This researcher finalized a list of Internet activities after examining survey questions that were already used and validated on similar subjects, as well as noting the delineation of categories. For example, the 2010 UK research conducted by My Job Group used the following two questions to better understand the personal use of the Internet at work:

Do you know if your employer has an HR/disciplinary policy regarding social media?

A. *No, I don't know if they have a policy regarding social media*
B. *Yes, they do have a policy regarding social media*
C. *Yes, they do not a policy regarding social media*

(My Job Group, 2010, p. 11)

The next two questions, taken from the UK study, also proved valuable in designing the survey for this investigation:

How many times per day do you spend on social media sites whilst you're at work?

A. *No time/I don't use social networking sites*
B. *Up to 10 minutes*
C. *11 to 30 minutes*
D. *31 to 60 minutes*
E. *Over an hour to 2 hours*
F. *Over 2 hours*

How do you think social networking sites have affected your productivity at work?

A. *I'm just as productive as before*
B. *Don't know/Don't use social networking sites*
C. *I'm less productive as I'm constantly distracted*
D. *I'm more productive than before*

(My Job Group, 2010, p. 14)

This researcher also deliberately separated "Don't know" from "Don't use" to solicit more honest answers in his survey, noting that the UK researchers found that "Don't know" is more often the most honest answer. (My Job Group, 2010, p. 13)

Lastly, the following resources were also consulted to design optimal questions:

- Statistics Canada Canadian Internet Use Survey
- Pew Internet & American Life Project
- Oxford Internet Institute

Responses to the online survey questions were used as a basis for the subsequent in-cubicle observations and qualitative interviews. To promote participation, the surveys and interviews were explained as a means to improve the development and application of ICT protocols. As well, respondents were informed of all sources obtained for this research, including aggregated quantitative data. Lastly, no direct link was made between responses and any summary reports, as yet not provided to the organization. Permission was granted to conduct research in this workplace without requests for any reports.[2].

3.5 Participant-Observation

To more fully comprehend what people are actually doing and to clarify findings from the online survey, a modest participant-observation approach was employed of about a dozen colleagues. *Ad hoc* and at-a-distance observations were recorded in late 2013 until early 2014. These observations provided an opportunity to better understand the social dynamics at play and to obtain a perspective in real-time – as opposed to the individual and retrospective nature of surveys and interviews. If an observer walked into an open cubicle, a typical work practice

---

[2] If demands for some type of report are made at a later stage, this researcher may be placed into the role of a "researcher-consultant" as explored by Czarniawska (2001). This researcher is confident that, like Czarniawska, he could handle such requests without compromising employee trust or confidentiality.

during the most number of hours each day would show employees sitting at their desks, primarily on their computers preparing documents, exchanging emails, visiting Websites. Sometimes, they would be away at meetings or small-group work sessions, and occasionally on their personal or work-provided smart phones.

This researcher managed a team of about a dozen employees that gave him the opportunity to enter cubicles regularly, noting the content displayed on computer screens. Over the course of several months, this researcher deliberately scanned the monitors of colleagues as he passed by their cubicles, and he would also take note of their reactions when he entered their cubicles while they were online. The ready access to all software allowed employees to keep Internet browsers open and offered the ability to quickly close them. The layout of some cubicles did not permit the monitor to be facing the opening of the cubicle, affording these employees greater privacy for their computer use.

Given this researcher's employment at the field site, the "participant-observation" method, as articulated by Clifford (1983), was embraced in order to observe, describe and understand the colleagues' Internet usage, especially for personal purposes.

> Participant-observation serves as a shorthand for a continuous tacking between the "inside" and "outside" of events: on the one hand grasping the sense of specific occurrences and gestures emphatically, on the other stepping back to situation these meanings in wider contexts. (Clifford, 1983, p. 127)

However, this researcher acknowledged the need to reconcile "participation" with "observation" as Dyck notes. In one specific investigation, Dyck (2000) doubts he would have been able to identify "the pertinent social dimensions" of his subjects nor "recognize the opportunities that these present for ethnographic research" (p. 40) had he not been an insider.

Dyck further contends that it was his “insider” status that allowed him to understand “these situationally specific contexts, imagined selves, identities and communities (that) may be created, shared and enjoyed.” (Dyck, 2000, p. 40) And, this dynamic also emerged in this investigation; for example, this researcher was able to empathize with the reality of the respondents, such as problems with computer hardware or sluggish Internet access.

While Dyck (2000) conceded it became difficult for him to converse with his subjects without feeling like he was “in some senses acting like a spy” (p. 43), this perception was not a problem for this researcher. All data were collected through surveys and interviews with this researcher clearly identified as a researcher, not a colleague. Both observation and interview approaches served to open up and confront the issue of perception of this researcher’s role as either a colleague in pursuit of common organization goals or as an independent researcher. At each interactive stage of the research process, this researcher carefully asserted his presence and actions as someone conducting research separate from any organizational imperative. For example, participants were explicitly informed of this researcher’s role in the survey invitation: “While Adrian is an employee of HRSDC’s Public Affairs and Stakeholder Relations Branch, this research is not related to his assigned work-related tasks or responsibilities.” (Annex 2) In addition, participants were assured that their specific responses would not be shared with management. The Explanation and Consent form explained: “There is no expectation by management for access to the research results. However, recommendations may be formulated and provided to management arising from Adrian’s thesis to foster a more effective use of the Internet in the workplace.”

In the context of participant-observation, this researcher refrained from using any information gained through casual conversations, although general contextual information could not be “unheard” and completely discounted. Whereas Dyck (2000) began his research through personal relationships and migrated to formally organized interviews, this research began with formally organized surveys and interviews. Colleagues were initially made aware of the research. So, after several months, if they remembered, they were aware that they were being observed in a general way. For fear of influencing normal activity, this researcher did not explicitly ask colleagues if they did *not* wish to be observed. Indeed, as a manager with a certain authority, there was a clear risk of blurring of roles: as a colleague, this manager had the right to see what was on their employee’s computer screens; however, as a researcher, to what extent should this information be used? Therefore, this researcher was able to glimpse what employees were doing sometimes, but no great effort was made to record specific details or time they spent doing it. This researcher’s comprehension of any strategies to conceal Internet usage emerged as a composite but still valuable observation. Despite the lack of detail, this approach appeared wisest given the implications and complications of a manager observing one’s employees for research purposes. In addition, a high level of observed detail may not have been necessary as it would not substantially advance this thesis to know, for example, if employee X plays Solitaire. Fortunately, the limitations and fruit of this participant-observation was compensated by the candid descriptions and explanations provided in the survey comments examined and analyzed in upcoming chapters.

In summary, this researcher had to balance his perceived and actual role as a manager in this workplace while wanting to obtain the most robust observations and data. Despite the many safeguards, this perceived dual role was unavoidable as there was no way to distance the two roles in the minds of the respondents. Considering other options, no benefits would be gained by taking a leave of absence from his job to return into the workplace during this time as a researcher since pre-existing relationships would still interfere. Despite the struggle to reconcile and distinguish the two hats, it did afford a better understanding of the employees' point of view since this researcher reports to his own supervisors. Without a doubt, although this methodology is presented in a linear style, a messy informal "bricolage" approach – as detailed earlier in this chapter – emerged as a dynamic in this methodology.

3.6 Qualitative Interviews

Several respondents of the online survey who indicated a willingness to continue to participate in this study were selected for a subsequent qualitative interview stage. To better understand the reasons the employees act as they do, 11 employees (up from a planned 5-7), who volunteered at the end of the quantitative survey, were selected for additional interviews in the first half of 2013. Workers and supervisors of varying functions and levels with differing usage patterns were invited into hour-long interviews. The principle of saturation was taken into account to avoid redundancy. Interviews took place before and after the workday, and during lunch hours, to maintain a distinction between colleague/researcher and to avoid impinging on work hours. Interviews were recorded and transcribed so that responses could serve as material for analysis. As with the survey, participation was voluntary, and confidentially was guaranteed. In the thesis, whenever their comments are featured, the initials of respondents are disguised to further prevent their identification. Interestingly, no concerns were raised about their views being divulged to upper-management; however, the absence of vocal concern could be attributed to the explicit protection provided in the consent form.

Clifford (1983) describes a Flaubertian free indirect style for interviews that avoids direct quotation "in favor of a controlling discourse always more-or-less that of the author."

(p. 137). However, there was no need to adopt this paraphrasing approach since respondents expressed their written and oral ideas using the parlance of the modern-day office workplace – in both English and French. Indeed, the verbatim text of the interviewees served to shine light on personal Internet usage at work by providing examples and confirming testimonies (Clifford, 1983). The text from the transcripts included in this thesis represent a “cleaned-up” representation, that is, verbal tics and completely off-topic comments were not captured. A precise word-by-word transcription required for a conversation analysis approach towards everything that was said during the hour-long interviews was never the goal. Instead, the focus is on the content of answers not the fine details of how they were expressed. Lastly, this researcher drew upon his training and experience as a print journalist for several major news organizations to ensure accurate notes were taken by hand.

Previous research on similar subjects has relied heavily on interviews. The qualitative portion of Schwartz’s 1998 study consisted of semi-structured interviews of 57 managers, employees, and ethics officers at four large Canadian companies representing different industries (p. 50). To support his choice of qualitative interviews, Schwartz cited the study's objectives; the preliminary and exploratory nature of the study; methodological triangulation; and the nature of the topic being studied (i.e. ethical decision-making).

> Only through interviews, as opposed to other research methods, is there a possibility for the interviewer to probe and encourage the respondent until adequate data is generated. The interview method allows the researcher to extend and clarify responses as needed. Interviews also allow the researcher to explore new avenues opened up by the respondent. A quantitative survey may not provide respondents with an adequate opportunity to fully describe their experiences with their companies' codes of ethics. (Schwartz, 1998, p. 52)

In this investigation, we were able to explore the potential deeper, loaded meanings associated an employee's personal surfing at work, beyond the object of his or her specific activity (the object auctioned, the email sent or the travel plans booked), or a supervisor's decision to look the other way while employees engage in unauthorized Internet activity.

Relevant support of this qualitative approach was found in Cowtan's research into electronic monitoring in a Canadian workplace in 2000. "Face-to-face interviewing was chosen as the survey method for two reasons. First data from the interviews tend to be more in-depth, and second, I had a better understanding of the sample population." (Cowtan, 2000, p. 98) In addition, Marecek, Fine and Kidder (1997) argue that qualitative research effectively allows social scientists to "engage questions of authority and interpretation" (p. 632) – two key elements necessary for this investigation into the non-compliance of signed policies.

Alvesson's (2003) *localist* position on interviewing was helpful for this research with its emphasis that "interview statements must be seen in their social context" (p. 16). Accordingly, the "hard work" in understanding the statements took place afterwards beyond simple coding or processing of the data. And, learning from the metaphors that Alvesson (2003) employs to describe the types of interviews, this researcher was able to detect and handle the following:

- Local accomplishment: the mastering of complex interaction in the interview situation;
- Establishment and perpetuation of a storyline: ambiguity of situation and the need for sensemaking.

(Alvesson, 2003, p. 15)

The first point is inevitable in any interview situation. The second was expected and encountered as interviewees attempted to explain their personal use of the Internet at work.

Alvesson's other metaphors, such as identity work and moral storytelling, were not experienced widely in this research. Lastly, Alvesson's (2003) three major elements of interviewing – scene, subject and language – were taken into account to best uncover the complex and multiple layers of meaning between interviewer and interviewee.

In conclusion, the value of participant-observation and interview approaches for this investigation was constructive – for both respondents and this researcher.

> When researchers listen to participants, we learn new things. Participants become more than transmitters of raw data to be refined by statistical procedures. They come to be active agents, the creators, of the worlds they inhabit and the interpreters of their experiences. At the same time, researchers come to be witnesses, a word whose root means knowledge. In bringing their knowledge – of theory, of interpretive methods, of their own intellectual, political, and personal commitments – to participants' stories, researchers become active agents as well. (Marecek et al, 1997, p. 637)

3.7 Document Analysis

Fourthly, to better understand the major instrument of compliance used by the employer, this researcher examined the documents that explicitly frame what is considered the ethical use of the Internet in this workplace. This approach was inspired by Schwartz's (1998) ethical assessment of corporate codes at four companies based on a set of universal moral standards. However, given the non-judgmental approach of this investigation, there was no pretention of making connections to any type of moral standards. Rather, the objective was to better understand the nature and availability of formalized written organizational rules on the personal use of the Internet.

Three documents were examined (See Annex 3):

1. The Acceptable Use Policy that appears on the computer screen each time an employee logs into the computer system;
2. A Social Media handbook for employees of this department (as previously explained) that was promoted across the field site and available on the employee-only Intranet;
3. General guidelines for the use of social media applicable to all federal government employees.

3.8 Quantitative Data

Lastly, it was hoped that the participants' self-reported usage of their Internet usage in this proposed study could be compared with general patterns in ICT usage within the organization. An analysis of quantitative data from employer surveillance tools, e.g. number of times employees access the Internet, would have allowed this researcher to compare the overall, organization-wide actual behaviour to the self-reported anonymous questionnaire data. However, access to this data was not possible due to technical and privacy barriers. This researcher was able to obtain and analyze only the self-reported quantitative data that was provided in the anonymous surveys which was then confirmed in follow-up interviews with a sub-set of the respondents.

3.9 Analysis

This researcher examined the material generated using inductive analysis. Blais and Martineau (2006) define inductive analysis as a collection of systematic steps – essentially guided by the research objectives – that permits the treatment of qualitative data: "un ensemble de procédures systématiques permettant de traiter des données qualitatives, ces procédures étant essentiellement guidées par les objectifs de recherche" (p. 3). An inductive analysis is focused on reducing "data" obtained using a variety of strategies in order to make sense of it. The goal in reducing data is to synthesize, typically by generating categories that can be used to create new-found knowledge (Blais et Martineau, 2006).

In addition, an analysis of themes that emerged from the data followed the first three of Morse's (1994) four-stage cognitive process, namely:

- **Comprehension:** "learning everything about a setting or the experiences of participants…through observations, interviews, use of other documents" (p. 27-35);
- **Synthesizing:** content analysis: a merging of several stories, experiences or cases to describe a typical, composite pattern of behavior or response;
- **Theorizing:** lateral linkages: a comparative method linking to descriptions of experience in other sources.

Morse's fourth stage of "Recontextualizing", defined as the development of the emerging theory so that the theory is applicable to other settings, was not a relevant objective, given the case-study approach taken in this research.

Lastly, descriptive statistics from the online survey served to describe the Internet usage, but not to generalize nor find correlations between socio-demographic variables and behaviours. In similar research in the United Kingdom, researchers conceded there was a self-reporting bias towards individuals claiming there was no impact of personal use of the Internet on their workplace productivity (My Job Group, 2010). Researchers recommended that detailed empirical observation and measurement were needed to obtain more meaningful and honest responses. This multi-faceted approach of the proposed methodology was designed to capture this type of verified observation and measurement.

In summary, a non-judgmental approach was employed to understand what was happening in this field site. The researcher was sensitive to his membership in the group of respondents. Multiple methods allowed triangulation to approach the problem from a variety of perspectives and with different tools. Lastly, a qualitative analysis synthesized the insights for this case-study approach.

Chapter 4: Presentation and Discussion of Results

More than 70 office workers and supervisors – about a 30% response rate – answered questions in an anonymous 30-question online survey focused on the personal use of the Internet at the field site. The quantitative instrument measured self-reported behaviour of Internet usage for both work-related and personal purposes, as well as awareness of practices and policies. Based on these results, a series of hour-long, follow-up interviews were conducted with 11 survey respondents – of varying functional levels, that is, from junior employees to senior managers – to better understand the reasons and motivations behind the survey answers. Lastly, a modest participant-observer stage recorded the behaviour of employees at their workstations.

In the anonymous responses to the online survey (see Annex 1), an over-whelming 90% of respondents stated they accessed the Internet at work using work-provided devices, such as a computer or a smartphone, for personal reasons. See Table I for more details.

Table I: Answers to the Question: *On a typical day, how many times do you access the Internet at work, on your employer-provided computer or smartphone -- for personal purposes?*

Response	Chart	Percentage	Count
Not at all		10%	8
1-4 times		50%	39
5-9 times		17%	13
10 + times		23%	18
	Total Responses		**78**

General news sites (82%) were listed as the destinations where respondents spend up to 30 minutes each day. Professional networking sites, such as Linked In, accounted for 32%. Seemingly personal sites, such as Web-based email, accounted for 41% with online shopping at 40%, and social media sites at 31%.

Table II: *Using a work-provided computer or smartphone, the time estimated spent while at work visiting the following types of Web sites for personal purposes:*

	Up to 10 minutes each workday	11 to 30 minutes	31 to 60 minutes	1-2 hours	2-3 hours	more than 3 hours	Never	Total Responses
General news sites	27 (49%)	18 (33%)	4 (7%)	2 (4%)	0 (0%)	0 (0%)	4 (7%)	55
Social networking sites	11 (21%)	5 (10%)	1 (2%)	0 (0%)	0 (0%)	1 (2%)	34 (65%)	52
Professional networking sites	14 (25%)	4 (7%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	37 (67%)	55
Dating-related sites	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	50 (100%)	50
Sports-related sites	9 (18%)	4 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	37 (74%)	50
Shopping-related sites	18 (36%)	2 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	30 (60%)	50
Auction-related sites	3 (6%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	48 (94%)	51
Investment-related sites	2 (4%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	46 (94%)	49
Entertainment-related sites	14 (28%)	1 (2%)	2 (4%)	0 (0%)	0 (0%)	0 (0%)	33 (66%)	50
Gambling-related sites	2 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	48 (96%)	50

Video & file-sharing sites	13 (25%)	2 (4%)	0 (0%)	0 (0%)	0 (0%)	1 (2%)	35 (69%)	51
Web-mail sites, e.g. Gmail, Hotmail	16 (30%)	6 (11%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	31 (58%)	53
Adult-oriented (sexually explicit) Web sites	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	49 (98%)	50

Even though the sites could be seen as supporting their job within the Communications branch of this government department, taking a break was the most popular reason (25% *Often* and 71% *Sometimes*) for the personal usage followed by completing personal online tasks (18% *Often* and 63% *Sometimes*). For a full list of the reasons, please see Table III below.

