LAURA RODRIGUEZ

Principles that Should Govern the Right of Employers to Monitor Employee's Computer Mediated Workplace Communication: Private Sector.

LLM RESEARCH PAPER

LAWS 582: MASTERS LEGAL WRITING

FACULTY OF LAW

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA
UNIVERSITY OF WELLINGTON

2016

Contents (References - table of contents)

3. Principles that Should Govern the Right of Employers to Monitor Employee's Computer Mediated Workplace Communication: Private Sector.

4. Principles that Should Govern the Right of Employers to Monitor Employee's Computer Mediated Workplace Communication: Private Sector.

Abstract

This paper explores the issues that arise from the surveillance of digital communications at the workplace and how New Zealand has addressed these issues. To achieve that purpose, this paper explores the two prevalent approaches to privacy rights at the workplace: The ownership of the resources (Anglo-American) and the continental Dignity-based (Europe). New Zealand has aligned itself with the Anglo American approach. This approach is less protective of employee's privacy interests. This paper shall demonstrate that the legal protection of employees from electronic monitoring would be greatly improved by deriving those protections from "human dignity".

Word length

12141 words excluding footnotes, tables, graphics and abstract.

Subjects and Topics

Electronic Surveillance at the workplace
Privacy Act 1993
Surveillance of email and Internet at the workplace.
Dignity and the link with privacy rights at the Workplace

"*Laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths disclosed, and manners and opinions change with the change of circumstances, institutions must advance also, and keep pace with the times." Thomas Jefferson 1986.*

I Introduction

In the business world employers seem to invest significant resources in efforts to monitor how their employees use workplace technology (e.g. email, internet, workplace devices) for communication purposes. Their reasons for doing so can range from assessing an employee's productivity to ensuring that the employer is not exposed to potential liability for an employee's actions. Although issues that arise from surveillance schemes in the workplace have been widely discussed, especially in employment law matters, the rise of surveillance technology and its penetration into the workplace has created new concerns and has exacerbated existing ones.

The power bargaining gap is one of the issues that has always existed in the employment relationship, but it has been worsened by the rise of technology. Larry Natt Grantt wrote that "new monitoring technologies have intensified employer privacy concerns because the instruments abolish the desirable balance of power between employers and employees"[1]. Privacy concerns have also arisen from electronic monitoring of employee's digital communications. Technology (e.g. keystroke software) can be highly invasive because it may "allow employers to get an insight into employee's personal life by facilitating to employers to manipulate, access, and collect information about employees in greater amounts"[2]. Additionally, sociological studies have shown electronic surveillance has a strong impact in employees well-being. For example, "empirical study demonstrates that workers who were electronically monitored manifested higher rates of depression, anxiety, and fatigue than others in the same business that were not monitored"[3].

---

[1] Larry O Gantt "Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace" (1994) 8 (2) Harv. JL & Tech 345 at 346.

[2] At 346.

[3] Michael L Rustad and Sandra R Paulsson "Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe" (2005) 7 U Pa J Int'l Bus L 1 at 18 Retrievable from <http://ssrn.com/abstract=935098> .

Legal systems around the world have addressed issues that arose from the surveillance of employee's *Computer Mediated Workplace Communications* (CMWC)[4] in different way. The Anglo-American jurisdictions for example, have developed the "property-rights approach" that "holds that since employers own the work tools, they can initiate surveillance at will"[5]. Thus "employees have no reasonable expectation of privacy when using company E-mail/Internet facilities"[6]. In contrast, continental Europe "employ the notion of human dignity in determining the outcome of workplace monitoring issues."[7] The outcome of this difference is that employees' privacy interests are less protected in the Anglo-American jurisdictions than in their European counterpart[8].

New Zealand's approach is aligned with the Anglo American view that gives predominance to the employer's ownership of the network infrastructure over an employee's privacy rights. Paul Roth analyzes that the "privacy interests of employees normally must take a back seat to the above matters because of overriding practical, contractual, and statutory obligations"[9]. In other words, in New Zealand employers' ownership of the network infrastructure overrules the expectation of an employee to privacy. The result is that infringements are reduced to a contractual matter. Therefore, so far, legal sources have failed to recognize that by offering some protection to employee's privacy interests when using CMWC, an employee's human dignity is ultimately afforded greater protection.

---

[4] According to Snyder are all the forms of electronic text- based tools to send and receive messages in organizations. Rebecca M. Chorry established, that among other, this concept includes the use of Email, social networking sites and Instant messages: *See* Jason Snyder "E-mail privacy at the workplace:A Boundary Regulation Perspective" (2010) 47JBC 266; Rebecca M Chory and Others "Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses" (2015) 28(1) E.R. & R.J. 23 at 24.

[5] Rustad and Paulsson, above n 3, at 10.

[6] At 10.

[7] Temp. Envtl. L. & Tech. J. 73 Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers By Peter J. Isajiw1146

[8] See Temp. Envtl. L. & Tech. J. 73 Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers By Peter J. Isajiw1146

[9] Crawford, Aaron, Raymond Harbridge, and Pat Walsh. "Privacy in the Workplace: The Effects of the Privacy Act 1993 on Employment Practices in New Zealand." Labour & Industry: a journal of the social and economic relations of work 6.3 (1995): 51-72.

Having considered the above, this paper proposes shifting the New Zealand Legal approach towards one that is based on the link between employee's privacy rights and Human Dignity and which is more protective of the employees privacy interests. This paper is organised into four main sections. The first section explores important social factors that should have been taken into account when law makers addressed the issue of employee's privacy and surveillance at the workplace. The second section studies two approaches to the issue of electronic surveillance at work (Anglo-American and European) by exibiting the main features of each tradition. The third section explores New Zealand's legal approach and concludes that the fundamentals of the current framework are aligned with the Anglo American approach of the employer's ownership of the technology. The fourth section recommends a change of the philosophical fundaments of the legal framework in order to embed employee's human dignity as a value of upmost importance. This paper proposes a legal solution that balances an employer's right to achieve their economic objectives with an employee's human dignity.

II Background

When addressing the legal protection of employees from abusive electronic monitoring, legal sources must to establish first which legal interests they are safeguarding. This is only possible by exploring the real circumstances that employees as human beings (thus sentient beings) face when they are under constant surveillance at the workplace. In other words law makers should questioned first, what is the impact of electronic surveillance in employees' personae (e.g. emotional, physical, and interpersonal among others)? Sociological theories are an adequate mechanism to achieve a better understanding of the above, from a more real and humane perspective.

Another reason to incorporate the sociological perspective into the research, is the ideological foundation of this paper on the school of legal realism[10] and the theory of responsive law[11] . Philippe Nonet, said that a responsive law "perceives social pressures as

[10] One of the examples of legal realism is given by Noel Cox when he states "Constitutions are at the mercy of technology as much as society and perhaps even more": Noel Cox *Technology and Legal Systems*(Ashgate Publishing, Ltd., Hampshire,2006) at 119

[11] *See* Phillippe Nonet, Philip Selznick *Law and Society in Transition: Toward Responsive Law* (2d ed, Transaction Publishers, New Jersey ,2009)

sources of knowledge and opportunities for self-correction."[12] In the same line of thinking, Bryan Tamahana said that "much legal development occurs not through new legislative enactments but through jurists' gradual addition of new content—taken from social sources—through the creation of new legal propositions.[13]

The sociological influences that should impact the design of legal frameworks in matters of electronic surveillance at workplace are explained by five main theories: Panopticon effect, Communication Privacy Management, Theory of non-clinical paranoia, the Boundary permeability theory and the Generation Gap theory. These theories give a better conceptual understanding of social dynamics at the workplace. On the following there is a table that connects the social facts with the theory that explains it:

Table 1: Relation between sociological theories and social phenomenon that arise from Electronic surveillance the workplace.