Table III: *Reasons for accessing the Internet for personal use at work*

	Often	Sometimes	Never	Total Responses
To stay in touch with friends/family	10 (15%)	41 (60%)	17 (25%)	68
To complete personal tasks, e.g. banking or travel	12 (18%)	43 (63%)	13 (19%)	68
To take a break	17 (25%)	48 (71%)	3 (4%)	68
To reduce stress	12 (18%)	32 (47%)	24 (35%)	68
To relieve boredom	8 (12%)	26 (38%)	34 (50%)	68
It’s faster or cheaper than accessing the Internet at home	2 (3%)	4 (6%)	62 (91%)	68
I don’t have Internet access at home	1 (1%)	1 (1%)	66 (97%)	68

In addition to the mixture of personal tasks while at work, the research also showed an overlap in the access to the Internet – both from personal devices and those provided by the organization – as shown in the following table.

Table IV: *Primary methods used to access the Internet at work for personal purposes:*

Response	Chart	Percentage	Count
On my desktop computer or laptop		77%	53
On a smartphone, e.g. Blackberry, provided by the employer		3%	2
On my own smartphone/mobile device, e.g. iPhone, or tablet, e.g. iPad		19%	13
Other, please specify...		1%	1
	Total Responses		**69**

We were able to confirm, in a general way, that employees at this field site use the Internet at different times of day. And, some frequently positioned their computer monitors away from the opening in cubes to avoid passers-by seeing the content of screens. They would keep a browser, such as Internet Explorer, open but minimalized for easy but concealed access to the Internet.

Almost all respondents indicated a level of moral ease – 32% *Completely comfortable* and 59% *Somewhat comfortable* – in using the Internet at work for personal reasons. Only 9% stated they were *Not comfortable at all*. This level is consistent with the 10% of respondents who responded that they did not use the Internet at work for personal tasks. Reasons for their comfort level clustered around three main reasons:

- **The convergence of work and personal lives:** "*Today's modern IT-enabled workplace blurs the lines between personal and professional time, especially with the onset of work-issued smart phones;"* and *"Allows completion of personal tasks that can only be done in a work day, like talking with a medical office"; "often work and personal tasks blur";*
- **The need to support work-related duties:** *"I read the news during my lunch break, so I can be updated on what is taking place in the world"; "It's okay as long as it's limited, the sites are legal, and the work gets done. Often the sites complement my work. It's not for a personal business"; "With reasonable and positive means, it can be acceptable. If you are a hard worker, and are honest and open with your colleagues and managers, and are sharing relevant information not necessarily within the written scope of your job description, I can see value in permitting online 'personal' use."* And lastly, *"Mon travail promouvoit l'utilisation des médias sociaux."*
- **The need to take a break:** *"Provides a quick break from work and time to re-focus when needed"; "I feel it relieves stress"; "I use the Internet for personal time in lieu of taking breaks."*

The small minority who were not completely comfortable with the personal use of the Internet drew limits related to the workplace, for example: *"(I) think it's inappropriate to use work resources for personal needs"; "Fear of others walking by and thinking I am slacking off"; "the only thing I'm not comfortable with is visiting soft-porn (bathing suit models) sites...I'm okay with everything else".*

Even though there was general comfort related to the personal use of the Internet at work, results showed some sensitivity as revealed in only half of respondents (49%) reporting that they discuss their Internet usage with colleagues. Of these respondents, 91% said they discuss their usage with colleagues, but only 59% with family/friends and 56% with a manager/supervisor. Respondents were then asked if they try to conceal their personal use of the Internet, and 57% said *Sometimes* (54%) and *Always* (3%). Of those who do try to conceal their usage, most of the reasons related to potential embarrassment or a perception of a lack of professionalism, as shown in Table V below.

Table V: *Reasons for concealing personal Internet usage at work*

Response	Chart	Percentage	Count
I don't think others will understand my reasons		13%	5
I don't think others will understand the benefits		13%	5
I'm embarrassed		15%	6
I'm acting against the rules		15%	6
I don't know		26%	10
Other, please specify...		46%	18
	Total Responses		**39**

Notably, for this question about concealment, a substantial 46% of the respondents selected "Other, please specify" where a large proportion of the explanations were related to issues of professionalism and time management, including: *"perceived lack of professionalism"; "concerned it does not look professional"; "perception of poor time management"; "I don't want to be seen as using work time for personal internet usage"; "Je ne veux pas être perçue comme gaspillant du temps qui devrait être dédié au travail."* A lack of professionalism and time management, specifically, not wanting to appear unproductive, was also an explanation, e.g.: *"Don't want to appear unproductive"; "I think it's a work ethic thing,"* A certain number of responses referred to colleagues' perceptions in general, such as: *"for appearances – it's better to have work-related content showing and to avoid questions about (limited) personal usage of the Web"; "The perception of my usage by fellow colleagues"; "Reading personal as opposed to working is frowned upon".*

The Internet usage rules for employees in this organization allow for personal use before work, during morning and afternoon breaks, and after work. Some 35% of responses incorrectly identified these authorized times, with 20% of respondents answering *Don't know*. Table VI shows the time periods when respondents indicated they used the Internet for personal purposes. In addition, many employees admitted to personal use outside of these times, thereby being in known or unknown violation of rules. Table VII categorizes the results according to authorized and unauthorized periods, revealing that unauthorized access accounted for about one-quarter of Internet use.

Table VI: *On a typical workday, when do you access the Internet for personal use? (Please check all that apply)*

Response	Chart	Percentage	Count
Before starting work		55%	38
Anytime in the morning		25%	17
During morning break		26%	18
During lunch		84%	58
Anytime in the afternoon		22%	15
Afternoon breaks		32%	22
After a specific task is completed during the day		35%	24
At the end of the workday		36%	25
	Total Responses		**69**

Table VII: *Periods of Internet use categorized according to times given by respondents*

Response	Chart	Percentage	Instances
During Unauthorized times (defined as "anytime" or after a specific task is completed)		26%	56
During Authorized times (according to the periods permitted by workplace rules, i.e. before & after work, during prescribed breaks)		74%	161

In the online survey results, an overwhelming 95% of supervisors reported being aware – 76% were *somewhat aware* while 19% were *completely aware* – of both the personal authorized and unauthorized use of the Internet by their staff. Somewhat validating this perception, 74% of employees stated that they believed their immediate supervisors were *somewhat* (49%) or *completely* (25%) aware of their personal Internet usage. For example, respondent "LB" is a supervisor who stated that he knows that his manager is aware of his Internet usage, and he is equally aware of the habits of his own staff. *"Yes, he's aware. Does he think I'm 100% compliant? I don't think I believe that I'm 100% compliant. And, do I believe that all my employees are 100% compliant? I don't know."* Respondent "BK", an employee who indirectly supervises other staff, stated she *"100% absolutely"* knows that her supervisor is aware of the personal use of the Internet at work. *"(In fact), my manager often calls me over (saying), 'Come look at this stupid picture (online)',"* she added.

Some 62% of supervisors stated that they *sometimes* (48%) or *always* (14%) tolerated infractions of rules related to the personal use of the Internet at work. The reasons for overlooking infractions were varied, such as treating personal Internet usage as the same as personal conversations (by telephone 77% and face-to-face 69%), allowing employees to complete personal task at work (62%), and affording employees a stress-relief measure (54%), as shown in Table VIII:

Table VIII: *Reasons given by supervisors for tolerating infractions of Internet rules*

Response	Chart	Percentage	Count
It allows my employees to feel comfortable knowing that their personal online tasks can be completed at work		62%	8
It relieves work-related stress, anxiety among my staff		54%	7
It compensates my staff for demands, such as unpaid overtime		31%	4
It's the same as chatting about non-work-related topics with colleagues face-to-face		69%	9
It's the same as making or receiving personal phone calls		77%	10
It's a benefit for doing a good job, such as getting their work done quickly		46%	6
Use of the Internet shouldn't be controlled		8%	1
Other, please specify...		38%	5
	Total Responses		**13**

One supervisor explained that he overlooked infractions among his staff:

> *"As long as they got the job done, if they're listening to YouTube and had a blog roll open on the left side of their screen – as long as they got their work done efficiently, I didn't give a damn. (Respondent "PJ")*

Respondent "BK", an employee who indirectly supervises other staff, stated she would overlook an infraction as long as *"it wasn't excessive. If I thought that the individual's work was negatively impacted, I would say something. But so long as they are meeting stated expectations, reading email from their kid's school, doing banking, or exchanging emails with spouses (would be overlooked)."*

From the employee perspective, "FJ" explained why he believes his supervisor overlooks rule violations: *"If the work is getting done, then exactly how and why the pace is getting done shouldn't be as critical."* Another employee, "EB", with supervisory experience in a prior role, stated that his supervisor is aware of his Internet usage but is not concerned:

> *And, if he were to be concerned, I feel he would come to me, but as long as the work is not suffering… And, if the work is not suffering, and there are no red flags, nothing egregious, then it really comes down to a judgment call, a very subjective decision on his part whether to look the other way, for example, the quality of work or the reputation of the employee."*

Arising from interviews, explanations by supervisors for not taking action on the violations of employees were grouped into the following four reasons that will be analyzed in the next chapter:

1. My employees will put in extra time at work to compensate for their personal use.
2. My employees often go above and beyond.
3. My employees are performing well, that is, they are getting their work done.
4. I want to foster trust among their employees; this trust will lead to more productive employees.

On the worker side, the two most popular reasons given for their level of comfort in using the Internet at work for personal tasks were:

- it was seen as the same a making or receiving personal telephone calls; and
- it gave respondents an opportunity to complete personal online tasks at work.

A large percentage (72%) of respondents cited reasons for their personal use as:

- relieving work-related stress;
- compensation for demands by the employer;
- benefit for doing a good job; and
- making up for limited vacation time.

Interestingly, about a quarter (26%) of respondents gave an unprompted reason for feeling a level of comfort in their decision to use the Internet for personal reasons. The largest categories were related to the rule violations acting as both a reward and an incentive, as best noted in this comment at the end of the anonymous survey:

> *With reasonable and positive means, it can be acceptable. If you are a hard worker, and are honest and open with your colleagues and managers, and are sharing relevant information not necessarily within the written scope of your job description, I can see value in permitting online "personal" use.*

And, another respondent summarized several of the workplace dynamics that will be analyzed in the next chapter:

> *Some of us work hard and are unable to benefit from breaks, lunch and we work a lot of overtime. There is a push for work life balance and this helps some of us meet our personal tasks. My colleagues are in the same boat and I know that we are professional and would never abuse the system.*

Within this field site, employees were regularly exposed to several tools used by the employer to disseminate the rules regarding computer and Internet usage. Firstly, whenever an employee started their computer access to the network, they were presented with an Acceptable Use Policy (see Annex 3a) that they were to acknowledge before being granted access to the computer network. Secondly, in the two years prior to this investigation, two major guidance documents were published and promoted across the field site and across the entire federal bureaucracy (see annexes 3b & 3c). The documents explained the policies, in detail, related the use of the Internet – for personal, professional and work-related purposes – specifically, for all employees of the department in which the respondents work, and for all federal public servants, in general.

As one of the final questions of the anonymous survey, respondents were asked for effective methods to foster compliance with organizational rules related to the Internet. As shown below in Table IX, the results revealed corporate culture (98%) and the behaviour of managers and supervisors (94%) as helpful. On the other end, respondents ranked monitoring (25%) and performance incentives (25%) as not helpful at all.

Table IX: *Ideas to attain compliance with organizational policies related to Internet use*

	Not at all helpful	Somewhat helpful	Helpful	Extremely helpful	Total Responses
Clearly written policy documents	7 (9%)	23 (31%)	31 (41%)	14 (19%)	75
Training materials	8 (11%)	26 (35%)	33 (45%)	7 (9%)	74
Workshops	14 (19%)	24 (33%)	26 (36%)	9 (12%)	73
Speeches by managers	17 (24%)	27 (38%)	23 (32%)	5 (7%)	72
Performance incentives	18 (25%)	17 (23%)	26 (36%)	12 (16%)	73
Behaviour of managers and supervisors	5 (7%)	13 (18%)	37 (50%)	19 (26%)	74
Internal control mechanisms, e.g. surveillance	18 (25%)	23 (32%)	21 (29%)	11 (15%)	73

Corporate culture	2 (3%)	10 (14%)	39 (53%)	23 (31%)	74

Chapter 5: Analysis of Results

5.1 Introduction

In the analysis of results from this case-study investigation, we will see evidence of informal relations between managers and their staff built on a tacit toleration of rule-violation. This chapter will show how this relationship satisfies the conditions of a situated morality, specifically Anteby's (2008) Moral gray zone, that promotes desired occupational identities and relaxed organizational constraints for these office workers. The evidence uncovered through survey and interview responses, plus observations of both employees and managers, shows:

- A desire to appear professional in spite of the non-work-related activity;
- A mutual use of the Internet as informal compensation for time and effort; and
- A shared sense of trust between employees and their managers fostering job satisfaction.

We also analyze the relevance of de Certeau in the tactics of respondents in addition to their perceptions of employer strategies. Lastly, this chapter ends with possible reasons for the sustainability of the Moral gray zone.

5.2 Desired Occupational Identities

The personal use of the Internet was observed in strong relation to the desired professional identities of the modern-day office workers in this case-study investigation. In explaining the dynamics surrounding their use of the Internet in a survey plus interviews and observations, three themes related to their identity emerged, namely:

- A desire to act professionally by being informed, networked;
- A desire to be seen as behaving professionally, defined as being perceived as a productive and respectable employee; and
- A desire to simultaneously play roles as office worker plus parent, spouse and friend to those outside of the workplace.

5.2.1 A desire to act professionally by being informed, networked

As we saw in the previous chapter, the most frequently visited sites for personal reasons were general news sites (82%) far out-distancing online shopping (40%) and social media sites (31%). In fact, this "personal use" could, in fact, be connected to the predisposition and responsibilities of these respondents who work in the functional area of government communications requiring a high degree of autonomous duties and an awareness of the public environment. *"A lot of my work overlaps with personal use... I use the Internet to research social media functions but need to log into my personal account to learn about features,"* explained one respondent at the end of the anonymous survey. Time and again, the employees interviewed articulated this inter-connection between work and personal Internet usage: "*I maintain iGoogle on my computer so I can keep an eye on weather, breaking news, etc", and "Pour lire des journaux (nouvelles) ou des blogs politiques"*. "PJ", an employee and former supervisor, explained the Internet realities of his workplace:

> *Especially in communications, we often search for or need something on the Internet. For us, the line is very grey, blurred and we couldn't do our job without the Internet. We could be doing research for something, an analysis for something that takes us*

down a very wrong road. You're looking for something and find something (that is personally) interesting.

And, in a comment provided at the end of the survey, another respondent linked his curious nature and necessary occupational nature to his Internet use : *[Internet use] is a one of those situations that borders on a fine line. Sometimes when we are doing something for work purposes we see something that catches our eye. We want to investigate it. It's hard to turn off the curiosity light.*

Lastly, given that the third most popular type of sites visited were professional networking sites, such as LinkedIn – basically a "Facebook for career development" – we see another link between Internet usage and the professional identities of the respondents. The desire to act professionally by using the Internet to stay informed and networked was best explained by employee "FJ":

> *I use the Internet, as well, to follow people on Twitter, and the majority of the people I follow are in Government.*
>
> *And, when someone shares a link that's not related to work there are times that I check it out and read the first paragraph to see if it is interesting. And, if I find it compelling but it's not work-related, then I would bookmark it (to read) for later on the bus on my way home on my tablet, since I have a data plan, or in the evening on my computer.*
>
> *If the content is related to my job or Government-related, I would stop to take time to read the report for advice (I give) on current or future projects.*

This connection between professional identity and the personal use of the Internet is consistent with the common themes found by Fichtner and Strader (2014) in their review of 22 studies involving non-work-related computing (NWRC) issues, specifically:

- Employees who work in a job that requires creativity engage in more NWRC.
- There is a positive correlation between job autonomy and NWRC.
- The more time an employee spends on the Internet for job-related tasks, the more time he or she will spend on NWRC.
- The more opportunity an employee has to spend time on the Internet at work, the higher his or her perception that NWRC activities are acceptable.
  (Fichtner and Strader, 2014)

5.2.2 A desire to be seen as behaving professionally

Secondly, in this field site, there was a profound link detected between personal Internet use and the desire to appear professional in spite of the non-work-related activity. In the anonymous survey, interview and participant-observation results, reasons related to occupational identity emerged to explain both the level of comfort felt by respondents plus their actions to conceal a personal use of the Internet. Respondents conveyed a desire to be seen as behaving professionally, defined as being perceived as a productive and respectable employee by their colleagues.

Of those who try to conceal their usage, most of the reasons related to potential embarrassment or a perception of a lack of professionalism. For example, in the online survey, only 15% of the respondents cited a violation of rules as to why they would try to conceal their use, while 46% provided explanations related to appearing professional, with verbatim answers best summarized by *"for appearances – it's better to have work-related content showing and to avoid questions about (limited) personal usage of the Web"; and "Je ne veux pas être perçue comme gaspillant du temps qui devrait être dédié au travail."*

This sentiment also manifested itself in the frequent positioning of the computer monitors away from the opening in cubes to avoid passers-by seeing the content of screens. This preference cannot be explained by an employee seeking to protect awareness to any work files since communication projects are typically divided into autonomous segments, such as drafting a media release, undertaken by an employee towards a common initiative, for example, a public presentation by a government official. Perhaps “EB” described this desire to uphold his identity most powerfully: *“I don’t really want someone walking by and seeing me on the Shopping Network, Facebook or something else.”* As we saw in a large number of responses, it was the potential embarrassment and damage to the perceived identity of respondents – not the violation of the explicit rules – that was driving them to conceal their personal use. The desire of employees to appear professional spoke to their sense of identity, specifically, how they perceive themselves and how they want to be perceived, that is, the management of their impression amid this office workplace activity. Respondent “BK” explained that this sense of professionalism serves to prevent abuses: *“I wouldn’t go to sites that I wouldn’t feel comfortable with my ADM (assistant deputy minister, the senior manager in the branch) seeing me visit.”* “BK” then explained the connection between her role and the issue of trust, explored later in this chapter: *“I think (my manager) trusts my professional judgment that I wouldn’t do anything to get into trouble.”*

This observed reality is consistent with the occupational communities described by Van Maanen and Barley (1984) that create and sustain relatively unique work cultures consisting of:

- task rituals;

- standards for proper and improper behaviour work codes surrounding relatively routine practices; and
- compelling accounts attesting to the logic and value of rituals and standards.

And, in the airplane factory, Anteby (2008) found desired occupational identities were fostered through the leniency afforded workers to break rules and create home. His moral gray zone featured enacted identities in evaluating how workers viewed themselves and how others viewed them. In this case-study investigation, the desire to protect the perception of an office worker's professional identity served to conceal and moderate – but not defend or rationalize – the violation of the workplace rules governing personal Internet use.

5.2.3 A desire to use ICTs to play multiple roles

Lastly, the connection to the personal use of the Internet was observed in the blurring of identity between office workers and their role as a parent, spouse or friend outside the workplace. The blurring of work and personal tasks and time is clearly evident in this research. As we saw in the previous chapter, employees reported using the Internet often (18%) and sometimes (63%) to complete personal tasks, such as banking or travel, in many instances against organization rules. In one of the most extensive comments provided in the anonymous survey, this respondent summarized the reason she accessed the workplace Internet for personal use in one word: "Multi-tasking" and then explained:

> *The ability to multi-task between personal items – research, staying on top of a situation, monitoring the health of a severely ill or aging family member, etcetera – is part of the blurring of lines between work and personal lives that the modern IT era heralds. In many cases this likely leads to an increase in productivity among workers who use information technology in their daily lives - especially those with work-issued*

smart phones for whom the work-day hours are relatively arbitrary, and who are still sending emails at 9:30pm.

In addition to demonstrating Anteby's (2008) view that bending the rules can cater to occupational identifies, the perception of respondents in this case study supported the findings of König and Caner de la Guardia (2014) in their exploration of the positive side of personal Internet use at work: "people's personal use of the internet at work can be considered as a response to the blurred border between work and non-work – as many employees are expected to answer work emails at home, they might reciprocate this by answering private emails at work." (p. 355)

On another level, likely aiding the blurring phenomenon, is the juggling of the technology for personal and work tasks, as captured best in the following comments entered at the end of the anonymous survey:

Il me semble que l'utilisation des Blackberry personnels doivent aussi être considérée. Je suis toujours émerveillée de voir combien les jeunes fonctionnaires répondent à deux Blackberry, soit celui du bureau et le leur.

(The) key point is that the internet is interwoven into our lives, and as a government we are not adapting well. Phone/personal devices are good examples. Employees should not be expected to have a work device and a personal device. That is counter-productive.

And, in a comment that explicitly speaks to the ease for employees to allow the convergence of personal and work ICTs:

I do not have a mobile device (cell or BB) so my work e-mail is often the way most people reach me when they need a response in a hurry.

We saw support among respondents to merge personal and workplace ICTs. And, this notion was expressed without major concern for any increased monitoring that Mazmanian et al (2006) noted about the Blackberry becoming an "electronic leash".

5.3 Relaxed Organizational Constraints

By analyzing various relaxed organizational constraints, we can better understand how office workers negotiate what is acceptable in terms of non-work related Internet use, and how their supervisors justify their subjective enforcement of the rules. As we saw in the description of results, almost three-quarters of respondents cited reasons supporting the existence of a situated morality in which they violated rules governing the use of the Internet for personal reasons. Their reasons included:

- relieving work-related stress and boredom;
- compensating for the extra demands by the employer; and
- earning a reward for doing a good job.

This research points to benefits for supervisors, such as the flexibility to recognize the extra efforts of their staff to complete work under tight deadlines; an alternative form of compensation for doing a good job; and, most importantly for the relationship, the fostering of trust. Workers also identified a form of informal compensation for their hard work, plus a perceived increase in productivity, if they can use the Internet for personal purposes.

5.3.1 To relieve work-related stress and boredom

As we described in the previous chapter, almost thirds (65%) of respondents explained that they often or sometimes used the Internet for personal purposes as a way to reduce stress. In a comment made at the end of the anonymous survey, one respondent acknowledged both the value and risk behind this anti-stress remedy:

> *I think personal internet use can be distracting but if it wasn't an option I'd find something else to have mini unwinds during the day. Having said that, personal internet use is a slippery slope and requires discipline in order for it not to negatively effect ones work.*

In their review of 22 studies involving non-work-related computing (NWRC) issues, Fichtner and Strader (2014) found that employees perceive NWRC as a form of stress relief; however, efforts to prove that job stress leads to more NWRC were inconclusive. In this work site, characterized by often-urgent communication demands on employees from government ministers, the research did not shed any light on causation. Beyond general references to relieving stress, respondents were not asked to elaborate on sources of stress, such as time pressures or work-overload.

Another major benefit cited by respondents in this investigation was to relieve boredom (50% in total with 38% reporting "sometimes" and 12% "often"). The causes related to the boredom were not uncovered in this investigation; however, they may be linked to the lack of work-related tasks as one employee, "BD", explained: *"There are some people who complete their tasks and will fill their time going on the Internet because they have some extra time."* Employee "MZ" stated, "*there were periods of time when I had extra time (so I used the Internet for personal purposes)."* Therefore, we are seeing traces of Roy's (1954) Banana Time study of New York garment factory workers who kept boredom at bay through routine behaviours during break times. And, the continuation of this observation from the factory floor to the office cube would support findings of Ivarsson and Larsson (2011) who found that: "Some Internet surfing is actually a consequence of organisations' inability to come up with decent work tasks to fill the whole day" (p. 63). However, Fichtner and Strader (2014) did not find any consensus in their review of associated studies to confirm that boring work environments lead to increased non-work-related computer use.

5.3.2 To compensate for the extra demands by the employer

As noted previously, the employees of this communications branch are focused on providing products and services to government ministers. Given the unpredictable nature of politics, employees can often find themselves in the midst of urgent deadlines to complete tasks for senior officials. Echoing Anteby's findings that moral gray zones offer a flexible way to compensate employees, some employees reported that their personal use of the Internet is a way to get something in return for additional effort given to the organization. An employee, "JL", with prior supervisory experience summarized this rationalization: *"They (managers) do have compassion because they know that for a whole week you've been working late until 9pm and had no time to get to the bank…[so] it's okay to pay my bills [online]."*

The reality in this workplace would support the connection between work overload and personal Internet use, specifically its justification due to excessive job expectations (Fichtner & Strader, 2014). And, this embodiment of value in Internet use appears consistent with Tennakoon et al's (2013) observation that managers and professionals routinely take their work into their private hours with no extra pay since compensation relates "more to specific duties and responsibilities than to prescribed hours of work" (Tennakoon et al, 2013, p. 114).

5.3.3. To earn a reward for doing a good job

In a motivation related to informal compensation as explained in the previous point, a quarter (26%) of respondents reported perceiving personal Internet use as benefit for doing good work, such as getting tasks done quickly or working overtime. Employee "EB" best summarized this link between good productivity and personal Internet use: *"And, if (my manager) were to be concerned, I feel he would come to me, but as long as the work is not suffering, having the freedom to explore the Web freely is much more valuable to (me in my) research analyst position."* The literature is sparse on the personal use of Internet as a reward; however, it can be understood through the lens of a moral gray zone, explored later in this chapter.

As we have clearly seen, employees in this investigation primarily explained their violation of organizational rules as a way to obtain informal or alternative forms of compensation from the employer. Interestingly, explanations by supervisors for not taking action on violations were grouped into four similar major reasons, also pointing to the flexibility in offering informal compensation as a benefit of the non-enforcement of rules:

1. My employees will put in extra time at work to compensate for their personal use.
2. My employees often go above and beyond.
3. My employees are performing well, that is, they are getting their work done.
4. I want to foster trust among their employees; this trust will lead to more productive employees.

Interestingly, two of the main reasons provided by employees – to compensate for the extra demands by the employer and to earn a reward for doing a good job – mirror the first justification given by supervisors and speak to the mutually agreed upon parameters of this situated morality. Evidence for this shared recognition of the benefit of the flexibility stemming from this moral gray zone can be seen in the following responses: Supervisor “LB” stated: “*Do I believe that all my employees are 100% compliant (with Internet usage rules)? I don’t know. Do I think they make up for it by giving me extra time at the end of the day? Yes.”* In a related rationale, doing more work than is required was another reason to overlook infractions. As a supervisor, “LG” said she was aware of the Internet use of the people she supervised: “*I do know they were online, but I was okay with that because of the time they were putting into at work.”* And this perception was shared by workers, as we saw in the previous section.

Lastly, if a worker were productive, it would often lead supervisors to overlook any violations of personal Internet use, as articulated by “LG”, a manager of more than 20 workers:

> *Some people do listen to live music streaming or listen to a game or the Olympics. As long as it doesn’t interfere with their work, I’m okay with it in moderation, but not if they’re listening to games or the Olympics all the time as it’s got to affect their concentration.*

Surprisingly, even a worker who said she did not use the Internet at work for personal tasks agreed that she would likely overlook any infraction if the employee were doing their work. *“If I had been a director or manager, I would overlook someone listening to music because they are still being productive.”* employee “NK” stated.

In this workplace, both workers and their supervisors saw the personal and often unauthorized use of the Internet as unofficial compensation for conditions of employment, such as working late. For the supervisors in this case study, they are caught in a middle area where they are not designers of the organization's policies; however, they are expected to step in with authority if an egregious use of the Internet emerged. Senior manager "LG" explained: *"If there were an issue, I would deal with it. If their work isn't up to par, I wouldn't look the other way. For example, some people listen to [continually downloaded] music with discernment. If it's reasonable, I would look the other way."* And, this approach appears shared by workers as expressed in this response from employee "CI": *"I don't know if they would really actively think of [making us compliant] unless there is cause for concern or there is some department push to look into it or mention it to staff."*

These justifications align with Anteby's (2008) finding that the moral gray zone in his manufacturing plant allowed for the benefits of homers to emerge for supervisors who, like the office workers, were covered by a rigid labour agreement. Specifically, Anteby (2008) showed how the tolerance of the creation of homers provided:

- Greater flexibility from workers during peak production periods;
- Compensation for doing well;
- A hidden incentive or "efficiency wage"; and
- Compensation for restrictive collective agreements.

The office workplace in this case study exhibited the same characteristics as Anteby's (2008) moral gray zones that he described as collective endeavours, not individual or "one-shot deals" between a manager and an employee. The participants, not the organization, define the rules in moral gray zones, according to Anteby (2008), that appear to exist in both airplane factories and in offices. Leniencies are part of the managerial toolkit, allowing for "local regulation": in other words, moral gray zones allow work to be done (Legace, 2009). Supervisors in this investigation did not single out one employee for special treatment; rather, the tacit acceptance of rule-breaking amid relaxed organizational constraints afforded layers of benefits to both organization and employee, most noticeably, informal compensation and recognition, flexibility, and trust. We can also see a similarity with Gouldner's Indulgency pattern of informal relations and leniencies between workers and managers generating organizational benefits, to be examined in the next section.

5.4 A Trusting Environment

As shown above, evidence emerged of informal relations between supervisors and their staff in their negotiation of the personal use of the Internet at work. Arguably, the most important observation emerging from this situated morality is the positive dynamic of trust – both intentionally fostered by supervisors as well as perceived by workers – creating the perception of a happier, more productive workplace. It is relevant to note that the last three benefits perceived by supervisors are similar but occur at different points. The first reward is for past productivity that has already occurred, while the last one is an incentive for productivity to emerge through an extension of trust. In other words, the supervisor's view is "my employees are productive and I reward them by overlooking rules" or "I overlook by demonstrating my trust in the hopes that my employees will become/remain productive."

Indeed, trust was cited as a greater, long-term imperative behind the reasons that some of the infractions that were overlooked. For example, one supervisor stated: *"The rules are bent for employees who deliver on their work. If all work is done on time and delivering more work, I would never check on employees who are producing because I implicitly trust them."* Supervisors said they trusted their employees to make up any time spent on the Internet for personal purposes. In addition, supervisors want to show their workers they were trusted to increase job satisfaction along the lines that: *"If I trust them, they will be more productive."* Senior manager "LB" best expressed this management approach:

> *A minor use of the Internet is okay in the workplace. Maybe it maintains morale or allows me to show I trust my employees, and there is pay off for that. It all goes to my management style.*
>
> *If my employees know that I trust them, they are more likely to engage with me more, or they are more likely to tell me the truth about things, and they are more likely to come up with ideas. It's better to have a conversation.*
>
> *If you are spying on employees, they will learn to hide their behaviour in other ways. A boss who is not liked very well won't have employees who perform well.*

And, this perception was shared by workers. In answer to the question, "Do you think your supervisors think you are compliant?" "BB" responded: *"100% of the time? I doubt it that he thinks I'm always in compliance. I think he trusts my professional judgement that I wouldn't do anything to get into trouble."* "MZ" recalls her former supervisor being aware of her personal Internet usage and linked it to shared trust. *"She trusted me and it never interfered with my duties. I always delivered on time."* MZ, who was interviewed after she left the field site and now supervises staff, explained that she developed a trusting attitude, in part, because she was trusted herself. *"If you give them (employees) trust, then they probably trust you and work harder and be more productive, tend not to be away [from work], and provide more input in work."*

This is the same two-way, mutual trust found by both Gouldner in the gypsum mine and by Anteby in the airplane factory. The Indulgency pattern prompted the mine workers to trust the management and follow its lead (Gouldner, 1954). And "Old Doug", the manager, trusted that the workers would get their jobs done (Hallett & Ventresca, 2006). Anteby (2008) explains that moral gray zones in organizations rely on trust between supervisors and their workers. These zones test middle management's ability to manage and to prevent abuses of mutual trust. Indeed, Konig and Caner de la Guardia found a similar connection between ICTs and trust in their 2014 research, explained later.

5.5 Not a Tactic of Retaliation or Organizational Misbehaviour

While we observed desired occupational identities, relaxed organization constraints plus a shared sense of trust, the analysis did not reveal notions of retaliation or any organizational misbehaviour, such as cyber-loafing and time banditry.

To begin, Lieberman’s (2010) "Hydraulic effect" of employees releasing frustrations by engaging in minor ethical wrongdoings was not observed in this investigation. No notion of malicious intent or retaliation emerged in the explanations or justifications provided in the survey, interviews nor in the participant-observation. In fact, the research showed predominantly positive perceptions about employees’ roles and their views of the organization. Employee “EB” best expressed his sentiment: *“I would never do anything to jeopardize my job, the files I’m working on, that is, the corporate body, or my reputation.”*

Michel de Certeau (1984) would likely contend that the creation of homers by Anteby’s (2008) factory workers was a rebellious tactic striking out against the control of management. In the office workplace, de Certeau’s view would be somewhat supported by Lim (2002) who found that office employees will intentionally break rules to use the workplace computer for personal reasons as a means of retaliation against their organization. De Certeau explains that employees respond with tactics that are “available to the common man for reclaiming his own autonomy from the all-pervasive forces of commerce, politics and culture." (np) However, this dynamic was not observed in this case study as there was no trace of the personal use of the Internet as a malicious, or even protest action, against the organization. In fact, only one respondent of the online survey selected, *"It gives me a way to retaliate against the organization's control over me"* to explain their personal use of the Internet. One could argue that we see evidence of de Certeau's subtle tactics in employees trying to conceal their Internet use by turning their screens away from the eyes of passers-by; however, this was viewed more substantively in the context of professionalism, as previously presented in this chapter.

In addition, a conventional lens of organizational misbehaviour (OMB) does not apply in general to the use of the Internet in this investigation, nor specifically in terms of time banditry, defined by Martin et al (2010) "as the propensity of employees to engage in non-work related activities during work time (that is) they are using paid organizational time for personal reasons." (p. 26) Only 12% of the respondents in this investigation perceived their activity as a form of time theft. Yes, the results show that employees were disregarding the rules, and they were often on paid time when using the Internet; however, they strongly contended that their actions were necessary to allow them to act professionally by being informed, networked and to play simultaneous roles as office worker, parent, spouse and friend. And, as we saw described in the previous chapter and analyzed in this chapter, a whopping 96% of respondents explained that they often or sometimes used the Internet for personal purposes to take a break. Contrary to any notion of "time banditry," they pointed to a series of benefits for the organization that are far from counter-productive to the work environment. For example, many respondents saw their personal Internet use as enhancing their productivity, such as employee "FJ" who cited workplace studies: *"There are a lot of* *studies that suggest short breaks from tasks allow people to apply yourself more effectively. (For example) we have mandated coffee breaks."* Senior manager "LB" likened his personal Internet use to taking a break away from his desk: *"I go downstairs for coffee 3 times a day, and it probably increases my productivity because I can work around to think, get a jolt of caffeine and stretch my legs… at the end of the day, it makes me a happier employee and taxpayers are better off."* These responses further supported other research that found taking breaks by doing general unwork-related actions can increase job satisfaction and enjoyment (Roy, 1959) as can engaging in personal Internet usage (Duhita & Daellenbach, 2015), (Messarra, Karkoulian & McCarthy, 2011), (Coker, 2013).

5.6 Strategies of Control

About one-third of respondents (33%) stated that they should be able to freely access the workplace Internet for personal use, with 53% saying it should "sometimes" be controlled, and only 16% of supporting regulations. As employee and former supervisor "PJ" explained:

> *I think it's a poor manager who tries to over-regulate employees' use of the Internet as long as they are producing and delivering. I think employees who enjoyed their job [should have freedom]. I would be more likely to check on employees who were consistently not producing or delivering for potential abuse of the Internet.*

In this field site, we saw several of Van Gramberg et al's (2014) management strategies to regulate or control the online behaviour of employees, namely policy and procedures in the workplace, monitoring and surveillance, and discipline and dismissal.

However, respondents did not see much value in monitoring, policies or speeches as ways to foster compliance of workplace rules governing Internet use as shown previously in Table IX.

Monitoring was the most frequent technique of control that was mentioned without prompting. Employee "MZ" explained: *"I got the sense that my use was being monitored. It's their [the government's] equipment and the organization would have the right to know how the equipment is used, and I assumed that was being monitored."*

Only one respondent, "NK", referred to a professional code of conduct governing her actions, and she made that comment to explain her workplace identity. *"I strongly believe for all Internet users in [our] professional field that the Code of Ethics and Values be followed."* Codified rules of conduct within organizations are often based on the "boundary zone" of actions, where employees may be confused and need guidance on how to behave in the organization (Balch & Armstrong, 2010): "An action that is clearly out of bounds requires little ethical sophistication to judge. On the other hand, an action that is marginal – perhaps ethical, perhaps not – requires ethical imagination and sophistication to assess…" (p. 291) At this field site, the "imagination" and "sophistication" may find its source in a moral gray zone, as explained later in this chapter.