Theory	*Social phenomenon at the workplace*
Panopticon effect.	How surveillance increases the power bargain gap between employee and employer.
Communication Privacy Management	Employees expectation of privacy
Non clinical paranoia	Distress that employees suffer when they know they are being monitored and why
Boundary permeability	Why individuals bring work home and personal issues to the workplace. Root of this fact and its relationship with portable devices at the workplace.
Generational Gap	Convergence of different demographic groups at the workplace and the entrance of a new techno-savy group into the workforce, the Generation y

[12] At 77.

[13] Brian Tamanaha "A Vision of Social-Legal Change: Rescuing Ehrlich from "Living Law"" (2011) 36 L&SI 297 at 302

1. *Panopticon Effect And The Application On The Electronic Surveillance At The Workplace.*

This theory was formulated by Bentham in the 18th century as an architectural plan and explained by Mack in 1969 as:

> A prison or other highly controlled environment in which all parts of the interior are visible from a single point because a central tower is surrounded by a circular building comprised of individual cell that are opens on both ends (…) [14]

Botan explains that the panoptic effect can be applied to a contemporary environment when surveillance is conducted at the workplace making the employee visible and in contrast making the surveillance authority invisible[15]. When applying this theory to the workplace the four components of the Panoptic effect are: "(1) Employee perception of being surveilled; (2) surveillance potential of the technology (3) management policy and (4) maturation"[16]. The most important factor of the above mentioned is the employee's perception of being surveilled, this and is what creates the panoptic effect. "There can be surveillance without employees being aware of it, but not a panoptic effect"[17]. In the table below, the above components of the Panopticon effect are applied to the employment relationship when surveillance of CMWC is conducted:

Table 2: Panopticon, surveillance and workplace.

---

[14] M P Mack *A Bentham reader* (Pegasus New York: 1969) cited by Carl Botan "Communication work and electronic surveillance: A model for predicting panoptic effects "(1996)63CM 293 at 299

[15] At 308

[16]Carl Botan and Mihaela Vorvoreanu "What Do Employees Think about Electronic Surveillance at Work? John Weckert (ed) *Electronic Monitoring in the Workplace: Controversies and Solutions* (Idea Group Inc (IGI),London, 2005)135

[17] Botan "Communication work and electronic surveillance: A model for predicting panoptic effects" above n 14, at 300.

Panopticon component	Application to the workplace when employer surveillance employee's CMWC
Employer perception of being surveilled	Employees usually know they are being surveilled when using CMWC but if there is not a clear policy of CMWC usage, employees may not be aware of when or how the employer is carrying on surveillance.
The surveillance potential of the technology that is given by how much the technology makes employees visible and how much the technology keeps the surveillance authority invisible	The surveillance potential of the technology used to monitor employee's CMWC usage is high because it make the employees behavior extremely visible and the surveillance authority operates in the darkness. (e.g. Keystroke software)
Management policy determines when technology that can be used for surveillance actually will be.	The more weak is the Internet policy for example, the more uncertainty employees will have about when they are being surveilled
Maturation determines how surveillance technology becomes integrated with management policy	"Surveillance procedures are well established, legal or union opposition has been resolved and the results of surveillance are an acknowledge part of organizational decision making and disciplinary proceedings"[18]

Additionally, this theory is useful because it explains from a sociological perspective the connection between surveillance at the workplace and the power bargain gap between employer and employee. In Botan words:

> Surveillance technology can transform most physical structures into the electronic equivalent of a panopticon that can be used to enforce coercive and reward relationships because the action of today's workers can be made as visible as were the actions of the occupants of the physical panopticons cells while the observer can be rendered as completely invisible[19]

Raven also provides an explanation about the link between surveillance and increase of the employer power at the workplace: "Having used coercive power along surveillance, the power holder attributed any successful influence to the power holder rather than the target tending thereby to further devalue and distrust the target"[20]. Other panopticon effects caused by surveillance technology are discussed in more detail below, for example the

[18] At 300.

[19] At 299.

[20] B H Raven " The bases of the power : Origins and recent developments " (1993) 49 JSI 227 at 270

impact that being monitored has in workers self-esteem, paranoia and autonomy at the workplace.

2. *Communication Privacy Management (CPM) Theory: The root of the expectation of privacy of employees.*

Communication Privacy Management theory was first proposed by Sandra Petronio, and is described as "a theory of relational communication that relies on the boundary metaphor to discuss how individuals constantly manage the dialectic between revealing and concealing private information".[21] According to Petronio, CPM is regulates in five principles:

> First, people believe that they own their private information. Second, they believe that they retain the sole right to regulate the flow of their private information to others. Third, privacy rules are negotiated in order to regulate the flow of private information to others. Fourth, people with whom private information is shared become co-owners of that information and are obligated to follow the established privacy rules. Finally, when privacy rules are inadvertently or intentionally violated, boundary turbulence results, which can lead to a number of negative outcomes for both the relationship and the individuals involved[22].

Applying the above to the workplace, employees are selective to whom disclose their personal information and they expect the receiver follow the initial rules of disclosing and use. These boundaries are breached, where there is an intrusion of a person that employees did not expect to have access to their information, or maybe because the receiver did not follow the psychological contract. This results in "boundary turbulence". Boundary turbulence occur then "often results in mistrust, anger, suspicion, or uncertainty about sharing private information."[23]. One example of this, is "the covert, unobtrusive nature of e-mail monitoring that creates a dilemma for employees' ability to control the boundary around their e-mail content, which can result in boundary turbulence"[24].

---

[21] Snyder , above n 4, at 272.

[22]Sandra Petronio "Translational research endeavors and the practices of communication privacy management" (2007) 35 JACR 218 at 219.

[23] At 219.

[24] Snyder , above n 4, at 290

When there is not a clear CMWC usage policy that has been discussed between employer and employee, employees can create boundaries around the information they disclose via email or IM) [25], possibly to be caught by surprise by the employer who was monitored in the darkness, leading to boundary turbulence, which means distrust and relationship conflict at the workplace. Despite the numerous negative consequences of breaching a sense of privacy for employees not only for the individuals under surveillance but also for companies as well, there is not one piece of statutory law in New Zealand that makes it mandatory for employers to have an email and internet policy.

3. Paranoia and well-being of employees

Non Clinical Paranoia in a monitored workplace is explained by Kremer as "forms of social misperception and misjudgment characterized by exaggerated, rather than false or delusional, distrust and suspicion of other individuals, groups, or organizations."[26] Kramer explains the link between paranoia and electronic surveillance at work in these words:

> Monitoring and surveillance systems communicate to employees that they are not trusted, which potentially breeds mistrust and resentment in return. Thus, individuals may begin to be suspicious about those implementing such systems. What are they after? Why don't they trust US? (…)Monitoring systems designed to improve the quality and reliability of service can also foster paranoia[27].

Paranoia is not only the outcome of the boundaries breach above explained, but also the consequence of the first theory this paper explored, the Panopticon of Bentham. As it was mentioned, when there is a panopticon effect the employees believe that they are being monitored but there is a degree of uncertainty. Botan explained that "surveillance authority

---

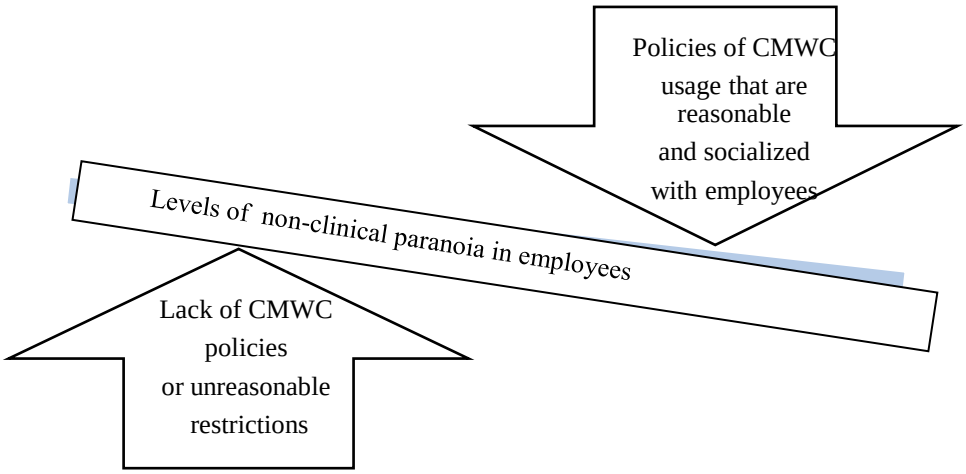
[25] "It might not be enough for organizations to have a policy that employees read and sign, but they should also consider taking steps to sell the rationale for this policy to employees": At 290

[26] RM Kramer "Organizational paranoia: Origins and dynamics" (2001) 23 Res Organ Behav 1 at 23

[27] "Surveillance should affect employees because of the apparent attack on their self-esteem that is implicit in the suggestion that they are bad enough, lazy enough to make surveillance necessary. In a sense, electronic surveilling serves as a kind of meta-communication that conveys that he employer does not trust employees": Botan "Communication work and electronic surveillance: A model for predicting panoptic effects" above n 14, at 300

creates uncertainty as to when surveillance is active, exactly what is observed and whether the results will threaten job security". This state of anxiety, uncertainty, paranoia and lack of self-steem can be reduced by having a clear CMWC policy (e.g Internet Policy, ICT Policy or e-mail Policy). It must be said, the mere existence of a CMWC agreement is not enough to diminish paranoia. "The organization needs to take steps to communicate adequate justification for its monitoring policy". [28] As it can be seen in the next image:

Diagram 1. Relation between non-clinical paranoia and lack of Policies of CMWC



4. The Boundary permeability Theory: Portable devices as CMWC.

The concept of boundaries in sociological literature is 'the physical, temporal, emotional, cognitive and/or relational limits that define entities as separate from one another'[29]. The Boundary Permeability theory addresses how people construct, maintain, negotiate and cross the boundaries between work and family roles[30]. One of the factor that has changed has changed and blurred those boundaries between personal and professional life is use of

[28] Snyder, above n 4, at 290

[29] Blake E Ashforth, Glen E Kreiner and Mel Fugate "All in a day's work: Boundaries and micro role transitions" (2000) 25(3) ASJC 472 at 474.

[30] Linda Duxbury Christopher Higgins, Rob Smart "Mobile technology and boundary permeability" (2014) 25 Brit J Manage 570 at 571.

smartphones and portable devices in general because employers expect employees to be available for work outside the workplace[31]. This expectation increases when the smartphone, tablet or computer is given by the employer to the employee to conduct work daily activities. This interference does not occur only in employees "family time", but also *vice versa*. For example, when employees bring personal affairs to the workplace by using CMWC for not work related tasks the employer's interest in productivity can as a result be affected. When this occurs and is counterproductive to the employer's interests usually there are disciplinary consequences for employees which are established on the employment agreement.

5. *Generation gap theory: The introduction of generation Y and its impact on The workplace*

The generation gap theory is explained as the differences in attitudes, expectations and beliefs based on unique generational experiences [32] according to the time on history when the individual was born. The most recent generation to enter into the organizational market is the Generation Y with 72 million prospective employees internationally"[33].

This generation brings two important aspects to the workplace according to psychological studies[34]: Their close relation with technology on a daily basis and their necessity for autonomy. Contrary to Baby-Boomers and Generation x, Generation Y has proven to have the closest relationship with the technology, therefore their behavior at the workplace is linked with CMWC more so than the traditional way of communication like memos or phone calls used by baby boomers. Additionally the necessity of this generation for having

---

[31] "There is evidence that supervisors produce more fluid work–family borders by requiring computer and communications use outside the workplace": Derks Daantje and others " Smartphone use and work–home interference: The moderating role of social norms and employee work engagement" (2014) 88 J Occup Organ Psychol 1 at 5.

[32] *See* Abdelbaset Queiri and Others "Generation-Y Employees' Turnover: Work-Values Fit Perspective (2014)9 IJBM 199.

[33] Daisy A. Mitchell "Generation y information technology employees in the workplace: a qualitative study on how leadership motivates creativity and retention" (Doctor of Philosophy Theses, Capella University, 2015) at 1. Retrieved from <http://gradworks.umi.com/36/82/3682646.html> .

[34] At 36.

autonomy has been discussed widely in organizational psychology papers. In words of Karen M Myers "Millennials have an affinity for CITs and computer mediated communication (CMC); they see work in flexible terms and they desire flexible work schedules to accommodate their desire for work-life balance"[35].

Bearing in mind the number of Generation Y employees, for lawmakers and employers to understand the dynamics of this generation at the workplace is to understand a completely new behavioral trend regarding communication and usage of CMWC for the future years. In New Zealand for example one of the factors that the Law commission took into account to propose the reform of the Privacy Act 1993 was the change of generation: "The commission also make proposals for better taking into account the perspective of different cultures and young people".[36] The question then is, whether the changes proposed in this legislature are effective to achieve that objective or not.

III Legal Approaches to Privacy Issues That Arise From Electronic Surveillance at the Workplace: Anglo American and European Approach.

The Anglo-American and European approaches have been thoroughly studied by academics due to their philosophical juxtaposition regarding the Privacy right. Privacy, in the Common law system views, is a right closely connected to private property, while in European countries and civil law jurisdictions privacy notion is a matter of human dignity[37]. This foundational divergence is reflected on the legal protections of employees from electronic monitoring at the workplace:

A Anglo-American Approach: The Predominance of the Ownership of the Networked Infrastructure.

[35] Karen K Myers and Kamyab Sadaghiani "Millennials in the Workplace: A Communication Perspective on Millennials' Organizational Relationships and Performance" (2010) 25 J Bus Psychol 226 at 231.

[36] Law Commission *Review of the Privacy Act* (NZLC R123, 2011) at 42.

[37] Peter J Isajiw "Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers" (2001) 20 Temple Envtl.L.& Tech.J. 73 at 14.