In fact, many respondents, such as employee "FJ", called into question whether a solution resides in any traditional methods of organizational control: *"I'm of the opinion that specific policies on the use of the Internet versus the phone, water-cooler are related to time management – if they're looking to distract, there are so many ways. Focusing on [rules regulating use of] the Internet is short-sighted. It's really a management and work problem."* Another respondent remarked: *"If people are not being productive, then those individuals should be disciplined. If people are being productive, (there is) no need to police their Internet usage."*

And, in the anonymous survey, many respondents provided other methods to foster compliance with workplace rules governing the Internet, such as those expressed in the following detailed comments:

> *Be open about it. Encourage employees to feel at home in the workplace and blur the lines but make it clear what is expected of them. They earn a paycheque - they owe superior work performance. Providing them with Internet use is, frankly, an expected recruitment and retention issue, and without it we will see declines in productivity, innovation, leadership, etc. Employees will find a way around the bans using technology, and it will create a poisonous atmosphere.*
>
> *Some employees will always do what they want to. Some will always follow the rules. Most will work somewhere in between. I think making employees feel useful and valued will help to engage them in the office, and make them want to be better workers, including following policies. Surveillance is expensive, and doesn't catch what people do on cell phones.*

In another free-form survey comment, a likely older supervisor flatly rejected the value of monitoring:

> *They are more productive when they know that managers are not looking over their shoulder. Many of them are younger and extremely technologically adept, and for them the work/personal lines (especially online) are blurred.*
> *Many of them bring personal, private-life skills to the workplace to the benefit of us all - especially in the area of online marketing savvy, use of social media, etc. It would be doing them and us a disservice to monitor them too closely.*
> *As long as they maintain a respectful workplace environment, complete their tasks, innovate, lead, and do not use the Internet inappropriately (i.e. browsing for illicit items, material, etc.), I support their blurring of those lines.*

Ironically, the workplace trust within the moral gray zone is built upon an informal relationship stemming from a tacit tolerance for rule violation. Yet, it appears vulnerable to be shattered by workplace surveillance. In a detailed comment at the end of the survey, one respondent wrote:

> *When a culture of mutual respect is created, employees are more apt to want to contribute 'above and beyond' expectations.*
> *Monitoring behaviour and/or technologies is both disrespectful and ineffective in creating happy, productive workers.*

Indeed, this sentiment is shared by research in the decades after ICT monitoring has been installed in workplaces. As cited earlier, König and Caner de la Guardia's 2014 study exploring a work-life balance found: "employers in our sample only seldom seem to restrict internet use or check the type of web pages visited by employees, maybe because employers fear that a restriction could foster a climate of distrust." (p. 359) And, Van Gramberg et al (2014) found that:

> …electronic surveillance, whether or not it is expected or accepted, can result in panoptic effects where employees begin to feel they are being controlled by the very equipment they need to use at work and yet they are powerless to deal with it.
> A body of research demonstrates that employee responses can range from passive compliance to lack of trust, low morale and low commitment, problems which are counter to the purpose of human resources management (HRM) policies and practices. (Van Gramberg et al, 2014, p. 2246)

Therefore, if traditional bureaucratic control mechanisms are not sufficient as found in this investigation, can more diffuse mechanisms such as Barker's Concertive control approach help us understand counter-productive behaviour that is accepted by the group, such as the widespread personal use of the Internet on the job? While a fascinating ethnographic case, an observer will see that Barker's 1993 study of factory workers at a small manufacturing company has little in common with employees working in office cubes. Could it be that everyone's actions or inaction are visible on Barker's factory floor, as opposed to the semi-private existence of the office worker's cube? As well, Barker (1993) concedes that Concertive control does not free employees from Weber's "iron cage" of rational control. Instead, Barker's (1993) concertive system constricts the "iron cage" tighter to constrain the participants more powerfully. Barker writes, "Workers in a concertive organization create the meanings that, in turn, structure the system of their own control. Rule generation moves from the traditional supervisor-subordinate relationship to the actors' negotiated consensus about values." (1993, p. 412) Lastly, Barker's theory rests on a system of value-based normative rules that controlled actions in collective pursuits through self-managing teams.

However, the problematic in this investigation focused on a system where individuals ignore normative and explicit rules for personal ends. So, why don't self-managing teams – widely embraced by office-based organizations – serve to curb the growing unauthorized use of Internet among team members? Why doesn't the cage tighten its hold on activities that inherently do not contribute to the advancement of the teams? Is it because the unauthorized practice is so pervasive that everyone is doing it on the team, so it evens out? Or, is it because there are other dynamics at play? This investigation has shed light on another dynamic: a Moral gray zone that suggests an unauthorized practice can contribute to the advancement of the organization.

5.7 Sustaining a Moral Gray Zone

Our analysis did not reveal notions of retaliation or any organizational misbehaviour, such as cyber-loafing and time banditry, in the personal use of the Internet in this workplace. Instead, the survey, interview and observation data obtained from employees and supervisors point to the existence of a moral gray zone, defined as "(situations) in which workers and their supervisors together engage in practices that are officially forbidden, yet tolerated by the organization" (Anteby, 2008, p. 2). As explained in the Problematisation chapter, two conditions are necessary for the existence of moral gray zones, namely:

1. There is a violation of official company rules.
2. Supervisors provide explicit or tacit approval of the violations.

(Anteby, 2008)

Respondents in this case-study investigation admitted to the personal use of the Internet outside of the times permitted by the organization, thereby knowingly or unknowingly breaking rules. With the rule violations tacitly overlooked, we then saw how the situated morality of a moral gray zone in this office workplace provided the same benefits to the organization that Anteby (2008) discovered in his research in a manufacturing plant.

In the office workplace in this investigation, we have observed desired occupational identities centering particularly on professionalism, relaxed organization constraints, plus a shared sense of trust derived from a moral gray zone. We observed a situation in which individuals must continually make judgments as to the appropriateness of their actions. They appear to do so not solely on the basis of their individual ethical values, but as part of a collective, following tacit understandings featuring an informal contract based on mutual trust – a give and take – with limited adverse and many positive consequences for the organization.

The data points to the emergence and sustainability of the moral gray zone, fostered by the workers and their supervisors for different but complementary reasons, serving to diversify and strengthen its roots. For example, desired occupational identities were promoted through a sense of professionalism while using the Internet for non-work-related tasks. Then, the relaxed organizational constraints afforded layers of benefits to both organization and employee, most noticeably, informal compensation and recognition, flexibility, and mutual trust – tools sought by both managers and their staff for a smoothly functioning workplace.

The notion raised by many respondents in support of merging ICT tools – such as computers and smartphones for combined work and personal purposes – pointed to another possible reason for the sustainability of the moral gray zone. In explaining why he believes his supervisor overlooks infractions, employee JF replied: *"[We] use the Internet for day-to-day tasks because it's part of our lifestyle. There's a bit of blurring between work and home life. People use their Blackberry at home for work."* Another reason for the tacit overlooking of rules could be in the complicity of both workers and supervisors that fosters not just trust, as explained earlier, but also teamwork and a common experience with ICTs. This view was best described by employee and former supervisor "PJ" who highlighted shared professional benefits because the Internet was interwoven into their daily, desired work habits:

> *Sure [he is aware], because we all access the Internet during various times of the day, such as listening to music on YouTube, but I might send a link to show them [colleagues] something.*
> *I don't think that's detrimental but is, in fact, good for teamwork.*
> *All of us – from director on down – we're all involved in that.*

Not a day goes by we're not showing something [that we found online].

And, in another anonymous comment at the end of the survey, we can see recognition of an informal relationship and a situated morality within the work environment:

> *With reasonable and positive means, it can be acceptable. If you are a hard worker, and are honest and open with your colleagues and managers, and are sharing relevant information not necessarily within the written scope of your job description, I can see value in permitting online "personal" use.*

The majority of office workers defended their moral gray zone by contending that they were not doing anything "wrong" – a sentiment best expressed by employee "BK":

> *"I don't think using the Internet at work is any more stealing time than answering my [work] Blackberry at home. There's a give and take. My life is so fluid between all roles of life: parent, student, employee; [for example] I log in at night to clear [work] emails."*

Lastly, despite the dire predictions of Van Gramberg et al (2014) about the adverse impact of workplace surveillance on workplace relations, Anteby (2008) contends that moral gray zones rely on a trust that is difficult to break. Even if monitoring of employees increases, gray zones are here to stay because they involve tacit management approval and occupational identity pursuits (Anteby, 2008). According to Anteby: "It is not because employees are more highly monitored that gray zones will disappear; instead, employees are now made more aware of their supervisor's tacit approval. In other words, the give and take operating in gray zones is made more explicit." (Lagace, 2009, p. 2)

Through the research findings and analysis described above, we discovered that office workers and their supervisors negotiate what is acceptable in terms of non-work related Internet use – even when it is prohibited – through informal relations between built on a tacit toleration of rule-violation. This relationship was shown to satisfy the conditions of a situated morality, specifically Anteby's Moral gray zone that promoted desired occupational identities and relaxed organizational constraints, namely:

- A desire to appear professional in spite of the non-work-related activity;
- A mutual but unofficial compensation in flexibility and compensation; and
- A shared sense of trust between employees and their managers fostering job satisfaction.

While we saw evidence of tactics, they were not of the retaliatory kind articulated by de Certeau or even those working in Lieberman's (2010) "Hydraulic effect". Lastly, the research showed that personal Internet use is not always cyber-loafing, cyber-slacking or time banditry; in fact, in addition to the benefits linked to the moral gray zone, there was evidence of positive outcomes for both employees and the employer when they took a break to use the Internet for personal tasks, such as stress relief and increased productivity.

Conclusion

Summary

The prevailing view for the last three decades has relegated unintended personal ICT usage to a stable home in *Organizational misbehaviour* and *Counter-productive work behaviour,* alongside other behaviours, such as physical aggression and violence, substance abuse, absenteeism, theft, destruction of property. Contrarily, this research did not begin with the assumption that the personal use of the Internet at work is “bad”. Rather, in addition to Michel Anteby’s (2008) adaptation of Moral gray zones for a workplace, this researcher found value in Anteby’s non-judgmental perspective toward unauthorized activities, specifically the creation of “homers”. The underlying premise and compass direction for this thesis was modeled on Anteby’s approach. We focused on why and how a rationally designed and professionally managed organization could permit a moral gray zone to develop. We sought answers through the study of personal Internet use by refraining from judgement to better understand the depth and impact of the dynamics surrounding supervisors, their staff and the Internet.

Through the approach and our findings, we discovered answers to our central research questions, namely, the ways in which a situated morality allows:

- Office workers to negotiate what is acceptable in terms of non-work related Internet use, often when it is prohibited; and
- Supervisors to justify their subjective enforcement of rules governing the non-work related Internet use among their employees.

Survey and interview responses, plus observations of both workers and supervisors, revealed evidence of:

- A desire to appear professional in spite of the non-work-related activity;
- A mutual use of the Internet as informal compensation for time and effort; and
- A shared sense of trust between employees and their managers fostering job satisfaction.

Although we started with Anteby's (2008) Moral gray zone, we also found similarity between the situated moralities shared by our office workers and Gouldner's (1954) gypsum miners who enjoyed an "Indulgency pattern". Both are workplace dynamics that generated organizational benefits, such as mutual trust, when rules were violated with tacit approval. While we saw evidence of tactics, they were not of the retaliatory kind articulated by de Certeau (1984), nor were they manifestations of the minor "escape-valve" actions of Lieberman's (2010) "Hydraulic effect".

Lastly, this investigation greatly benefitted from answers from supervisors and workers to an anonymous 30-question online survey focused on self-reported behaviour of Internet usage for both work-related and personal purposes, as well as awareness of practices and policies. Based on these results, the series of hour-long, follow-up interviews conducted with 11 survey respondents – again of varying functional levels – provided robust insights into the reasons and motivations behind the survey answers.

Contributions

The resulting contribution of this thesis can be explained in varying degrees and with some originality in three areas: empirical, methodological, and theoretical.

Foundationally, the research was conducted in an uncommon field site, that is, a government workplace typically difficult to investigate, even by employees. Once access was gained, this investigation built upon themes that were previously mainly observed in factories, so we are now able to show similarities and differences with the peculiarities of an office environment. The researcher's familiarity of this field site and its respondents likely enhanced the collection of insights to understand the consequences of actions – intended and unintended – by both employee and employer. And, the deliberate inclusion of managers and staff allowed us analyze the workplace dynamics from dual perspectives.

Lastly, the pervasive non-judgmental approach may have more easily unearthed the often-frank admissions of rule violations from both workers and their supervisors. In their explanations, greater benefits to themselves and their organization were hailed – consistent with the benefits of a moral gray zone – from the promotion of desired professional identities to relaxed organizations constraints to a reduction of stress and enhancement of job satisfaction. A rebuttal to the negative perception in the literature towards the personal use of the Internet was best captured by supervisor "PJ" in explaining the circumstances in which he overlooked Internet infractions among his staff: *"As long as they [staff] got the job done – if they're listening to YouTube and had a blog roll open on the left side of their screen – as long as they got their work done efficiently, I didn't give a damn."*

The design and implementation of this ethnographic workplace approach was not particularly innovative. However, its use of multiple methods – anonymous survey, in-depth interview and observation – did detect and probe the existence and sustainability of a situated morality. And, the participation of more than 70 workers and supervisors yielded a nearly 30% response rate. Most notably, the respondents came from a diverse group, ranging from junior employees to senior managers, who contributed to a fuller understanding of the dynamics of personal Internet use at work.

Most originally, this investigation overcame the traditional risk aversion of public servants in allowing researchers to study their daily practices. It is not common for a government office and its employees to serve as an unfettered research site for an independent thesis investigation. Thanks to a courageous senior executive, permission to conduct this research *in situ* was granted. Then, this researcher needed to be inventive to supplement his long-established identity as a colleague with that of a student-researcher. Care was taken – through detailed disclaimers and appropriately timed interventions – to keep collective work responsibilities separate from independent research tasks. At all times, caution was needed to mitigate bias from the researcher and from the research process to uncover insights on a topic that inherently straddled the often-blurred line between the work and personal lives of respondents.

There was no ambition to construct a theory or to offer generalizations of the personal use of the Internet in the workplace from this research. However, we did see that a case-study approach was valuable in discovering patterns and validating observations from other settings, such as Roy's garment factory, Gouldner's gypsum mine, and Anteby's manufacturing plant. Indeed, this thesis found evidence of informal relations between managers and their staff built on a tacit toleration of rule-violation. The daily practices of workers and their supervisors revealed a relationship that was shown to satisfy the conditions of a situated morality, specifically Anteby's Moral gray zone, in promoting desired occupational identities and relaxing organizational constraints.

The research showed that personal Internet use is not always cyber-loafing and should not automatically be seen as time banditry as it has been predominantly portrayed in the literature since the Internet age entered the workplace. In fact, taking an ICT break was found to herald stress relief, foster job satisfaction and enhance productivity among our respondents – matching the positive outcomes that Roy (1959) observed with his garment machine operators – showing that organizations can still benefit when their employees have fun at work – more than a half-century later. This is perhaps the most important theoretical contribution from this thesis: it takes personal Internet use out of the organizational misbehaviour and retaliation perspective and places it within a positive lens to more fully understand this workplace phenomenon.

Research Limitations

This researcher has no allusions that this work is without flaws. Indeed, there are several major limitations that must be noted. Firstly, this researcher recognizes that the potential to theorize from a case-study approach is limited. Case studies can show a detailed view of an activity, but they cannot provide the foundation for a robust theory or even generalization flowing from the data. It is hoped that this researcher did not fall victim to the risk that Stake (2000) articulates when a researcher possesses a strong desire to generalize and then fails to fully understand important features of the case study.

Secondly, the time between the field site investigation and the completion of this thesis should have been much shorter. However, given the heavy work and family commitments of this part-time student, a shorter time frame was not possible. Fortunately, the field site conditions – such as Internet access and workplace policies – have not changed in the years since the surveys, interviews and observations were completed. And, the body of literature that casts a positive spotlight on the personal use of the Internet has, in fact, grown since this researcher defended his *projet de these*.

Thirdly, since this researcher was also a colleague of respondents, no amount of precautions or disclaimers could prevent any unintentional bias that may have coloured the research and analysis. Lastly, a fuller, detailed portrait of the dynamics could have been created with a more robust participant-observation approach, as originally planned.

Ideas for Future Research

An "alternate universe-type" thesis topic regularly beckoned this researcher in the final stages of this investigation. It was centred around a thread of unintended consequences both positive – as seen in Moral gray zones – but also negative effects, such as those surrounding workplace surveillance. This researcher believes more research is warranted to probe the negative, or counter-productive, impact on organizations from Internet-related strategies that are explicitly designed to achieve positive outcomes, most notably increased productivity. For example, we heard respondents in this case-study investigation eerily echo the emerging fears from the human resources management and surveillance domains.

> *The Internet is an information and communication tool. If people are subject to 'Big Brother' tactics, then you are moving in the wrong direction. The criteria is not Internet use but job performance. If a civil servant is doing what is expected of him or her, then Internet use is not an issue.* (One of the comments entered at the end of the anonymous survey in this investigation)

This view supports Van Gramberg et al, 2014 who wrote:

> While not advancing a dystopian view, we argue that in many workplaces new surveillance technologies are being routinely utilised to increase employer control and that such low-trust practices are likely to be counter-productive and may undermine the profession of human resources management. (p. 2234)

Other goals of surveillance and monitoring – protecting networks from viruses, protecting organization from legal liability, and preventing theft – can still be attained through the use of ICT tools; however, perhaps the focus could be taken away from the monitoring of specific Internet use by employees, for fear of putting at risk the valuable mutual trust between managers and their staff. Interestingly and optimistically, Anteby dismisses the risk that enhanced surveillance of employees could diminish moral gray zones:

> (…) important reasons suggest that moral gray zones are here to stay. First, moral gray zones involve tacit managerial approval. Thus, it is not because employees are more highly monitored that gray zones will disappear; instead, employees are now made more aware of their supervisor's tacit approval. In other words, the give and take operating in gray zones is made more explicit. (Lagace, 2009, p.2)

On a related note, we saw the presence but mixed success and potential harm from three key levers for organizations to control the online behaviour of employees: policy and procedures in the workplace, monitoring and surveillance, and discipline and dismissal (Van Gramberg et al, 2014). However, the major finding of tacit rule violations within a moral gray zone – and its resulting positive consequences – supports the perceived limited value of monitoring as well as other practices to promote compliance that we found in this research. Therefore, if organizations persist in the three major levers, as identified by Van Gramberg (2014), then this researcher suggests more studies along the lines of Henle et al (2009) and their experiments to improve the effectiveness of Acceptable Use Policies.