A fundamental analysis for Anglo-American traditions is that "privacy implies notions of property, ownership and expectations with regard to the exclusion of outsiders without specific legal rights"[38]. Hence, as part of a property whole, privacy is seen as a possessive right that may be alienated preemptively[39].

Applying this concept into the workplace where employees sell their capacity to labour, it alienates certain aspects of the person and puts them under the control of the employer[40]. In this case an employees' privacy as property right is overruled by another property right: the employer's ownership of the networked infrastructure, this constitutes the so called "Property-Rights Approach".

This approach holds that "the employer, by virtue of ownership of the premises and equipment, has the right to oversee the activities of employees"[41] Under this approach, the employees seems to sell their control over their personhood to the employer while they are at work[42]. Whatever material is contained in employees' work computer belongs to their employer, and if the employers has an e-mail and Internet policy forbidding all personal use, he is legally able to access to employees personal CMWC[43].

In the United States this approach is enshrined in the important federal legislation Electronic Communications Privacy Act of 1986 ("ECPA")[44]. ECPA prohibits the intentional, actual or attempted interception, use, disclosure, or "of any other person to intercept or endeavor to intercept any wire, oral, or electronic communication"[45]. But at the same time, "the ECPA exempts e-mail service providers from liability for all interceptions or accessions of e-mail communication in the workplace"[46]. This exemption allows the

---

[38] Lawrence E Rothstein "Privacy or. Dignity? : Electronic Monitoring in the Workplace" (2000) 19 NY Sch J Int'l & Comp 379 at 382;

[39] At 382

[40] At 382

[41] Isajiw , above n 37, at 15

[42] Rothstein, above n 38, at 382.

[43] Rustad and Paulsson, above n 3, at 91.

[44] Electronic Communications Privacy Act of 2000 18 USC § 2515.

[45] § 2515

[46] Isajiw, above n 37, at 6.

provider of a private communication system to monitor the use of its equipment [47], therefore if the employer provides the equipment and/or the network, surveillance of the electronic communications of its employees falls into this exception.[48]

B European Approach: The intrinsic link between Privacy Rights and Human Dignity.

In contrast with the Anglo-American approach, the European view of privacy "relates to moral autonomy and as such is encompassed by human dignity, which inheres in legal personality and is considered an extension thereof"[49]. The European workers' right to privacy is inextricably linked with the development of trade unions, worker self-control and self-determination[50]. Another dimension of the concept of human dignity is a social one that promotes a humane and civilized life[51]. That is, as human beings and being part of society employees have a fundamental necessity to build interpersonal relationships. A person's human dignity is diminished with actions that reduce a person's status as a thinking being, a citizen and a member of a community[52]. On the other hand, employees' Human dignity is respected if employers recognize that people subordinate themselves to them while at work, but this subordination extends only to the performance of work-related activities[53].

Examples of European legislation that have adopted this approach in matters of surveillance at the workplace are 1. Spain, where the Labor Act [54] set out that "the employer may adopt any appropriate measures to verify and control the performance of the employees' duties, always respecting human dignity"[55] . In Austria the Federal Law Gazette Art. 96 establisheed that "control measures and technical installations should not

---

[47] Rothstein, above n 38, at 401.

[48] At 402

[49] Karen Eltis "The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Case law in Canada and Israel: Should Others Follow Suit? " (2003) 56 Mcgill LJ 289at 314.

[50] Rustad and Paulsson, above n 3, at 48

[51] Rothstein, above n 38, at 383

[52] At 383

[53] Isajiw , above n 37, at 16

[54] *El Estatuto De Los Trabajadores 1980 (*Spain) [Labor Act 1980].

[55] S (2) (20)

be undertaken by the employer if such measures impinge upon human dignity[56]. Another example is the Italian Privacy Commissioner who in 2007 issued guidelines for employers' to monitor employees' email and internet, in the motives section he established:

> The workplace is a community where it is necessary to ensure that data subjects' rights, fundamental freedoms, and dignity are protected. To that end, employees must be enabled to freely express their own personalities within the framework of mutual rights and duties.[57]

"The protection of human dignity allows a broader scope of action against treating people in intrusive ways"[58] and therefore more protective of employees' privacy interests. "It is rooted in the notion that each person is unique and autonomous and, therefore, should be free from the manipulation and domination of others, including employers"[59]. To conclude, in contrast to Anglo American traditions, this dignity-based approach is what "in effect is a human rights model that arms employees with countervailing privacy rights to challenge abusive employer surveillance practices"[60]

IV New Zealand Legal Approach: The Legal Status Quo

Karen Eltis explained that in contradiction to civil law jurisdictions, the common law tradition views that a person's right to privacy fundamentally derives from his or her property rights[61] . An outcome of this philosophical conception in common law countries is their adoption of the "ownership approach" to address issues of electronic surveillance at the workplace[62]. New Zealand being a common law system does not provide us with an

---

[56] *Arbeitsverfassungsgesetz* 1974 (Austria) [Federal Law Gazette 1974] art 96

[57] *The Garante per la protezione dei dati personali* (Italy) [Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context] 1 March 2007 Retrievable from <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1408680>

[58] Rothstein , above n 38, at 383.

[59] Isajiw, above n 37, at 15

[60] Rustad and Paulsson, above n 3, at 52.

[61] Eltis, above n 49, at 312.

[62] See JamesWatt "Electronic workplace surveillance and employee privacy: a comparative analysis of privacy protection in Australia and the United States." (LLM Thesis, Queensland University of Technology, 2009) Retrievable from < http://eprints.qut.edu.au/26536/>

exception to this tradition as it predominantly applies the ownership approach to resolve matters such as the monitoring of employees' CMWC.

This section sights what the relevant legislation and case law is when exploring the issue of electronic surveillance of employees' CMWC in New Zealand, how it is applied, and if it is effective to protect employee's privacy interests from abusive electronic monitoring. This section also explores whether New Zealand applies the ownership approach wholly to this matter or if exceptions exists where dignity is also considered.

*A **Privacy Law As Applied to the Issues of Electronic Monitoring of Employee's CMWC Usage:***

The privacy framework in New Zealand is constituted by The Privacy Act 1993[63](The Privacy Act), The Recommendation of the Council of the Organisation for Economic for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy an Transborder Flows of Personal Data" (OECD Guidelines)[64], Human Rights review Tribunal (HRRT) decisions and the decisions of the Privacy Commissioner. The Privacy Act recognizes that a breach of privacy may be detrimental to dignity but at the same time imposes a high threshold to determine what complaints can be brought to the Privacy Commissioner.

The Privacy Act sets out that a breach of a privacy principle must be accompanied by significant humiliation, significant loss of dignity, or significant injury to feelings"[65]. Any complaint must to be settled first between an employer and employee, the Commissioner may refer the matter to the Director of Human Rights Proceeding for the purpose of

---

[63] Privacy Act 1993.

[64]Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

[65] Section 66(1)(b)(iii).

deciding whether proceedings should be instituted.[66] The Director will then decide if the case should be taken to the Human Rights Review tribunal[67]

The Privacy Act is based on 12 principles that draw on the 1980 OECD Guidelines[68]. The next image is a re-cast of the Privacy Act principles from an employment lens, based on the work of Crawford, Harbridge and Walsh, and it illustrates how these principles are grouped by privacy issues and applied to the employment relationship [69] (this is not the original text of the Privacy Act)

Table 3: Privacy principles applied to the employment relationship.