As well, there may be some connection between the levers and the attitudes and behaviours of employees that warrants more attention. For example, in their 2013 study, Wang et al concluded that an acceptable use policy for the Internet is more effective for employees with high self-esteem than for those with low self-esteem, and electronic monitoring is more effective for employees who are satisfied with their job than for those who are dissatisfied with their job. The connection between job satisfaction and unauthorized Internet is definitely worthy of more research. This case-study investigation unearthed some relevant sentiments, but it did not validate the summary review of Fichtner and Strader (2014) who concluded that there was no overall correlation between job satisfaction and non-work-related computing (NWRC). They did, however, point to behavioural indications of low job satisfaction – such as lack of concern for punctuality and absenteeism – as prevalent among people who are more likely to engage in NWRC (Fichtner & Strader, 2014). Specifically, it would be interesting to see if more liberal rules on personal Internet use could promote job satisfaction.

However, maybe more fundamental research is warranted into whether it is even feasible to expect compliance amid the tidal wave of work-personal life blurring that we observed in this investigation. As König and Caner de la Guardia (2014) noted, if personal Internet use is border-crossing behaviour that is beneficial for the work-life balance of employees, then it should not be restricted by employers. This view is also supported by respondents in this investigation who pointed to the overlap between personal and workplace ICTs, supporting the conclusions of Ivarsson and Larsson (2011) who remarked that a prohibitive approach is unenforceable since more employees are using their own smartphones for personal Internet use during the workday.

As explained in previous chapters, Barker (1993) offers a fourth approach of Concertive control to build on the three original types of control – Simple, Technological, and Bureaucratic – to recognize that, in a post-bureaucratic organization no longer structured as a rule-based hierarchy, an employee works with a team of peers who are all equally responsible for managing their own work behaviors. Barker's approach focused on self-directing, self-managing teams was of limited value in this investigation in understanding employee relationships amid counter-productive behaviour. However, the successful management of the Internet usage in workplaces may give rise to a fifth, more applicable approach to organizational control. Research may be warranted into the design of a new approach that would likely require the following elements:

- be based on the individual office worker;
- recognize the blurring lines between tasks previously done at home, such as shopping or communicating with friends and family, and those conducted at work;
- acknowledge the need for access to the ICTs for employees to complete their work and personal duties; and
- provide insights to why employees chose to abide by some workplace rules and not others.

Indeed, control in the organization must become personal to update Weber's "specialists without spirit, sensualists without heart" (Barker, 1993) and to embrace "Web surfers without uniformity" as a possible way to explain an employee's uneven level of compliance with workplace rules.

But even if more effective levers for control can be developed and the blurring of work-personal life is reduced, there's a more fundamental issue: no suite of employer strategies will work if employees do not acknowledge a problem with their personal use of the

Internet at work. As we saw in this investigation, a large majority of respondents in this case study simply did not perceive they were doing *anything* wrong.

The Bottom Line

Since this thesis is the product of a student-researcher more heavily influenced by the private sector than by academe, the question must be asked: What is the practical value-add of this thesis? The answer is simply: this case-study investigation sheds some light on a relatively new but here-to-stay workplace phenomenon of personal Internet use by focusing on the situated morality created and sustained by employees and their supervisors. Specifically, in countering three decades of a predominantly negative "cyber-loafing" labels, this thesis links the theories of Gouldner, Roy, de Certeau and Anteby to shine a brightening spotlight on the positive impact of the personal use of the Internet in the office workplace through the lens of a productive moral gray zone.

And, for the "real-world" of employees and employers, the realization of the potential positive outcomes from the access to the Internet for personal use can help improve workplace policies and practices. In addition, as some respondents noted, maybe the core issue is not a potential abuse of the workplace ICT. Rather, the challenge could be the ability of a supervisor to effectively create an engaging workplace environment, so employees do not stray to find relief in an ICT as a symptom of a deficient workplace relationship, as one employee remarked in this investigation's survey:

> *I'm of the opinion that the issue is not one of 'compliance' with an organization's policy on personal Internet usage. Rather, I believe that when meaningful work is being done, in a timely manner, an employer need not concern him/herself with personal Internet usage at work.*

And, this view seems to pervade the wisest and most successful approaches to "managing human resources" in the workplace, namely, "it's not about the technology, it's the people." Indeed, further research could benefit organizations by focusing on ways to improve relationships centred on the attainment of individual work objectives, not just organizational goals. The ultimate solutions will likely be found in the interaction among colleagues in their meaningful roles and duties towards organizational goals, not in their interaction with the tools and techology.

References

Alder, G. Stoney (1998). Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives. *Journal of Business Ethics*, 17 (7), 729-743.

Alvesson, Mats & Dan Karreman (2000). Varieties of discourse: On the study of organizations through discourse analysis. *Human Relations* 2000, 53, 1125.

Alvesson, Mats (2003). Beyond Neopositivists, Romantics and Localists: A Reflexive Approach to Interviews in Organizational Research. *The Academy of Management Review* Jan. 2003, 28 (1), 13-33.

American Management Association and The ePolicy Institute. (2005) The 2005 Electronic Monitoring & Surveillance Survey. Retrieved March 10, 2007 from http://www.amanet.org/research/pdfs/EMS_summary05.pdf

Anadón, Marta & Lorraine Savoie Zajc (2009) L'analyse qualitative des données *Recherches Qualitatives,* 28(1), 1-7.

Anteby, Michel (2008). Moral Gray Zones: Side Productions, Identity, and Regulation in an Aeronautic Plant. Princeton, NJ: Princeton University Press

Askew, Kevin Landon (2012). The Relationship Between Cyberloafing and Task Performance and an Examination of the Theory of a Planned Behavior as a Model of Cyberloafing. Graduate Theses and Dissertations. Retrieved March 27, 2016 from http://scholarcommons.usf.edu/etd/3957

Balch, Dennis & Robert Armstrong (2010). Ethical Marginality: The Icarus Syndrome and Banality of Wrongdoing. *Journal of Business Ethics*, 92(2), 291-303.

Bandura, Anthony (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, 3, 193–209.

Barker, James R. (1993). Tightening the Iron Cage: Concertive Control in Self-Managing Teams. *Administrative Science Quarterly*, 38 (3), 408-437.

Beniger, James R. (1986). The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge: Harvard University Press.

Blais, Mireille et Stéphane Martineau (2006). L'analyse inductive générale : description d'une démarche visant à donner un sens à de données brutes. *Recherches Qualitatives,* 26 (2), 1-18.

Bowling, Nathan A. & Melissa L. Gruys (2010). Overlooked Issues in the conceptualization and measurement of counterproductive work behavior. *Human Resource Management Review* 20 (1) 54-61. Special issue: New Perspectives in the Study of Counterproductive Behavior in Organizations.

Brown, John Seely & Paul Duguid (1991). Organizational Learning and Communities-of-Practice: Toward a Unified View of Working, Learning, and Innovation *Organization Science*, 2 (1), 40-57. Special Issue: Organizational Learning: Papers in Honor of (and by) James G. March

Brown, William S. (2000). Ontological security, existential anxiety and workplace privacy. *Journal of Business Ethics* 23 (1) Part 1, 61.

Bucciol, Alessandro, Daniel Houser & Marco Piovesan (2013). Internet temptation at work lowers employee productivity. PHYSorg.com. 12 Feb 2013. Retrieved April 18, 2015 from http://phys.org/news/2013-02-internet-temptation-lowers-employee-productivity.html

Clegg, Stewart (1981). "Organization and Control " *Administrative Science Quarterly*, 26 (4), 545-562.

Clifford, James (1983). On Ethnographic Authority. *Representations*, No. 2 (Spring 1983) 118-146, University of California Press.

Coker, Brent L. S. (2013). Workplace Internet Leisure Browsing, *Human Performance*, 26:2, 114-125.

Cook, Mary F. (1988). What's Ahead in Human Resources? *Management Review*, 77 (4), 41.

Cowtan, Carla Jayne (2000). Electronic Monitoring in the Workplace: Tools for Social Change. Master of Arts thesis, The University of Guelph, Canada.

Czarniawska, Barbara (2001). Is it Possible to be Constructionist Consultant? *Management Learning* (32) 253-266. Sage Publications.

Dalton, Gene W., Paul R. Lawrence & Richard D. Irwin (1971). Management and Control in Organizations. Georgetown: Irwin-Dorsey.

De Certeau, Michel (1983). Les sciences sociales face à la rationalité des pratiques quotidiennes *Problèmes d'épistémologie en sciences sociales*, vol 2 Paris : Centre d'études des mouvementés sociaux.

De Certeau, Michel (1984). The Practice of Everyday Life. Translated by Steven F. Rendall. Berkeley: University of California Press.

Dilchert, Deniz S. Ones, Robert D. Davis & Cary D. Rostow (2007). Cognitive ability predicts objectively measured counterproductive work behaviors. *Journal of Applied Psychology*, 92 (3), 616-627.

Douglas, A., & Berendien Lubbe (2010). An Empirical Investigation into the Role of Personal-Related Factors on Corporate Travel Policy Compliance. *Journal of Business Ethics*, 92 (3), 451-461.

Dyck, Noel (2000). Home field advantage. In *Constructing the field: Ethnographic fieldwork in the contemporary world*. (ed.) V. Amit. Ch. 3, 32-53. London: Routledge.

Duhita, Satya & Urs Daellenbach (2015). Is Loafing at Work Necessarily Detrimental? Centre for Labour, Employment and Work, Victoria University of Wellington.

Edwards, Richard C. (1981) "The social relations of production at the point of production." In Mary Zey-Ferrell and Michael Aiken (eds.). *Complex Organizations: Critical Perspectives* 156-182. Glenview, IL: Scott, Foresman

Fichtner, J. Royce & Troy J. Strader (2014) Non-Work-Related Computing and Job Characteristics: Literature Review and Future Research Directions. *Journal of Psychological Issues in Organizational Culture*, 4 (4).

Foucault, Michel (1968). “Réponse à une question” in Michel Foucault, Dits et écrits, 1954-1988. Paris: Gallimard, 1994, 673-695.

French, Michael T., M. Christopher Roebuck & Pierre Kebreau Alexandre (March 2004). “To test or not to test: Do workplace drug testing programs discourage employee drug use?” *Social Science Research*. San Diego. 33 (1), 45.

Garrett, R. Kelly & James N. Danziger (2008) *Journal of Computer-Mediated Communication.* 13 (4), 937-958.

Giacalone, Robert A. & Mark D. Promislo (2010). Unethical and Unwell: Decrements in Well-Being and Unethical Activity at Work. *Journal of Business Ethics*, 91 (2), 275-297.

Gouldner, Alvin W. (1954) Patterns of Industrial Bureaucracy. Glencoe, Illinois: The Free Press.

Greenberg, Liane & Julian Barling (1999). Predicting employee aggression against coworkers, subordinates and supervisors: The roles of person behaviours and perceived workplace factors. *Journal of Organizational Behavior*, 20 (6), 897-913.

Hallett, Tim. & Marc J. Ventresca (2006). How institutions form: Loose coupling as mechanism in Gouldner's patterns of industrial bureaucracy. *The American Behavioral Scientist*, 49 (7), 908-924.

Haggerty, Kevin D. (2006). "Tear Down the Walls: On Demolishing the Panopticon". Chapter 2 in D. Lyon (ed) Theorizing Surveillance: The Panopticon and Beyond. Portland: Willan Publishing. 23-45.

Harvey, Pierre-Léonard, (December 3, 2008). Lecture notes from Séminaire d'intégration COM 7100, Autumn 2008, Université du Quebec à Montréal.

Human Resources and Skills Development Canada (2010). HRSDC Branches. Retrieved November, 19, 2010 from http://www.hrsdc.gc.ca:80/eng/corporate/about_us/hrsdc_branches.shtml#pasr (intranet access only within organization)

Human Resources and Skills Development Canada (2011) *Human Resources and Skills Development Canada Handbook for the Personal and Official Use of Social Media*, 2nd edition, February 2012. Included as Annex 3b.

Ivarsson, Lars, & Patrik Larsson (2011). Personal Internet usage at work: A source of recovery. Journal of Workplace Rights, 16, 63–81.

Kish-Gephart, Jennifer J., David A. Harrison & Linda K. Treviño (2010). Bad apples, bad cases, and bad barrels: Meta-analytic evidence about sources of unethical decisions at work. *Journal of Applied Psychology*, 95 (1), 1-31

Kornberger, Martin & Andrew D. Brown. (2007). 'Ethics' as a discursive resource for identity work. *Human Relations*, 60 (3), 497-518.

Knoll, Michael, Robert G. Lord, Lars-Eric Petersen & Oliver Weigelt (2016). Examining the moral grey zone: The role of moral disengagement, authenticity, and situational strength in predicting unethical managerial behavior. *Journal of Applied Social Psychology*, 46 (1), 65-78.

König, Cornelius J. & Mariette E. Caner de la Guardia (2014). Exploring the positive side of personal internet use at work: Does it help in managing the border between work and nonwork? Computers in Human Behavior 30 (2014) 355–360.

Kunda, Gabriel. (2001). Bringing work back in. *Organization Science*, 12 (1), 76-95.

Lagace, Martha (2009) What's Good about Quiet Rule-Breaking – Q&A with: Michel J. Anteby. *Harvard Business School Working Knowledge*, February 17, 2009. Retrieved March 30, 2016 from http://hbswk.hbs.edu/item/whats-good-about-quiet-rule-breaking

Leila, Canaan Messarra, Silva Karkoulian & Richard McCarthy (2011). To restrict or not to restrict personal internet usage on the job. *Education, Business and Society: Contemporary Middle Eastern Issues,* 4 (4), 253-266.

Lehman, David & Rangaraj Ramanujam (2009). Selectivity in Organizational Rule Violations. *Academy of Management Review*, 34 (4), 643-657.

Levi, Primo (1989). The drowned and the saved. London: Abacus

Liberman, Vadim (2010). Workers Behaving Badly. *Conference Board Review*, 47 (1), 12-19.

Lieberman, Seymour (1956). The effects of changes in roles on the attitudes of role occupants. *Human Relations*, 9, 385-402.

Lim, V. K. G. (2002). The IT Way of Loafing on the Job: Cyberloafing, Neutralizing and Organizational Justice. *Journal of Organizational Behavior*, 23 (5), 675.

Loch, Karen D., Sue Conger & Effy Oz (1998). Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics. *Journal of Business Ethics*, 17 (6), 653-663.

Lyon, David (ed) (2006). Theorizing Surveillance: The Panopticon and Beyond. Portland: Willan Publishing.

MacLane, Charles N. & Philip T. Walmsley. (2010) Reducing counterproductive work behavior through employee selection. *Human Resource Management Review* 20 (1) 62-72. Special issue: New Perspectives in the Study of Counterproductive Behavior in Organizations.

Martin, Andrew W. & Steven H. Lopez, Vincent J. Roscigno, and Randy Hodson (2013) Against the Rules: Synthesizing Types and Processes of Bureaucratic Rule-Breaking. *Academy of Management Review*. 2013:38 550-574

Martin, Laura, E., Meagan E. Brock, M. Ronald Buckley & David J. Ketchen, Jr. (2010). Time banditry: Examining the purloining of time in organizations. *Human Resource Management Review*, 20 (1), 26-34. Special issue: New Perspectives in the Study of Counterproductive Behavior in Organizations.

Marecek, Jeanne, Michelle Fine & Louise Kidder (1997). Working Between Worlds: Qualitative Methods and Social Psychology. *Journal of Social Issues*, 53 (4), 631-644.

May, Tim (1999). From Banana Time to Just-in-Time: Power and Resistance at Work. *Sociology*, 33, 767-783.

Mazmanian, Melissa, Joanne Yates & Wanda Orlikowski (2006). Ubiquitous Email: Individual Experiences and Organizational Consequences of Blackberry Use. Published in Proceedings of the 65th Annual Meeting of the Academy of Management, Atlanta GA: August 2006.

McAllister, Daniel. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal*, *38* (1), 24-59.

Messarra, Leila Canaan, Silva Karkoulian & Richard McCarthy (2011). To restrict or not to restrict personal internet usage on the job, *Education, Business and Society: Contemporary Middle Eastern Issues*, 4 (4), 253 - 266

Meunier, Dominique, François Lambotte et Sarah Choukah. (2013) « Du bricolage au rhizome : comment render compte de l'hétérogénéité de la pratique de recherche scientifique en sciences sociales ? », Questions de communication, 23 | 2013.

Miller, Seumas and Weckert, John (2000). Privacy, the workplace and the Internet. *Journal of Business Ethics*, 1 28 (3), 255-265.

Mischel, Walter (1977). The interaction of person and situation. In D. Magnusson & N. S. Endler (Eds.), Personality at the crossroads: Current issues in interactional psychology (pp. 333–352). Hillsdale, NJ: Lawrence Erlbaum.

Morse, Janice M. (1994). Critical Issues in Qualitative Research Methods. Beverly Hills, CA: Sage.

MyJobGroup.co.uk (2010). Social Media in the Workplace White Paper. Retrieved November, 19, 2010 from http://www.myjobgroup.co.uk/media-centre/press-releases/uks-frst-whitepaper-on-social-media-in-the-workplace-published.shtml

Namasivayam, Karthik & Lin, Ingird Y. (2005). Linking Employee Misbehavior to Consumer Satisfaction. *Journal of Foodservice Business Research*, 8 (3), 23-34.

Nord, G. Daryl, Tipton F. McCubbins, & Jeretta Horn Nord (2006). E-monitoring in the workplace: privacy, legislation, and surveillance software. *Association for Computing Machinery*. Communications of the ACM, 49 (8), 72-77.

Nouwt, Sjaak, Berend R. de Vries & Corien Prins (eds) (2005). Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy. The Hague: TMC Asser Press.