Privacy Issue	Privacy Principle applied to the employment relationship
Collection	1.Necessary purpose for collection
	2.Collection must be from individual concerned.
	3.Advice given to employee of collection
	4.Collection to be by lawful means
Security and storage	5.Protection against loss, alteration, disclosure, misuse.
	9.Information only held for as long as is necessary
Access and correction	6. Employees right of access
	7 Employees right of correction
	8.Information to be checked
Use	10. Information to be used only for purpose for which it was collected
Disclosure	11. Disclosure prevented
Unique identifiers	12. Prohibited to assign unique identifiers

[66] Section 77: "An individual may himself or herself bring proceedings if the Commissioner or the Director is of the opinion that the complaint does not have substance or ought not to be proceeded with."

[67] Section 83.

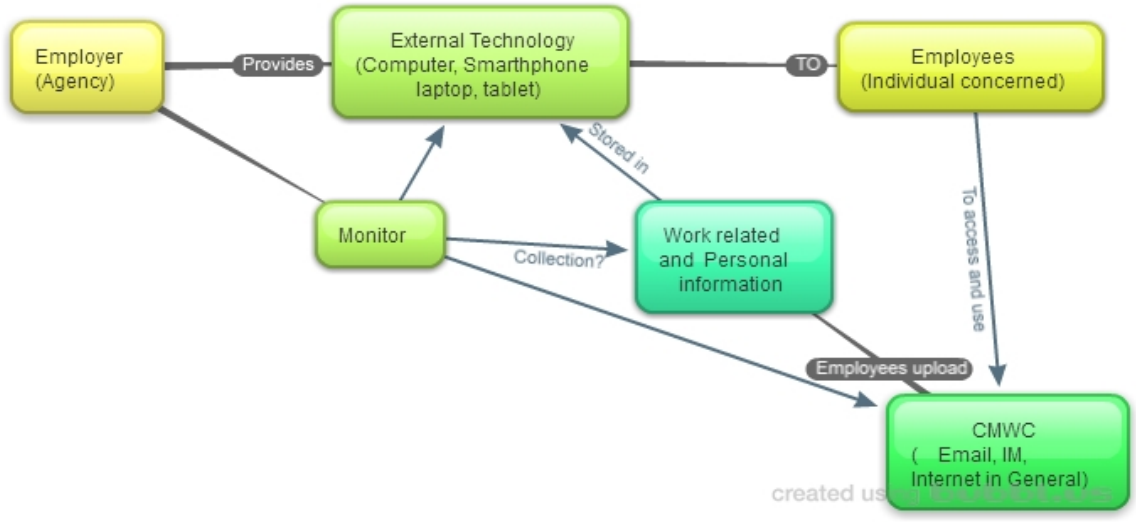
[68] Paul Roth "Privacy law reform in New Zealand: will it touch the workplace?" (Presented to Third Biennial Labor Law Conference of the New Zealand Labor Law Society in Otago Universiy,Wellington,2015)

[69] Aaron Crawford, Raymond Harbridge and Pat Walsh *Privacy in the workplace: the effects in the Privacy Act 1993 on Employment practices in New Zealand* (Victoria University of Wellington, Wellington, 1995) at 4

Below, this paper studies the application of a number of the principles as they were written originally at the Privacy Act. In the interest of relevance to electronic surveillance this paper only focuses on the principles: 1, 2,3,4,5, 9, 10 and 11, although all principles are susceptible to be applied to surveillance issues.

As an introductory note, this piece of legislation is under review according to the recommendations of the Law Commission[70] made in 2011, but according to Professor Roth it is probable any expected amendment will not touch the workplace[71]. This would be unfortunate considering that one of the factors which led the Law Commission to propose amendments to this act was ongoing technological changes: Technological innovations should be monitored and fed into privacy reviews. To assist, public sector agencies should be required to do privacy impact assessments when dealing with new developments.[72]As illustrated in the background, technology has impacted not only life outside the workplace but also the dynamics within organizations. Any reform to the Privacy Act should address employee's privacy interests when they use CMWC. The next diagram shows the dynamic at the workplace when there is electronic surveillance.

Diagram 2: Surveillance of CMWC at the Privacy Act 1993 light .



[70] *See* Law Commission, above n 36.

[71] Roth "Privacy law reform in New Zealand: will it touch the workplace?", above n 68, at 1.

[72]An 'agency' is widely defined as any person or body of persons, whether public or private, and whether corporate or unincorporated, with specified exceptions: Law Commission, above n 36, at 33.

As seen from the diagram employer's act as "agencies" [73] under the Privacy Act when they provide external technology to their employees who are the "individual concerned"[74] Employees use CMWC by uploading work-related and personal information to the system.[75]. Next, this paper explores the Privacy Act principles that are applicable to the issue of surveillance of CMWC at the workplace and how they protect employees from abusive monitoring[76].

1 Collection: Principles 1 to 4 of the Privacy Act 1993.

The question that arises from electronic surveillance at the workplace is if employers are "collecting information" for the purposes of the Privacy Act which if so would bind them by principles 1-4 of the Privacy Act[77]. Paul Roth argues that is not collection because the employer already holds the information in their computer system[78]. This approach is reflective of the Anglo-American view regarding ownership of the networked infrastructure, but it has not been applied to case law in New Zealand. Another argument offered to support the view that surveillance is not a collection of information is that the agency is not soliciting for the information[79]. This approach was adopted by the Court of Appeal (NZCA) in *Harder v Proceedings Commissioner*[80].

---

[73] Privacy Act, S 2.

[74] Section 2.

[75] Personal information "is any information that an employer might collect about an individual, whether or not that person is an employee. Information gathered by a manager or other agent of the employer is deemed to be information gathered by the employer itself": Richard Stanley Rudman *New Zealand Employment Law Guide* (2014 ed, CCH New Zealand, Auckland, 2014) at 420

[76] Law Commission, above n 36, at 12.

[77] Privacy Act, s 2.

[78] [It] Is important to state that "the Act's privacy principles are not enforceable in the courts, with the exception of principle 6, which deals with access to personal information where that information is held by a public sector agency" : Paul Roth "Privacy in the workplace" (Paper presented to the Labor, Employment and Work in New Zealand, Wellington ,1994) at [5-6];

[79] Privacy Act, s 2.

[80] Voice recording over a telephone did not constitute a "collection" of information because was unsolicited. "The unsolicited nature of the information was not affected by the fact that it was recorded or the way it was

The HRRT held a different position regarding information gathered through surveillance in *Armfield v Naughton* [81], setting out that the above approach is not congruent with the spirit of the Privacy Act because by narrowing the term collection "by soliciting in the sense of "to ask for" would be inconsistent with the promotion and protection of personal privacy.."[82] This last approach is accurate and more protective of privacy interests. Following this reasoning Principle 1, 2, 3 and 4 of the Privacy Act will be applied to surveillance at the workplace.

(a) Principle 1. Purpose of collecting information: What is considered as Lawful purpose and necessary for it, when conducting surveillance over employees CMWC usage?

Principle 1 of the Privacy Act "sets out that agencies must not collect personal information unless it's for a lawful purpose connected with the functions or activities of the agency, and collection is necessary for that purpose"[83]. Hence, this principle has three requirements: 1. there must be lawful purpose for collecting the particular information 2. The information must be needed for some function or activity of the employer. 3. The information must be necessary for the employer to achieve that purpose.

Regarding the concept of "lawful purpose" when it comes to surveillance of CMWC in an employment context, it can be inferred that it would be any objective connected with the interests of the business. This is reflected in the Privacy Act when it imposes certain obligations to the Privacy Commissioner when deciding cases. According to the act the Privacy Commissioner must:

> Have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information

---

recorded. It was therefore not relevantly collected": *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 (CA) at 25.

[81] *Armfield v Naughton* [2014] NZHRRT 48, (2014) 9 HRNZ 808

[82] At [3] per Tipping J.

[83] *Case Note 229558* [2012] NZPrivCmr 1. Retrievable from < https://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-229558-2012-nz-privcmr-1-employer-uses-monitoring-software-to-collect-personal-information/>

> and the recognition of the right of government and business to achieve their objectives in an efficient way[84].

When analyzing this provision one may conclude that it enshrines both approaches, the Anglo-American and the European one. First, this provision sets out that Human Rights should be taken into account in privacy matters (E.g. Dignity) but at the same time it gives significant weight to the interests of business to achieve their objectives. For example, the employers' interest in their employees to not use their equipment to personal matters. According to Paul Roth this provision allows to the Privacy Commissioner to balance interests when resolving any conflict. "However, it also tends to permit the Commissioner to operate in a manner that is less strict on employers, as is evident from a number of investigation case notes"[85]. It seems then, the Privacy Act has also attempted to protect dignity but in matters of the workplace, in reality, the Anglo-American approach is predominant and favours the employers' interests over their equipment.

This is also reflected in the legal enforcement schemes. For example, the Privacy Commissioner wrote in a brochure that is directed to business, what a purpose for employers to carry out surveillance on employees CMWC could be:

> [It] is therefore reasonable for employers to exercise some form of control over how that resource[86] is used. For example they need to ensure that employees' activities online will not compromise the business' reputation. They will also need to ensure, for example, that employees are not spending so much time on personal emails that their work is adversely affected.[87]

Employees' dignity however, is not mentioned even briefly making it clear again what values are most impact in matters of privacy at the workplace.

---

[84] The Privacy Act, s 14(a).

[85] Paul Roth "Privacy law reform in New Zealand: will it touch the workplace?" above n 68, at 4.

[86] The commissioner is making reference to Computers, the Internet and email.

[87] The Office of the Privacy Commissioner. *Privacy At Work: A Guide To Privacy Act to Employers* (2008) Retrievable from <https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf>

Regarding the concept of "necessity" to monitor employees CMWC, it refers to the means to achieve one of the possible purposes described above. The Human Rights Review Tribunal gave a definition in *Lehmann v Canwest Radioworks*[88] *Ltd* as: a measure "which is essential; something but for which the purpose cannot possibly be achieved"[89]. Additionally, the term "necessary" has been interpreted as "reasonably necessary".[90]
With exception of the Case note 229558[91] there is no decisions of the Privacy Commissioner that address whether surveillance over employees' CMWC is or not "reasonably necessary". The uniqueness of this case makes it worthy of further analysis:

(i) Case Note 229558 [2012] NZPrivCmr 1 Usage of Key-stroke software to monitor employees' CMWC.

In this case "the employer used information collected from Key-stroke logging to access the employee's personal web-based email account and copy several emails"[92] the employer also accessed the employees work computer and emails. Therefore, there are two subjects of surveillance in this case that are analysed in detail: 1. The Personal Email 2. The work computer and email provided by the employer.

1. Work computer and personal email: The Privacy Commissioner held that he was satisfied that the employer's action complied with the Privacy Act principles 1-2[93] implying that the intrusion was reasonably necessary and for a lawful propose. The reason he gave is that in both the employment agreement and employee manual the employer had clearly set out that work computers would be monitored. (…)[94] therefore the employee should not have had a privacy expectation. It seems the only factor The Privacy Commissioner took into account then, to determine if the surveillance was reasonable was if there was a relation between the data collected by the employer and the employment relationship, what he did not consider is whether the surveillance is detrimental to an employee's dignity. This

[88] *Lehmann v Canwest Radioworks Ltd* HRRT Decision No 47/06.
[89] At [50].
[90] Paul Roth "Privacy in the workplace", above n 78, at 5.
[91] *Case note 229558*, above n 82.
[92] *Case note 229558*, above n 82.
[93] Privacy Act, s 6.
[94] *Case note 229558*, above n 82.

position is an expression of the Anglo-American approach where privacy as a right is reduced to a contractual matter.

There is a fallacy in the decision because of the Commissioner's analysis of the usage of keystroke software to monitor employees. First, the Commissioner decided as stated above, that the employer's surveillance in this case was "reasonable necessary" and "lawful" (Principle 1). Contradictorily to this, he stated that the employer breached Principle 3(Individual's awareness of being monitored) by using keystroke software because "the policies in the agreement and manual were not explicit enough to make staff aware that such detailed information was being collected". The correct reasoning would be that when the usage of keystroke software at the workplace breaches Principle 3 it unavoidably breaches Principle 1. This kind of software allows such insight into an individual's communications that it should be considered *prima facie* disproportionate therefore unreasonable. Especially if the employee is not aware that he is under keystroke monitoring.

The fact the Commissioner took the usage of keystroke software into account in his decision is a small step forward to the protection of employees from invasive electronic monitoring. The downside is that this rare opportunity was not used to give any warning about the detriment of employees' human rights by this kind of technology. Key-stroke software[95] is a highly invasive technology and is increasing in use[96]. This computer program shows in real time and detail the employee's CMWC usage. It gives to employers a capability to read the entire content of emails, websites, or any other CMWC by taking screenshots of the employee's computer among other methods. It gives to the employer a

[95] Keystroke Software or Key Logging, "are meant to monitor the Internet traffic of entire enterprises. There is no shortage of such software available for purchase by both companies and individuals. Programs like Spector Pro can keep detailed logs of keystrokes,screenshots, instant messages, and URLs visited on individual computers.": Brittany Persen "Employee Monitoring: It's Not Paranoia You Really Are Being Watched!" (26 May 2008) PcMag <http://www.pcmag.com/article2/0,2817,2308363,00.asp>

[96] "These sophisticated programs can even track an employee's Web-based e-mail accounts provided by, for example, America Online, Hotmail or Yahoo - personal accounts that employees often assume are off-limits to monitoring. The extent of such tracking is large in scope as over 60 million employees have e-mail and/or Internet access at work.85 96% of employers who monitor e-mail track external - incoming and outgoing - e-mails.": Corey Ciocchetti, "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring." (2011) 48.2 AmBusLJ 285 at 287.

significant insight into employees' personal life (e.g. Sexual orientation, religion, political alignment, health issues, among others[97].). Information that can be used for discriminatory purposes and simply the fact that the employer has access to it is already an affront to human dignity.

To sum up, The Privacy Commissioner could had taken advantage of this case to offer a more elaborate and clear approach, compelling employers to be observant of employees human rights when using this kind of technology because of its potentiality to invade an employee's privacy. Or better still, he could send a message to employers to not use key-stroke at all without his authorization.