Ollier-Malaterre, Ariane, Nancy P. Rothbard, & Justin M. Berg. (2013). When Worlds Collide in Cyberspace: How Boundary Work in Online Social Networks Impacts Professional Relationships. *Academy of Management Review*, 38 (4), 645-669.

Orlikowski, Wanda J. & JoAnne Yates (2006). ICT and Organizational Change: A Commentary. *The Journal of Applied Behavioral Science*. Arlington: March 2006. 42 (1), 127-134.

Palm, Elin (2009). Privacy Expectations at Work – What is Reasonable and Why? *Ethical Theory & Moral Practice*, 12 (2), 201-215.

Panko, Raymond R. & Hazel Glenn Beh (2002). Monitoring for pornography and sexual harassment. *Association for Computing Machinery*. Communications of the ACM, 45 (1), 84-87.

Penfold, Ruth. (Dec. 1, 2002). Reviews. *The British Journal of Criminology*. 42 (1), 222

Public Affairs and Stakeholder Relations Branch (retrieved June 2016). Branch description available at Intranet site, ESDC IntraWeb (internal) http://hrsdc.prv/eng/pasrb/who_we_are/index.shtml

Public Affairs and Stakeholder Relations Branch (June 28, 2012). *Integrated Business Plan: 2012–2015*. Human Resources and Social Development Canada, Gatineau, Quebec.

Purcell, Kristen and Lee Rainie. Pew Research Center, December 2014. Technology's Impact on Workers. Available at: http://www.pewInternet.org/2014/12/30/technologys-impact-on-workers/ April 18, 2015.

"Quebec workers sanctioned for surfing too much on net." November 22, 2007. CBC News. Retrieved Nov. 26, 2007 from http://www.cbc.ca/canada/montreal/story/2007/11/22/qc-cityinternet1122.html

Ramarajan, Lakshmi & Erin Reid (2013). Shattering the Myth of Separate Worlds: Negotiating Nonwork Identities at Work. *Academy of Management Review*. October 2013 38:4621-644

Robinson, Sandra L. & Rebecca J. Bennett (1995). A typology of deviant workplace behaviors: A multi-dimensional scaling study. *Academy of Management Journal*, 38, 555-572.

Roy, Donald F. (1959). "Banana Time: Job Satisfaction and Informal Interaction." *Human Organization*, 18: 158-168.

Salvador, Rommel & Robert G. Folger (2009). Business Ethics and the Brain. *Business Ethics Quarterly*, 19 (1), 1-31.

Schwartz, Mark S. (1998). The Relationship Between Corporate Codes of Ethics and Behaviour: A Descriptive Exploration and Normative Evaluation. Ph.D. dissertation. York University, Canada.

Sloan, Ken & Joanne H. Gavin (2010). Human Resource Management: Meeting the Ethical Obligations of the Function. *Business & Society Review*, 115 (1), 57-74.

Smith, Jeff H., Ron Thompson & Charalambos Iacovou (2009). The Impact of Ethical Climate on Project Status Misreporting. *Journal of Business Ethics*, 90 (4), 577-591.

Suchman, Lucy (1987). Plans and Situated Actions: The Problem of Human-Machine Communication, Cambridge: Cambridge University Press.

Suchman, Lucy (2005). Affiliative Objects. *Organization.* 12 (3) 379-399.

Stake, Robert (2000) Qualitative Case Studies. In N. Denzin, N and Y. Lincoln. eds *SAGE Handbook of Qualitative Research*, Sage (435-455)

Tabak, Filiz & William P. Smith (2005). Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development. *Employee Responsibilities and Rights Journal*, September 2005, 17 (3).

Tannebaum, Arnold (1962). Control in Organizations, Individual Adjustment and Organizational Performance. *Administrative Science Quarterly*, September 1962.

Tennakoon, K.L. Uthpala Senarathne & Giovani J.C. da Silveira, Daphne G. Taras (2013). Drivers of context-specific ICT use across work and nonwork domains: A boundary theory perspective. *Information and Organization* 23 (2013) 107–128

Treasury Board Secretariat (2014). Management Accountability Framework. Retrieved June 2016. Available at http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/maf-crg/index-eng.asp

Treviño, Linda. K. & Gary R. Weaver, Scott J. Reynolds (2006). Behavioral ethics in organizations: A review. *Journal of management*, 32 (6), 951-990.

Umphress, Elizabeth & John B. Bingham (2011). When Employees do Bad Things for Good Reasons: Examining Unethical Pro-Organizational Behaviors. *Organization Science* 22.3 (2011): 621-40.

Valentine, Sean, Philip Varca, Lynn Godkin & Tim Barnett (2010). Positive Job Response and Ethical Job Performance. *Journal of Business Ethics*, 91 (2), 195-206.

Van Gramberg, Bernadine, Julian Teicher & Anne O'Rourke (2014). Managing electronic communications: a new challenge for human resource managers, *The International Journal of Human Resource Management*, 25:16, 2234-2252.

Van Maanen, John & Edgar H. Schein (1977). Toward a Theory of Organizational Socialization. Massachusetts Institute of Technology Alfred P. Sloan School of Management.

Van Maanen, John & Stephen R. Barley (1984). Occupational communities: Culture and control in organizations. *Research in Organizational Behavior*, Vol 6, 1984, 287-365.

Van Zolingen, Simone & Hakan Honders (2010). Metaphors and the Application of a Corporate Code of Ethics. *Journal of Business Ethics*, 92 (3), 385-400.

Vardi, Yoav (2001). The Effects of Organizational and Ethical Climates on Misconduct at Work. *Journal of Business Ethics*, 29 (4), 325-337.

Walumbwa, Fred O., David M. Mayer, Peng Wang, Hui Wang, Kristina Workman & Amanda L. Christensen (2011). Linking ethical leadership to employee performance: The roles of leader–member exchange, self-efficacy, and organizational identification. *Organizational*

Behavior & Human Decision Processes, 115 (2), 204-213.

Wang, Jijie, Jun Tian & Zhen Shen (2013). The effects and moderators of cyber-loafing controls: an empirical study of Chinese public servants. *Information Technology and Management* 14 (4).

Weatherbee, Terrance G. (2010) Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review* 20 (1) 35-44. Special issue: New Perspectives in the Study of Counterproductive Behavior in Organizations.

Weidemann, Jason (2000). Some Words on de Certeau. Retrieved April 20, 2015 from http://www.tc.umn.edu/~weide007/aboutme.html

Wolcott, Harry F. (1994). Transforming qualitative data: Description, analysis, and interpretation. Thousand Oaks: Sage.

Yin, Robert K. (1994). Case Study Research. Design and Methods, second edition. Thousand Oaks: Sage.

Yulihasri, E., T. Ramayah, Norzalila Jamaludin & Amlus Ibrahim. (2006). Use and Misuse of the Internet in the Malaysian Workplace: Preliminary Findings from an Exploratory Study.

Zyga, Lisa. (2013) Internet temptation at work lowers employee productivity. Feb 12, 2013. Retrieved April 18, 2015 from http://phys.org/news/2013-02-internet-temptation-lowers-employee-productivity.html

Annex 1: Questionnaire – Internet Usage at Work/Enquête – L'utilisation de l'Internet dans le lieu de travail

1. On a typical day, how many times do you access the Internet at work, on your employer-provided computer or smartphone?

   - For work-related purposes
     1. Not at all
     2. 1-4 times
     3. 5-9 times
     4. 10 + times

   - For personal purposes
     1. Not at all
     2. 1-4 times
     3. 5-9 times
     4. 10 + times

1. Dans une journée normale, combien de fois avez-vous accès à l'Internet au travail, sur votre fourni par l'employeur ordinateur ou un smartphone?

a. Pour les travaux liés à des fins

o Pas du tout

o 1-4 fois

o 5-9 fois

o 10 fois et +

b. Pour des fins personnelles

o Pas du tout

o 1-4 fois

o 5-9 fois

o 10 fois et +

Si vous avez répondu *Pas du tout* à la Question 1b, s'il vous plaît passez à la Question 10.

If you answered *Not at all* to Question 1b, please go to Question 10.

2. On a typical workday, when do you access the Internet for personal use? (Please check all that apply)
    - o Before starting work
    - o Anytime in the morning
    - o During morning break
    - o During lunch
    - o Anytime in the afternoon
    - o Afternoon breaks
    - o After a specific task is completed during the day
    - o At the end of the workday

2. Sur une journée de travail typique, quand pensez-vous accéder à l'Internet à des fins personnelles? (S'il vous plaît vérifiez tout ce qui s'applique)

o Avant de commencer les travaux

o Chaque fois que dans la matinée

o Pendant la pause du matin

o Pendant le déjeuner

o Chaque fois que dans l'après-midi

o Pendant la pause d'après-midi

o Après une tâche spécifique est achevée pendant la journée

o À la fin de la journée de travail

3. How do you mainly access the Internet at work for personal purposes?
    - o On my desktop computer or laptop
    - o On a smartphone, e.g. Blackberry, provided by the employer
    - o On my own smartphone/mobile device, e.g. iPhone, or tablet, e.g. iPad
    - o Other – please explain

3. Comment pouvez-vous principalement l'accès à Internet au travail à des fins personnelles?

o Sur mon ordinateur de bureau ou portable

o Sur un smartphone, e.g. Blackberry, fourni par l'employeur

o Sur mon propre smartphone/appareil mobile, e.g. iPhone, ou d'un tablet, e.g. iPad *o Autre - s'il vous plaît expliquer*

Si vous avez répondu *Sur mon propre smartphone/appareil mobile* ou *Autre*, s'il vous plaît allez à la Question 6.

If you answered *On my own smartphone/mobile device* or *Other*, please go to Question 6.

4. While at work using work-provided computers or smartphones, how much time do you spend visiting the following types of Web sites for personal purposes? (select all that apply):
    - o General news sites
    - o Social networking sites
    - o Professional networking sites
    - o Dating-related sites
    - o Sports-related sites
    - o Shopping-related sites
    - o Auction-related sites
    - o Investment-related sites
    - o Entertainment-related sites
    - o Gambling-related sites
    - o Video & file-sharing sites
    - o Web-mail sites, e.g. Gmail, Hotmail
    - o Adult-oriented (sexually explicit) Web sites

    - o Up to 10 minutes each workday
    - o 11 to 30 minutes
    - o 31 to 60 minutes
    - o 1-2 hours
    - o 2-3 hours
    - o more than 3 hours

4. Alors au travail en utilisant de travail fournis par des ordinateurs ou des téléphones intelligents, combien de temps passez-vous en visitant les types suivants de sites Web à des fins personnelles? (sélectionnez tout ce qui s'applique):

- o *Sites de presse*
- o *Sites de réseautage social*
- o *Sites de réseautage professionnels*
- o *Rencontres-sites*
- o *Sites des Sports*
- o *Shopping-sites*

- *Vente aux enchères*
- *Sites liés à l'investissement*
- *Divertissement sites*
- *Les sites liés vidéo & partage de fichiers*
- *Web-mail sites, e.g. Gmail, Hotmail*
- *Sites des adultes orientés (sexuellement explicite)*

o Jusqu'à 10 minutes chaque jour de travail

o 11 à 30 minutes

o 31 à 60 minutes

o 1-2 heures

o 2-3 heures

o plus de 3 heures

5. During the workday, using a work-provided computer, smartphone or mobile device, how often do you:
    - Read non-work related email messages, either on your work or personal email accounts?
    - Send non-work related emailed messages, either on your work or personal email accounts?

- Up to 10 minutes each workday
- 11 to 30 minutes
- 31 to 60 minutes
- 1-2 hours
- 2-3 hours
- more than 3 hours
- My personal email account is always open

5. Au cours de la journée de travail, l'aide d'un dispositif de travail fourni par l'ordinateur, smartphone ou mobile, à quelle fréquence vous devez faire:

- *Lire la non-travail des e-mails liés, que ce soit sur votre travail ou les comptes de messagerie personnels?*
- *Envoyer non liées au travail les messages envoyés par courriel, soit sur votre travail ou les comptes de messagerie personnels?*

o Jusqu'à 10 minutes chaque jour de travail

o 11 à 30 minutes

o 31 à 60 minutes

o 1-2 heures

o 2-3 heures

o plus de 3 heures

o Mon compte de messagerie personnel est toujours ouvert

6. Why do you access the Internet for personal use at work? (Please prioritize your purposes, with 4 being the most common reason, 2 a reason sometimes, and 0 never a reason)
    - o To stay in touch with friends/family
    - o To complete personal tasks, e.g. banking or travel
    - o To take a break
    - o To reduce stress
    - o To relieve boredom
    - o It's faster or cheaper than accessing the Internet at home
    - o I don't have Internet access at home
    - o Other. Please explain.

6. Pourquoi avez-vous accès à l'Internet à des fins personnelles au travail? (Veuillez prioriser vos fins, 4 étant la raison la plus commune, 2 une raison parfois, et 0 jamais une raison)

o Pour rester en contact avec des amis ou la famille

o Pour effectuer des tâches personnelles, e.g. bancaires ou de voyage

o Pour prendre une pause

o Pour réduire le stress

o Pour éviter l'ennui

o Il est plus rapide ou moins cher que l'accès à Internet à la maison

o Je n'ai pas accès à Internet à la maison

o Autre. S'il vous plaît expliquer.

7. Do you discuss your Internet usage at work with others?
    - *Yes*
    - *No*

    If Yes, with whom (select all applicable groups)

    - o Colleagues

- Manager/supervisor
- Family/friends

7. Avez-vous discuter de votre utilisation d'Internet au travail avec les autres?

• Oui

• Non

Si Oui, avec qui (sélectionner tous les groupes applicables)

- *Collègues*
- *Gestionnaire / superviseur*
- *Famille / amis*

8. Do you try to conceal your personal Internet usage at work?
   - Always
   - Never
   - Sometimes

   If "Always" or "Sometimes", why? (select all applicable reasons)

   - I don't think others will understand my reasons
   - I don't think others will understand the benefits
   - I'm embarrassed
   - I'm acting against the rules
   - I don't know
   - Other. Please explain.

8. Ne vous essayez de cacher votre utilisation personnelle d'Internet au travail?

• Toujours

• Jamais

• Parfois

Si «Toujours» ou «parfois», pourquoi? (sélectionner toutes les raisons applicables)

o Je ne pense pas que les autres comprendront mes raisons

o Je ne pense pas que d'autres prennent conscience des avantages

o Je suis gêné

o Je suis d'agir contre les règles

o Je ne sais pas

o Autre. S'il vous plaît expliquer.

9. How aware do you think your immediate supervisor is of your personal Internet usage?
    - o Completely aware
    - o Somewhat aware
    - o Not aware at all
    - o I don't know

9. Dans quelle mesure croyez-vous que votre superviseur immédiat est de votre utilisation personnelle d'Internet?

o Complètement conscient

o un peu au courant

o Pas du tout au courant

o Je ne sais pas

Si vous avez répondu Non du tout au courant, s'il vous plaît allez à la Question 11.

If you answered *Not aware at all*, please go to Question 11.

10. How do you think your immediate superior feels or would feel about personal Internet usage among employees?
    - o Approves
    - o Tolerates
    - o Doesn't care
    - o Disapproves
    - o Don't know

10. Comment pensez-vous de votre famille immédiate se sent supérieur ou se sentirait sur l'utilisation personnelle d'Internet parmi les employés?

o approuve

o Tolère

o Ne se soucie

o désapprouve

o Ne sait pas

11. How aware are you of the personal Internet usage of your colleagues?
   - o Completely aware
   - o Somewhat aware
   - o Not aware at all

11. Comment êtes-vous conscient de l'utilisation personnelle d'Internet de vos collègues?

o Complètement conscient

o Un peu au courant

o Pas du tout au courant

12. How comfortable do you/would you feel accessing the Internet for personal use at work?
   - o Completely comfortable
   - o Somewhat comfortable
   - o Not comfortable at all

Please select reasons for your response (select all that apply)

- o It makes me comfortable knowing that my personal online tasks can be completed even when I'm at work
- o It relieves work-related stress, anxiety
- o It compensates me for demands, such as unpaid overtime, by the employer
- o It's the same as chatting about non-work-related topics with colleagues face-to-face
- o It's the same as making or receiving personal phone calls
- o It's not as visible as chatting with colleagues in person or talking with family/friends on the phone
- o It's a benefit for doing a good work, such as getting my tasks done quickly
- o It makes up for the limited vacation time that I receive
- o Use of the Internet shouldn't be controlled by an organization
- o It gives me a way to retaliate against the organization's control over me
- o It is unproductive
- o It puts the organization's networks and/or computers at risk
- o It's a waste of IT resources
- o It's a form of time theft
- o It's a violation of organizational policies
- o My Internet usage is monitored by the organization
- o I don't know why I feel the way I do about my personal Internet use at work
- o Other. Please explain.

12. Comment vous sentez-vous / vous sentiriez-vous l'accès à l'Internet à des fins personnelles au travail?

o Complètement à l'aise

o Plutôt à l'aise

o Pas du tout confortable

S'il vous plaît sélectionner raisons de votre réponse (sélectionnez tout ce qui s'applique)

o Il me fait à l'aise en sachant que mes tâches personnelles en ligne peut être rempli même quand je suis au travail

o Il soulage le stress au travail, de l'anxiété

o Il me compense pour les demandes, telles que les heures supplémentaires non rémunérées, par l'employeur

o C'est la même chose que le dialogue sur la non-sujets liés au travail avec des collègues en face-à-face

o C'est la même chose que de faire ou de recevoir des appels téléphoniques personnels

o Il ne s'agit pas aussi visible que discuter avec des collègues en personne ou en parlant avec la famille / amis sur le téléphone

o C'est un avantage pour faire un bon travail, telles que l'obtention de mes tâches fait rapidement

o Il constitue pour le temps des vacances limitée que je reçois

o Utilisation de l'Internet ne devrait pas être contrôlé par une organisation

o Il me donne un moyen d'exercer des représailles contre le contrôle de l'organisation sur moi

o Il est improductif

o Il met réseaux de l'organisation et / ou des ordinateurs à risque

o C'est un gaspillage des ressources de TI

o Il s'agit d'une forme de vol de temps

o Il s'agit d'une violation des politiques organisationnelles

o Mon utilisation de l'Internet est surveillé par l'organisation

o Je ne sais pas pourquoi je me sens comme je le fais sur mon utilisation personnelle d'Internet au travail *o Autre. S'il vous plaît expliquer.*

13. When do you think your employer authorizes the use of work-supplied equipment to access the Internet for personal purposes? (Select all that apply)
    - o Once a week
    - o Once a day
    - o On breaks
    - o Before or after work hours
    - o Anytime
    - o Never

13. Quand pensez-vous de votre employeur autorise l'utilisation du travail fourni par l'équipement d'accéder à l'Internet à des fins personnelles? (Sélectionnez tout ce qui s'applique)

o Une fois par semaine

o Une fois par jour

o Sur les pauses

o Avant ou après les heures de travail

o Chaque fois que

o Jamais

Do you supervise or manage employees?

- o Yes
- o No

If No, please go to Question 16.

Ne vous supervisez ou gérer les employés?

- o Oui
- o Non

Si Non, s'il vous plaît allez à la Question 16.

14. How aware are you of the personal Internet usage of your staff?
    - o Completely aware
    - o Somewhat aware
    - o Not aware at all
    - o Does not apply

14. Comment êtes-vous conscient de l'utilisation personnelle d'Internet de votre personnel?

o Complètement conscient

o Un peu au courant

o Pas du tout au courant

o Ne s'applique pas

15. When do you tolerate infractions of rules related to personal Internet usage?
   - o Always
   - o Never
   - o Sometimes

Please select reasons for your response (select all that apply)

- o It allows my employees to feel comfortable knowing that their personal online tasks can be completed at work
- o It relieves work-related stress, anxiety among my staff
- o It compensates my staff for demands, such as unpaid overtime
- o It's the same as chatting about non-work-related topics with colleagues face-to-face
- o It's the same as making or receiving personal phone calls
- o It's a benefit for doing a good job, such as getting their work done quickly
- o It makes up for the limited vacation time that they receive
- o Use of the Internet shouldn't be controlled
- o It gives them a low-impact way to retaliate against the organization's control over them
- o I don't know
- o Other. Please explain.

15. Quand pensez-vous tolérer des infractions aux règles relatives à l'utilisation personnelle d'Internet?

o Toujours

o Jamais

o Parfois

S'il vous plaît sélectionner raisons de votre réponse (sélectionnez tout ce qui s'applique)

o Il permet à mes collaborateurs de se sentir à l'aise en sachant que leurs personnels tâches en ligne peut être rempli au travail *o Il soulage le stress au travail, de l'anxiété chez les membres de mon personnel*

o Il compense mon personnel pour les demandes, telles que les heures supplémentaires non rémunérées

o C'est la même chose que le dialogue sur la non-sujets liés au travail avec des collègues en face-à-face

o C'est la même chose que de faire ou de recevoir des appels téléphoniques personnels

o C'est un avantage pour faire un bon travail, telles que l'obtention de leur travail rapidement

o Il constitue pour le temps des vacances limitée qu'ils reçoivent

o Utilisation de l'Internet ne devrait pas être contrôlé

o Il leur donne un moyen à faible impact d'exercer des représailles contre le contrôle de l'organisation sur les

o Je ne sais pas

o Autre. S'il vous plaît expliquer.

16. How aware do you think other divisions in the organization, such as IT teams, are of daily personal Internet usage among employees?
    - o Completely aware
    - o Somewhat aware
    - o Not aware at all
    - o I don’t know

16. Dans quelle mesure croyez-vous que d'autres divisions de l'organisation, tels que les équipes informatiques, sont de l'utilisation quotidienne d'Internet personnelle parmi les employés?

o Complètement conscient

o un peu au courant

o Pas du tout au courant

o Je ne sais pas

17. How do you think personal Internet use affects productivity at work?
    - o Employees are just as productive as before
    - o Employees are less productive
    - o Employees are more productive

o I don't know

17. Comment pensez-vous l'utilisation d'Internet personnelle influe sur la productivité au travail?

o Les employés sont tout aussi productifs comme avant

o Les employés sont moins productifs

o Les employés sont plus productifs

o Je ne sais pas

18. Do you think your employer should control the personal use of the Internet at work?
    - Yes
    - No

18. Pensez-vous que votre employeur doit contrôler l'utilisation personnelle d'Internet au travail?

• Oui

• Non

19. Are you aware of any document governing the personal use of the Internet at work?
    - Yes
    - No

If Yes, which one(s)?

19. Êtes-vous conscient de tout document qui régit l'utilisation personnelle d'Internet au travail?

• Oui

• Pas de

Si Oui, lequel (s)?

20. Are you the type of person who complies with organizational rules, such as arriving and leaving on time, smoking in designated areas, respecting break periods, or parking in allocated spaces?
    - Always
    - Sometimes
    - Never

20. Etes-vous le genre de personne qui se conforme aux règles d'organisation, comme l'arrivée et au départ sur le temps, de fumer dans les zones désignées, en respectant les périodes de repos, ou de stationnement dans les espaces alloués?

o Toujours

o Parfois

o Jamais

21. Are you the type of person who complies with societal rules, such as respecting speed limits, putting the garbage out at the prescribed time, not using a phone while driving, or smoking in only designated public areas
    - Always
    - Sometimes
    - Never

21. Etes-vous le genre de personne qui se conforme aux règles de la société, comme le respect des limites de vitesse, en mettant les ordures dans les délais prescrits, ne pas utiliser un téléphone pendant la conduite, ou de fumer que dans les espaces publics

o Toujours

o Parfois

o Jamais

22. What is the best way to attain compliance with organizational policies related to Internet use?

(Please give each item a score from 1-4 in order of effectiveness, with 0 being not at all helpful, 2 somewhat helpful, and 4 being extremely helpful to foster compliance)

- Clearly written policy documents
- Training materials
- Workshops
- Speeches by managers
- Performance incentives

- Policy-compliant behaviour of managers and supervisors
- Internal control mechanisms, e.g. surveillance
- Corporate culture

22. Quel est le meilleur moyen d'atteindre la conformité avec les politiques organisationnelles liées à l'utilisation d'Internet?

(S'il vous plaît donner à chaque élément un score de 1-4 dans l'ordre de l'efficacité, 0 étant pas du tout utile, 2, un peu utile, et 4 étant extrêmement utile pour favoriser la conformité)

o les documents de politique clairement écrites

o Le matériel de formation

o Ateliers

o Discours par les gestionnaires

o incitatifs liés au rendement

o Politique de comportements fautifs des gestionnaires et des superviseurs

o Les mécanismes de contrôle interne, e.g. surveillance

o La culture d'entreprise

23. Where are you completing this survey?
    - At work
    - At home

    If you answered *At work*, are you using work-provided Internet access, such as on your cube computer or employer-provided mobile device?

    - Yes
    - No

23. Où êtes-vous remplir ce questionnaire?

o Au travail

o À la maison

Si vous avez répondu Au travail, utilisez-vous le travail fourni par l'accès à Internet, comme sur votre ordinateur cube ou fourni par l'employeur appareil mobile?

o Oui

o Non

Comments?

Commentaires?

Demographics / Démographie

Please tell me briefly about yourself.

Gender ***/ Sexe***

- Male / *Homme*
- Female / *Femme*

Age ***/ Âge***

- 20-29
- 30-39
- 40-49
- 50-59
- 60 +

Time working in the federal government

- Less than 1 year
- 2-4 years
- 5-9 years
- 10+ years

Temps de travail dans le gouvernement fédéral

o Moins de 1 an

o 2-4 ans

o 5-9 ans

o 10 ans et +

Do you work in:

- Public Affairs & Stakeholder Relations Branch
- Another HRSDC branch
- Another government department

Travaillez-vous dans:

o Affaires publiques et relations avec les intervenants

o Une autre direction-generale de RHDCC

o Un autre ministère du gouvernement

If you would like to participate in the follow-up observation or interview stages of this research study, please provide your name and a telephone number (this information will be kept separate from your responses).

Name:______________________ tel:_________________

Si vous souhaitez participer à des stades d'observation ou une entrevue de suivi de cette étude de recherche, s'il vous plaît fournir votre nom et un numéro de téléphone (cette information sera conservée séparément de vos réponses).

Nom: ______________________ *Tél:* _________________

Lastly, if you would like to receive a summary report of this research study, please provide an email address (it will be kept separate from your responses).

Email:______________________

Enfin, si vous souhaitez recevoir un rapport de synthèse de cette étude de recherche, s'il vous plaît fournir une adresse e-mail (elle sera séparée de vos réponses).

Courriel: ______________________

Thank you for your time – it is most appreciated!

Je vous remercie de votre temps - il est le plus apprécié!

Annex 2: Survey Invitation

Vous êtes invités à participer à une étude de recherche volontaire sur l'utilisation de l'Internet dans le lieu de travail.

Cette étude est menée par l'étudiant au niveau du doctorat Adrian Cloete pour l'Université de Montréal, sous la direction du Dr. Lorna Heaton, membre du corps professoral de la Faculté des communications.

Bien que Adrian est un employé de la direction des Affaires publiques et relations avec les intervenants de RHDCC, cette recherche n'est pas liée à l'accomplissement de ses tâches ou de ses responsabilités professionnel. Adrian a reçu l'autorisation de distribuer cette invitation au travail.

Si vous êtes intéressé à avoir de plus ample renseignements ou désirez à participer à cette étude, s'il vous plait visitez http://fluidsurveys.com/s/Internet/langfra où vous pouvez lire le formulaire *d'Explication et de consentement* et continuer à remplir le questionnaire en ligne. S'il vous plait, visitez le site dans les 5 prochains jours.

Merci beaucoup!

You are invited to participate in a voluntary research study on the usage of the Internet in the workplace.

This research study is conducted by a University of Montreal Ph.D. student Adrian Cloete under the direction of Communications professor Dr. Lorna Heaton.

While Adrian is an employee of HRSDC's Public Affairs and Stakeholder Relations Branch, this research is not in fulfillment of his assigned work-related tasks or responsibilities. He has received approval to distribute this invitation at work.

If you are interested in finding out more information or participating in this study, please visit http://fluidsurveys.com/s/Internet/langeng where you can read the *Explanation and Consent Form* and continue to complete an online questionnaire. Please visit the site within the next 5 days.

Thank you!

Annex 3a: Acceptable Use Policy

Page 1 of

Emploi et Développement social Canada | Employment and Social Development Canada

Canada

Maintenant et demain, l'excellence dans tout ce que nous entreprenons

Now and Tomorrow, Excellence in Everything We Do

Toutes les personnes qui utilisent ce réseau électronique doivent respecter les directives et les politiques établies par Emploi et Développement social Canada (EDSC) et le Secrétariat du Conseil du Trésor.

EDSC surveille ce réseau électronique. Des mesures administratives ou disciplinaires seront prises si l'on juge qu'une personne a utilisé le réseau d'une manière inacceptable ou irresponsable aux termes des directives et des politiques en cause.

Toutes les fonctions requises pour accéder à des renseignements électroniques, et pour stocker et transmettre de tels renseignements (p. ex. courriel, intranet, Internet, lecteurs réseau) font partie du réseau électronique d'EDSC.

Les diverses composantes d'équipement et différents dispositifs pouvant être connectés au réseau électronique (p. ex. ordinateurs de bureau et portatifs, téléphones, tablettes électroniques, imprimantes, télécopieurs, numériseurs, appareils BlackBerry) font également partie de ce dernier.

Les dispositifs personnels ne sont pas autorisés sur le réseau, à moins qu'une autorisation soit accordée, dans des circonstances exceptionnelles, conformément à ce qui est énoncé dans la Directive sur les dispositifs de stockage portatifs.

Les personnes qui utilisent le réseau électronique doivent connaître la directive d'EDSC sur l'utilisation du réseau ainsi que les autres directives et politiques pertinentes figurant sur le site iService.

All individuals using this electronic network must do so in keeping with the directives and policies set out by Employment and Social Development Canada (ESDC) and Treasury Board Secretariat (TBS).

ESDC monitors this electronic network. Administrative and/or disciplinary measures will be taken should an individual be deemed to have used it in a way that that is unacceptable or irresponsible in accordance with these directives and policies.

The ESDC electronic network includes all means to access, store or transmit electronic information (e.g. email, intranet, internet, network drives).

The electronic network further extends to any equipment/device that may be connected to it (e.g. desktop/laptop computers, telephones, tablets, printers, faxes, scanners and, BlackBerrys).

Personal devices are not permitted on the network, unless permission is granted under exceptional circumstances as defined in the Portable Storage Devices Directive.

Individuals using the electronic network are to be familiar with ESDC's Network Use Directive as well as other related directives and policies on iService.

J'ACCEPTE LES CONDITIONS / I AGREE TO THESE TERMS

Annex 3b: Departmental Social Media Handbook

Ressources humaines et Développement des compétences Canada
Human Resources and Skills Development Canada

Maintenant et demain
L'excellence dans tout ce que nous entreprenons

Now and Tomorrow
Excellence in Everything We Do

Human Resources and Skills Development Canada Handbook for the Personal and Official Use of Social Media

February 2012, 2nd Edition

Canada

Contributors	
Corporate Web	Access to Information and Privacy
Integrity Services Branch	Information Management
Labour Relations	Contracting and Purchasing
Official Languages	Legal Services
Common Look and Feel Centre of Expertise/e-Accessibility	Intellectual Property
Innovation, Information and Technology Branch	Publishing and Multimedia
IT Security Centre of Excellence	TBS and PWGSC

Table of Contents

includes Frequently Asked Questions (FAQs) to help employees and managers meet their legislative and policy obligations.

In addition to this handbook, you can find social media information, such as Web governance and best practices, on the Knowledge Portal, SharePoint and GCPedia.

Lastly, this handbook provides guidelines on how to properly use the access and services that employees currently enjoy. It does not provide approval to open or create new online services.

If you notice issues not addressed by this handbook, neither its links to policies nor its supplemental resources, please contact the Corporate Web's social media team. As well, feel free to send your ideas for additional issues that should be addressed in this handbook.

2. Key Contacts for Policy Guidance and Advice

- For Web issues, contact Corporate Web.
- For general social media questions, contact the Corporate Web's social media team.
- For *Values and Ethics Code for the Public Service*, Public Servant's Duty of Loyalty, and HRSDC Code of Conduct, contact the Office of Values and Ethics.
- For questions on Official Languages, contact your regional Official Languages consultant.
- For Accessibility, contact the CLF Centre of Expertise/e-Accessibility.
- For IT Security, contact IT Security Centre of Excellence.
- For questions about complying with privacy, access to information and other legislative requirements, contact our department's Access to Information and Privacy (ATIP) team at 819-994-0416.
- For Information Management, contact the National Service Desk.
- For Procurement, contact the contracting and purchasing team.
  - For questions on Intellectual property, contact Legal Services, Marcus Dirnberger.
- For questions on Publishing and Multimedia related to:
  - Publishing, contact Anne Latreille;
  - Video, contact Susan Stranks;
  - Distribution, contact publications@hrsdc-rhdcc.gc.ca; and
  - Graphic design, contact graphics.hrsdc-rhdcc@hrsdc-rhdcc.gc.ca.

3. Personal Use of Social Media

Personal use, defined as using social media for purposes unrelated to work—at home or at work—on- or off-duty (that is, during or after the workday), is guided by:

- Values and Ethics Code for the Public Service;
- Public Servant's Duty of Loyalty;
- HRSDC Code of Conduct (expected early 2012);
- Values and Ethics Code for the Public Sector (expected early 2012); and
- HRSDC Policy on the Use of the Electronic Network.

At **all times** when using social media for personal use—to minimize the risks previously outlined—public servants must:

- ensure Public Service political neutrality and impartiality;
- respect their Duty of Loyalty;
- refrain from public criticism of the Government of Canada, HRSDC or its policies;
- avoid statements that would appear to impair their ability to perform official duties;
- respect confidentiality and privacy;
- avoid causing harm to HRSDC, its reputation and programs;
- respect the Values and Ethics Code for the Public Sector (expected early 2012);
- respect the HRSDC Code of Conduct (expected early 2012); and, if applicable,
    - respect the Guidelines of Conduct for Service Canada; and/or
    - respect the Guidelines of Professional Conduct for the Labour Program.

In addition, when public servants use social media for personal purposes while **on duty** (that is, during the workday):

- It must be confined to breaks, lunch and immediately before or immediately after the employee's work day as per HRSDC Policy on the Use of the Electronic Network.

- They should not identify themselves as public servants, including through the use of departmental email addresses.

And, when public servants use social media for personal purposes while **off duty** (that is, unconnected to work):

- It must not be done using the Department's resources or equipment.
- They should neither identify themselves as public servants nor use their departmental email addresses.

If you have not been given responsibility to be a departmental spokesperson, then you are not authorized to identify yourself as a departmental employee and speak for the department in any forum—online or in person.

For additional guidance, contact the Integrity Services Branch (see Section 2).

4. Frequently Asked Questions for Personal Use

Question: Am I allowed to visit social media sites for private purposes, while at work?

Answer: Yes. The HRSDC Policy on the Use of the Electronic Network allows employees to use departmental computer networks for personal purposes provided that this activity:

- is on personal time, i.e. breaks, lunch, the time before and after work;
- is not for financial gain;
- does not add to costs; and
- does not interfere with the conduct of business.

For the list of specific Unacceptable and Unlawful Conduct and Activities, please see the Policy.

Note: HRSDC's electronic network is monitored to protect government resources and ensure compliance with the Policy. All traffic originating or terminating in the network is recorded.

Question: ***Whether using social media for personal purposes at work or at home, is there any guidance that I should follow?***

Answer: Yes, you should:

- uphold the public service Duty of Loyalty, and refrain from public criticism of the Government of Canada, HRSDC or its policies;

- uphold the political neutrality and impartiality of the federal public service;
- respect confidentiality and privacy;
- not identify yourself as a public servant, including through the use of departmental email addresses;

Please read and follow the tips outlined in the Seven Security Tips for Social Networking.

And, please see the *Values and Ethics Code for the Public Service* and the HRSDC Code of Conduct.

Question: How much can I disclose about my job in my personal conversations in social media?

Answer: You shouldn't identify yourself as an HRSDC employee when using social media for personal purposes. For example, don't sign personal messages with your title and don't list your current employer as part of your personal profile if you are using social media for personal purposes. Above all, don't give the impression that you are speaking on behalf of the Department.

Question: As a public servant, can I agree to the terms of use of third-party sites?

Answer: Yes, but only for your personal use. You should neither identify yourself as a public servant, nor use your departmental email address for personal use.

For official use of social media, public servants should not agree to terms of use on behalf of the Department.