2. Accessing by employer of the employee's personal email account: The Commissioner established that this intrusion was a breach of principle 1-4 of the Privacy Act because a personal email has a high privacy expectation. In this instance the Commissioner let pass an opportunity to engage employers in order to deter this kind of behavior which has no place in a democratic society that is respectful of human rights. The fact the employer accessed a personal email account is not only a privacy intrusion, it is a criminal offence under the Criminal Act 1961[98], but again this was not discussed.

To conclude the analysis of Principle 1, legal sources in New Zealand have being neglecting the normative value of the term "reasonably necessity" especially nowadays where keystroke software is used to monitor employees. The lack of guidelines leaves the impression that employee's privacy interests, when using CMWC, are always deferential to management's discretion. Although the threshold method about the "reasonability of the necessity" may offer a protection to the employees' privacy rights, there is a need for a legal framework that addresses the root of the problem. The best way of doing so is balancing the interest of employer with employees' human rights. As the Law Commission stated in the review of the Privacy Act document "a system based solely on complaints is not always adequate to resolve problems. A complaints process is necessarily ad hoc and piecemeal. It may

[97] *See* Human Rights Act 1993, s 21: "Prohibited grounds of discrimination".

[98] Criminal Act 1961, s 252 : Accessing computer system without authorisation (1) Everyone is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.

succeed in resolving individual cases, but is not so good at detecting and solving systemic problems"[99].

2 Storage, security and use: Principle 5, 9 and 10

Principle 5 of the Privacy Act addresses the steps that the agencies should take to protect the employees personal information already collected through surveillance. Under principle 5 an employer as agency, "who holds personal information must ensure it is protected by reasonable security safeguards against loss, unauthorized access, use, modification or disclosure, and other misuse"[100]. This principle is especially relevant when there is constant surveillance over employees CMWC and this is gathered by other employees. Usually Human Resources managers, other managers and IP staff are able to access the information that technology has retrieved from employees CMWC. These staff should acknowledge beforehand that they are agreeing to observe principle 5 of The Privacy Act and will take measures to protect personal information against misuse.

3 Disclosure: Principle 11.

Principle 11 of the Privacy Act[101] would be applied to the employment relationship by imposing "an employer who holds personal information must not disclose the information to another person or agency"[102]. To illustrate how the HRRT had applied this principle to matters that arise from electronic surveillance at the workplace, the case *Hammond v Credit Union Baywide* is explored in detail below.

(i) *Hammond v Credit Union Baywide:* Recognition of the Connection between Privacy and Dignity at the workplace.

---

[99] Law Commission *Review of the privacy act,* above n 36, at 6.19

[100] Rudman, above n 75, at 441

[101] Privacy Act, s 6.

[102] At 442.

The case *Hammond v Credit Union Baywide*[103]*(* NZCU Baywide) deals with the following facts: Ms. Hammond had shared a photo among a circle of friends on Facebook. "The photo featured a cake with written obscenities referring to NZCU Baywide, which was her employer at the time - although she was in the process of leaving the company for another employer"[104]. Ms. Hammond's privacy settings allow only people who are her friend to see this picture. "The company management received evidence of the photo and the human resources manager then coerced a junior employee to reveal the photo on her Facebook page. The manager made a screenshot of the photo and disclosed it to other senior managers"[105]. Once the company had the screenshots, these were distributed among other businesses in the region with the advice to not hire the Ms. Hammond. The HRRT then dealt with the breaching of Principles 1,2,3,4 and 11 of The Privacy Act.

An employee's Facebook is generally out of the scope of the CMWC definition unless it is accessed from a workplace computer or the account has been created for business purposes. As a remainder, CMWC are communications that are established by using the electronical means that the employer has provided or are for business purposes initially. In the above mentioned case it was a personal Facebook account. However the decision is still relevant for this paper regarding the application of principle 11 because it involves the disclosure of an employee's personal information that was gathered by the employer's electronic surveillance[106].

The HRRT considered that the employer breached principle 11 when the company disclosed the photo of the employees Facebook by sending it to recruiting companies. The HRRT decided the breaching of Principle 11, has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to Ms. Hammond's feelings among other undesirable consequences. "The decision sets a new benchmark for compensating

---

[103] *Hammond v NZCU Baywide* [2015] NZHRRT 6.

[104] Charles Mabbett "Record damages awarded for cake photo breach" (2 March 2015) The Privacy Comissioner <https://www.privacy.org.nz/blog/cake-privacy-breach/>

[105] At 4.

[106] The HRRT did not intend to explore further the breaching of principles 1-4 ,"the reason is that the plaintiff has not established to the probability standard a causal connection between the alleged breaches of Principles 1 to 4 and the forms of harm listed in s 66(1)(b)(i) to (iii) of the Privacy Act. Unless such causal connection is established, the claim must fail": *Hammond v Credit Union Baywide*, above n 103, at [134]

harm caused by a breach of the Privacy Act for unlawfully disclosing personal information"[107]. The considerations made by the HRRT, represent first of all the recognition of the technology (Facebook) and its true dynamics (e.g. Privacy settings to disclose information only with Facebook friends)[108] and secondly a more protective approach, closer to the European dignity-based concept.

For example, while the Employment Relations Act 2000[109] (ERA) set out that a remedy of a personal grievance may be reduced if the behavior of the employee has contributed to the adverse outcome[110], the HRRT took a completely different approach. The Tribunal did not take into account the fact that Ms. Hammond took a photo of the offensive cake and then uploaded it on to Facebook. The tribunal establishes that "Principle 11 does not condone the disclosure of personal information on the grounds there has been supposed misconduct on the part of the individual"[111] . This reasoning is more protective of privacy rights and the dignity of employees because it acknowledge that employees wrongdoing is not always an acquiescence to intrude in their privacy.

B Employment Law Applied to the Issue of Electronic Surveillance of Employee's CMWC.

This section studies the approach that employment institutions have taken to electronic surveillance at the workplace and also examines if as a common law jurisdiction, New Zealand employment law has applied fully the Anglo-American view.

---

[107] Charles Mabbett "Record damages awarded for cake photo breach", above n 104, at 11

[108] Employment institutions on the other hand, have neglected the true dynamics of technology creating a precedent that social media is no longer private even if the employee set up high privacy settings. For example: *See Hook v Stream Group (NZ) Pty LtdIt* [2013] NZEmpC 188 at [29]: "(…) is well established that conduct occurring outside the workplace may give rise to disciplinary action, and Facebook posts, even those ostensibly protected by a privacy setting, may not be regarded as protected communications beyond the reach of employment processes. After all, how private is a written conversation initiated over the internet with 200 "friends", who can pass the information on to a limitless audience?"

[109] Employment Relations Act 2000.

[110] At s 124.

[111] *Hammond v Credit Union Baywide,* above n 103, at 164

First of all, the employment case law researched addresses issues that arise from the employment relationship such as dismissals. In matters of surveillance of CMWC, the most mentioned motive for disciplinary actions is the employee's misuse of Internet or Email (In general all CMWC). When a dismissal occurs, employees are entitled to pursue a grievance action in order to obtain a reinstatement, among other remedies[112]. Employment institutions analyses the grievance action by applying the statutory test of justification under s103A of the Employment Relations Act 2000[113]. The intended outcome of this analysis is to decide if the process to take the decision was as would be expected from a fair and reasonable employer[114].