5. Official Use of Social Media

Business Value

Official use is defined as using social media for internal and public-facing initiatives in support of:

- departmental business, e.g. communication, employee engagement; and
- individual purposes, i.e. employee participation for business purposes.

Official use includes **internal** initiatives for workplace collaboration, employee engagement, research, and networking on internal platforms, such as the Knowledge Portal, SharePoint, GCPedia, GCconnex, and GCForums.

It also includes **public-facing** initiatives, such as communications, outreach, engagement, service delivery, research and networking on third-party platforms such as Twitter, YouTube and Facebook.

Laws, Policies and Guidelines

Official use is guided by:

- *Official Languages Act*
- *Privacy Act*

The Department of Human Resources and Skills Development Act and The Department of Social Development Act contain Privacy Codes which include offence provisions applicable to the improper collection, use and disclosure of personal information.

Treasury Board Secretariat (TBS)

- *Values and Ethics Code for the Public Service*
- *Values and Ethics Code for the Public Sector (expected in 2012)*
- *Guideline for External Use of Web 2.0*
- *Policy on the Use of Official Languages for Communications with and Services to the Public*
- *Policy on Language of Work*

- *Directive on the Use of Official Languages in Electronic Communications*
- *Directive on the Use of Official Languages on Web Sites*
- *Guideline to Acceptable Use of Internal Wikis and Blogs Within the Government of Canada*
- *Policy on the Duty to Accommodate Persons with Disabilities in the Federal Public Service*
- *Web Standards for the Government of Canada*
- *Government of Canada Procurement practices*
- *Intellectual property*
- *Information Management*

Human Resources and Skills Development Canada

- *Policy on the Use of the Electronic Network*
- *Policy on Departmental IT Security Management*
- *Code of Conduct (expected early 2012)*
- *Guidelines of Conduct for Service Canada*
- *Guidelines of Professional Conduct for the Labour Program*
- *Best practices and protocols*

At all times, official use of social media must:

- respect the HRSDC Code of Conduct, *Values and Ethics Code for the Public Service* and Duty of Loyalty;
- respect all policy and legislative requirements, as appropriate and listed above; and
- follow and/or create protocols on the development and use of social media initiatives (see next section).

In addition, all official **public-facing** initiatives **must** be approved by HRSDC management through regular Communications planning and Web governance channels.

Official internal initiatives must seek approvals for major initiatives with business plans reviewed by Web governance committees.

For additional guidance, see the Frequently Asked Questions section or contact the Corporate Web team or the appropriate policy centre (see Section 2).

Protocols

Official social media initiatives should be approached as follows:

1. **Manage the initiative formally and methodically:**
   - Develop a formal proposal with IITB, your communications advisor (public-facing initiatives only), Citizen Service Branch, your branch Web team, and other stakeholders.
   - Identify resources, e.g. technical, staffing.
   - Use and develop protocols and best practices, e.g. the portfolio Commenting and Service Standards on the HRSDC Web site and featuring guidance on moderation and hyperlinks.
   - Follow approval process, e.g. Web governance, Minister's Office.

   In addition, all public-facing HRSDC initiatives should:
   - be part of an approved communications strategy;
   - have clear and strong program business drivers;
   - target an audience already using social media;
   - deliver simple messaging;
   - be led by teams able to sustain the engagement;
   - include measurement and evaluation components; and
   - ensure Government of Canada and departmental policy and guideline compliance (e.g. Official Languages, Accessibility, Access to Information & Privacy, Common Look and Feel, Information Management, IT Security, Intellectual Property).

2. **Follow a principled approach to engage your colleagues and the public, respecting the Values and Ethics Code for the Public Sector:**

   Respect for Democracy
   - Avoid giving the perception of advocating or criticizing the Government of Canada and its policies.

- Respect the public service tradition of political neutrality and impartiality.
- Do not commit the Department to a course of action unless you have the authority to do so.

Respect for People
- Maintain a professional and respectful tone.
- Be courteous and constructive.
- Be accurate, complete, and relevant.
- Avoid aggressive or provocative comments.

Integrity
- Staff should disclose their official position/job title.
- Avoid appearance of advocating private interests.
- Avoid statements that could harm the reputation of HRSDC or the Government of Canada.

Stewardship
- Work within the laws of Canada.
- Meet all policy and legislative requirements.
- Do not disclose confidential or personal information.
- Be aware of potential security risks.

3. Create protocols for your specific needs and objectives.

- **Establish Rules of Engagement, Expectations and Monitoring** that will foster a spirit of collaboration and seize the potential of online communities of interest.
- **Seek Levels of Approvals** for public-facing social media and Web 2.0 initiatives according to your departmental head of Communications.

For additional guidance, see the Frequently Asked Questions or contact the Corporate Web team.

6. Frequently Asked Questions for Official Use

Official Languages

Question: What are my core obligations with respect to the *Official Languages Act* for both public and internal communications?

Answer: Members of the public have the right to communicate with and receive services from the Government of Canada in either English or French. When a third party is providing services to, or communicating with the public on its behalf, our Department must strive to ensure that the public's language rights are respected.

When social media are used for professional purposes as part of external initiatives, it is essential that our public obligations be respected. Members of the public have the right to communicate with the Government of Canada in English or French and to obtain services in one of those two languages. If a third party offers services to or communicates with the public on the government's behalf, the Department must ensure that the linguistic rights of the public are respected.

Question: Is there an obligation to provide all information in both official languages when using social media for official use on an external site, such as YouTube or Twitter?

Answer: Yes. Content should be posted simultaneously in both official languages on their respective accounts, channels and pages. When commenting is enabled, users should be encouraged to respond in the official language of their choice.

Responses to comments, video responses or questions should be answered in the official language of origin. When summaries are provided, they should be posted in both official languages simultaneously and be of equal quality.

Lastly, users should be made aware that some links on a third-party site will direct users to sites of organizations or other entities that are not subject to the OLA and that these sources are only available in the language in which they are written.

Question: What else can we do to meet our OLA obligations when using third-party sites?

Answer: HRSDC should not use unilingual platforms. In addition, make sure the location of the channel in the other official language is clearly displayed. As well, many third-party social media services have multiple language options for their interface. So, direct your audience to instructions on how to satisfy their preferences for the interface of the platform.

Question: What are the obligations related to these collaborative tools intended for employees located in regions designated as bilingual or unilingual for language-of-work purposes?

Answer: Social media tools (e.g. SharePoint, wikis, blogs) are considered regularly and widely used work instruments and part of work environments.

In regions designated bilingual for language-of-work purposes, the Department (manager) has a responsibility to create and maintain a workplace conducive to the effective use of both official languages by enabling its staff to use either language. See the *Policy on Language of Work* of the *Official Languages Act*.

Regions designated as bilingual for language-of-work purposes are specific geographic areas where both English and French are considered languages of work in the offices. The designated regions include the National Capital Region; parts of Northern and Eastern Ontario; the Montreal area; parts of the Eastern Townships, the Gaspé and West Quebec; and New Brunswick. A detailed list of the bilingual regions for Language-of-Work purposes is available at the following Web site.

In unilingual regions for language-of-work purposes, the language of work will be that which predominates: French in Quebec and English elsewhere.

Regions designated as unilingual for language-of-work purposes identify geographic areas other than bilingual regions for language of work purposes where Departmental offices are located.

Question: What are the requirements and exceptions related to the collaborative tools?

Answer:
In regions designated bilingual for language-of-work purposes, SharePoint, blogs and wikis are considered bilingual work instruments.

The Department would need to provide interfaces in both official languages and permit any user to choose their preferred official language to be compliant with official languages requirements.

Users are encouraged to add information in the official language of their choice.

All official best practices pages, navigation, and official departmental positions are available in both official languages simultaneously and are of equal quality.

The department posts a notice indicating the terms of reference regarding the use of both official languages.

In certain circumstances, they may be in one official language:

1. When used in regions designated as unilingual for language-of-work purposes. The language of use is the language that predominates in that region. The language would then be French in Quebec and English anywhere else in Canada. A notice must be posted to explain that the site is restricted to a unilingual region.

2. If it is restricted to a small group of employees working in one or more regions designated bilingual for language-of-work purposes and they have all individually identified in an objective manner a preference for the same official language. A notice must be posted to explain that the site is restricted to a specific group.
   a. Documents produced by the employees who use the site are subject to all relevant official languages obligations if they are disseminated off the site.
   b. The circumstances set out above do not exempt the department from its obligation to communicate with employees in both official languages.

Question: What are their specifics?

Answer:

For bilingual blogs:

- Users can respond to any post, or any reply to any post, in the official language of their choice.
- The department ensures that its response to a post is in the official language in which the post was received.
- The department advises users that the responses or replies displayed are in the language in which they were received.
- If the department decides to provide summaries of the blog, it ensures that the summaries are posted in both official languages simultaneously and are of equal quality.

For bilingual wikis and pages in development:

- The department can decide to make them available in either one or both official languages.
- When users are asked to edit pages, they can do so in their preferred official language.
- Once the content is finalized and approved, it is bilingual, or a link to the final document where there are English and French versions is provided. Both versions are posted simultaneously and are of equal quality. The appropriate links are established between the English and French versions. The department ensures that the document is posted in both official languages.
- When the content does not reach a final version but changes continually, the department determines at which point the content should be made available in both official languages.

For Discussion pages:

- Discussion pages are made available in both official languages.
- Users contribute in their preferred official language.
- If the department decides to provide summaries, the summaries are posted in both official languages simultaneously and are of equal quality.

Accessibility

Question: How can I make third-party sites accessible to people with disabilities?

Answer: Third-party social media service providers are not bound by Government of Canada Web accessibility practices; however, HRSDC must guarantee access to the same information for visitors with disabilities.

Contact the Corporate Web team, Accessibility Centre for Excellence or IITB's e-Accessibility team for ways to help enhance the accessibility of your initiatives.

Question: What about internal sites? Is there anything I can do to make them accessible?

Answer: The *Policy on the Duty to Accommodate Persons with Disabilities in the Federal Public Service* enables an inclusive, barrier-free environment in the federal Public Service to ensure the full participation of persons with disabilities.

Key accessibility features include the use of XHTML, scalable fonts, cascading style sheets, and text indicating the format and size of uploaded documents. Screen reader support can be provided by using text equivalents for non-textual elements (such as images) with <ALT> tags and by avoiding the use of colour alone to convey special information.

Question: What about making social media tools accessible on the Department's Web sites?

Answer: All departmental sites must meet the *Web Standards for the Government of Canada*. In practical terms, this means ensuring a WCAG 2.0 AA level of accessibility.

Contact the Corporate Web team, Accessibility Centre for Excellence or IITB's e-Accessibility team for ways to help enhance the accessibility of your initiatives.

Privacy and Access to Information

In instances where there is a collection of personal information as part of a social media activity:

- the legislative authority to collect, retain, use disclose or dispose of personal information must be established; and
- privacy notice statements must be posted to inform Web site visitors of their privacy rights.

  Failure to do so may result in HRSDC being non-compliant with the *Privacy Act* as well as departmental legislation.

Care should be taken when posting images or videos on Web sites. Metadata embedded in the image or items appearing in the picture or video may unintentionally result in the disclosure of personal information. This may result in the improper disclosure of personal information and, thus, be non-compliant with the Privacy Act and departmental legislation.

The *Department of Human Resources and Skills Development Act* and the *Department of Social Development Act* include offence provisions applicable to the improper collection, use and disclosure of personal information.

Question: Isn't everything in social media in the public domain, so I don't have to worry about privacy, right?

Answer: No. Privacy considerations **must** always be paramount in all activities carried out by HRSDC that involve the collection, use and disclosure of personal information.

Section 4 of the *Privacy Act* states that, "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."

This has been interpreted to mean that an institution must have parliamentary authority in an act or regulation, or authority provided by Order-in-Council, for the program or activity they will administer through social media.

Question: Is any privacy training required prior to engaging in social media?

> **Answer:** Yes. Departmental employees who are assigned to add comments or to monitor comments posted on the sites must receive privacy training. Contact our Department's Access to Information and Privacy (ATIP) team for more information.

Question: Do we have to post a privacy notice to followers when using social media?

> **Answer:** Certain initiatives may require a Privacy Notice. A review by our Department's ATIP team will determine if a specific initiative requires one.

Question: Does Access to Information apply to information on third-party sites, such as YouTube, Twitter and Facebook?

> **Answer:** Yes. Requests made under the *Access to Information Act* and the *Privacy Act* related to information posted on our social media sites are subject to the *Access to Information Act*, *Privacy Act*, HRSDC Privacy Codes, and must be responded to by the Department. In some cases, informal responses may be made.
>
> For questions about compliance with these acts, please contact our Department's ATIP Coordinator, Jackie Holden, at 819-994-0416 or jackie.holden@hrsdc-rhdsc.gc.ca.

Interacting with the public

Question: Are there rules or guidelines about how we should interact with the public?

> **Answer:** Yes. A common set of Commenting and Service Standards has been developed by HRSDC, Service Canada and Working in Canada social media teams. They are featured on the HRSDC Web site.
>
> These standards also provide guidance on "friending" and following others in social media channels.

Question: Are there rules of engagement for employees to follow on internal blogs and forums?

Answer: Yes. A set of rules and standards is used for the Deputy Ministers' and Service Excellence blog sites. They can be adapted for other internal venues. As well, see the Guideline to Acceptable Use of Internal Wikis and Blogs Within the Government of Canada.

Information Management

Question: Are existing Information Management policies applicable to content placed on third-party sites?

Answer: Yes. In social media initiatives, like any other departmental activity, we must manage the information used, acquired, or processed in the course of the activity.

For more information, the Information Management Life Cycle outlines seven steps to manage information throughout the entire initiative.

Question: What about Information Management stewardship on internal blogs and wikis?

According to the Guideline to Acceptable Use of Internal Wikis and Blogs Within the Government of Canada, "blogs and wikis do not have records management retention and disposition specifications. Page (article or document) ownership can become unclear when several people on a wiki make changes to the content of a page. For most business purposes, documents (or pages) must come to official or final stages, possibly for formal or more extensive consultation or to be used as an authoritative version.

It is recommended that the content author take responsibility for the retention and disposition decisions and processes: this may be as simple as moving finished content to another document form and maintaining the official record in a records management repository [...]".

For additional information, see the *Policy on Information Management*.

Intellectual Property

Question: Isn't everything in social media in the public domain, so I don't have to worry about intellectual property, right?

Answer: No. The Department must ensure it owns the sole and full rights to, or has secured appropriate licensing agreements to use any content or media it will share over the Internet and possibly that will be shared by others.

Without these rights, it would be an infringement of the moral and perhaps legal copyright of the artist responsible for the production of the media, whether video, audio, artwork, graphics or photography.

For example, if a departmental video includes anything that was not originally created by the Department, you will need to clear the rights to use that material. Even material created in-house may require clearing rights in certain circumstances. This material can include such elements as, but not limited to:

- video footage used in a clip;
- artwork and other objects that appear in the footage (e.g. if an interview is shot in front of a painting which is under copyright);
- photographs, drawings, graphics and other still or animated material; or
- music and sound effects.

In addition, talent rights must be checked to ensure that all fees are covered for paid talent (with the Alliance of Canadian Cinema, Television and Radio Artists) and that the agreement states re-use on multiple platforms, with specific mention of channels, such as YouTube.

Lastly, model release forms must be signed and kept on file for all recognizable individuals in videos commissioned by the Department. Public servants must also sign release forms.

IT Security

Question: Is an official IT threat and risk assessment needed before employees can access social media sites?

Answer: No. Security and Identity Management of the Chief Information Officer Branch issued security considerations when allowing connections to public social networking sites in TBS' April 2010 Security Policy Implementation Notice (SPIN) document: "From an IT Security stand point, connections to social networking sites are not substantially different than other connections to the Internet and will not normally require a new Threat and Risk assessment by each department."

The SPIN document also advises departments to meet the requirements of Management of Information Technology Security (MITS), with particular attention to section 16.4.6 on Network Security and Perimeter Defence.

For questions on MITS compliance, please contact the IT Security Centre of Excellence. Also, when accessing any social media sites, please follow the guidelines outlined in the article Seven Security Tips for Social Networking.

Question: Do I need to worry about passwords for managing third-party social media sites?

Answer: Yes. Creating strong passwords for all your online accounts (at work and at home) is a **must**! It is one of the first lines of defence for any IT system, service, and for maintaining the security of our network.

Precise protocols must be established for managing passwords. Protocols should include provisions such as:

- passwords should be changed on a regular basis, such as every 60 days;
- they should only be known to a few people;
- they should be changed immediately when someone leaves the team; and
- they should never be the same as a person's personal password.

A compromised password is the best way to embarrass the Department. Each of us is responsible to protect government information, so please always follow these simple password best practices.

Question: What do I do if one of our channels or accounts is compromised or hijacked?

Answer: If this is suspected, stop using the channel or account and report the incident to National Service Desk for investigation.

Question: Do I need to worry about downloading content from the third-party social media sites that we use?

Yes. HRSDC employees are not allowed to download third party applications to their desktops. Please refer to the HRSDC Policy on the Use of the Electronic Network for more detailed information.

Question: How can I learn more about IT security?

Answer: The Innovation, Information and Technology Branch has developed an IT Security Awareness Program and a mandatory IT Security Awareness Training course for all HRSDC employees. The purpose of the ongoing awareness program is to ensure that all staff understand IT security. For further information on the IT Security Awareness Program, visit the IT Security intranet site.

Purchasing Decisions

Question: As a public servant, can I agree to the terms of use of third-party sites?

Answer: For official use of social media, public servants should not agree to terms of use on behalf of the Department. The Government of Canada has signed terms of service agreements with Twitter and YouTube. Proposals to PCO and PWGSC are now required for all federal government departments and agencies to become part of these agreements and ensure a consistent approach across and within all departments.

For other official use of social media, public servants should not agree to terms of use on behalf of the Department. Contact the Corporate Web's social media team for more information.

Question: Should I go consider procurement issues when using a "free" social media site?

Answer: Yes, you should seek guidance to understand the implications of the various options, such as no-cost, open-source, and contracted services. Some involve government-signed terms and conditions, depending on the specific internal or public-facing social media channel or Web 2.0 tool.

Annex 3c: Federal Government Employee Guidelines

Guideline for External Use of Web 2.0 for public servants in the Canadian federal government

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24835

The publication date of this guideline is November 18th, 2011.