The "reasonability" is assessed differently by privacy and employment institutions when there is a dismissal based on the findings of electronic surveillance. Privacy institutions would analyse the reasonability of the surveillance itself whereas the employment institutions would focus on the wrongdoing and the disciplinary action as an outcome of it. The fact that the surveillance and its effect on privacy rights is not an item in discussion on employment case law is a reflection of the Anglo-American tradition that assumes, because the employer is the owner of the network they are entitled to monitor the usage of their own resources[115].

1 The Reasonableness of dismissal or an action based on misuse of CMWC (Internet, email, IM, computers) and the test 103A.

In words of Paul Roth "The emphasis is on fairness and due process, rather than any rights stemming from the Privacy Act[116] due to the lack of jurisdiction of employment institutions "to interpret the principles of the Privacy Act or apply them directly; only the Human Rights Review Tribunal has such a jurisdiction"[117]. The Court had recognized timidly that when assessing the reasonableness in employment matters "the Privacy Act's provisions

---

[112]The Employment Act 2000, s 79a.

[113] Section 103(1)(a).

[114] Gordon Anderson and John Hughes, Employment Law in New Zealand (2014 Ed, LexisNexis Wellington) at 800 [ER103A]

[115] See Rothstein, above n 38.

[116] Roth "Privacy law reform in New Zealand: will it touch the workplace?", above n 68, at 12

[117] At 4.

may be said to represent current community standards and expectation"[118], meaning that the principles of the Privacy Act can give an idea of the fairness of the disciplinary action, unfortunately this position does not have echo in cases that deal with the surveillance of CMWC, where the reality is that the Privacy Act does not play any role[119].

In such a context, applying the 103A test, the justifiability (what a fair and reasonable employer would have done) of a disciplinary action for misuse may hinge on whether the employee had a reasonable expectation of privacy. [120]The reasonable expectation of privacy is measured against 1. If there are privacy policies at the workplace or CMWC policies (This document may have various names, e.g. email, internet or IT policies) 2. The culture at the workplace 3. The relations between employee and employer for example, length of service. These three aspects are explained below by studying some relevant employment cases. In the interest of practicality this paper explores only cases after the 103 test was implemented (2004)[121].

1. Privacy expectation and privacy policies at the workplace[122]: In *Toleafoa v Vodafone New Zealand Ltd*[123] An employee was investigated for an alleged breach of the company's email policy. It was discovered that she had sent emails to a friend's work email address referring to her managers as "ufa" and "kefe"[124]. The ERA determined Ms Toleafoa has no privacy expectation because the employer's policy stated that all messages generated on its systems were company property and that it had the right to monitor all employee emails passing through its system,[125]therefore the dismissal was justified. The Authority determined that the employee took the risk of dismissal when she made derogatory

---

[118] *NZ Amalgamated Engineering Printing and Manufacturing Union Inc v Air New Zealand Ltd (2004)* 7 HRNZ 539, at 218

[119] Paul Roth "Privacy law reform in New Zealand: will it touch the workplace?", above n 68, at 11.

[120] Paul Roth, "Privacy in the Workplace.", above n 78, At 4

[121] Subsection 103 A was effective 1 December 2004: Anderson and Hughes, above n 112, at 800 [ER103 A.1]

[122] See also *Safe Air Ltd v Walker* EmpC Christchurch CRC 8/09 CRC 10/09 4 December 2009

[123] *Toleafoa v Vodafone New Zealand Ltd* [2011] NZERA Auckland 488

[124] At [19].

[125] At [41].

comments about the employer during working hours and while using the employer's technology and resources[126].

As inferred from above, the Authority presented some arguments in this case that are aligned with the "ownership" (Anglo-American) approach. For example that the employee dismissal is justified because she should have known "all messages generated on company systems were the property of Vodafone" because the policy stated it. This point is discussed further in the next section (See Section V (A) (7) of this paper), for now is enough to say that the Authority overlooked the employee's defense, based on the permissibility of reasonable personal use of email in the company[127]. This argument is especially important, because in a democracy respectful of human and privacy rights it is not enough to have a policy of internet usage at the workplace that establishes the ownership of all the CMWC. This policy must be clear, congruent and should not give place to ambivalences. An ambivalent policy would be one which sets out the supreme and total ownership of all digital communications but at the same time allows personal use. As stated above, the Authority omitted any comment about the adequacy of the policy in regard to employees' rights.

Reasonability based on a privacy policy only, puts a significant importance on the content of this document and the way it is enforced. As explored in the background, the theory of Communication Privacy Management[128]explains the psychologic process that individuals undergo to determine how and to whom they disclose their information. This inner self constriction is affected by privacy norms practiced at the workplace[129], but these norms ought to be clear for employees to desist from using employer's internet for private purposes.

There is one case, which although previous to 2004, is important because it acknowledges the above point. In *Allerton v Methanex*[130] the ERA dealt with the dismissal of an employee

---

[126] At [44].

[127] At [44]: The policy "stated all messages generated on company systems were the property of Vodafone. While personal use was allowed"

[128] See Petronio, above n 22, at 219

[129] At 219.

[130] See *Allerton v Methanex* [2000] 1 ERNZ 242, at [25].

who had sent personal emails from his corporate account. By doing so he breached the Internet policy because according to the employer it posed the great risk of computer viruses[131]. The ERA established:

> Methanex emphasises the potential risk to its systems from viruses that may have been imported via the plaintiffs' personal use of email, but it is difficult to understand how this is reconcilable with the employer's clear advice to employees that "reasonable" private email use is permitted. [132].

The ERA implied that the employer should not consider personal emails as a breach if he has allowed it explicitly. In this case the ERA did not express explicitly how clear the policy must be. This concept of how a policy should be designed is also not adequately addressed by employment law[133].

2. The culture at the workplace[134]: In *Linnell v Les Mills Internationa*l Ltd[135] addressed by ERA in 2012 it recognized that just because there is a policy for internet use, the culture at the workplace cannot be disregarded. In this case an employee was dismissed because she forwarded by email a joke of a male contortionist which a coworker found offensive. The ERA found that the manager had condoned this kind of behavior in the past and he had received those emails and deleted them[136].

The Authority ordered the employer to pay compensation for "humiliation, loss of dignity and injury to feelings"[137]. This case was a remarkable advance to recognizing the link between dignity and privacy at the workplace. First of all, the ERA acknowledged that there are important factors which can lead employees to decide if they disclose and share personal information through CMWC. An examples of this would be workplace practices.

---

[131] At [2].

[132] At [25].

[133] See also *Hall v Dionex pty LTD* [2015] NZEmpC 29

[134] See also *Air New Zealand Ltd v Bisson* EmpC Christchurch 17/6/2005, CC6A/05, CRC6/05, 17 June 2005: The Court set out that there were a culture of sharing passwords at the workplace and this should had been a factor when the employer decided the dismissal.

[135] *Linnell v Les Mills International Ltd* [2012] NZERA Christchurch 64

[136] At [52[.

[137] *Air New Zealand Ltd v Bisson*, above n 134, at 55.

However, the case did not sufficiently give the right to dignity its necessary consideration and comment.

3. Past conduct: In *Air New Zealand Ltd v Bisson*[138] the defendants were dismissed on the ground of Air New Zealand's review of internet usage by its employees in the engineering services division. This review highlighted heavy and/or inappropriate internet usage by some staff[139]. The Court established that the evidence shows, the only reason for dismissing the defendants was their alleged misuse of the internet at work. "There is no evidence of prior poor performance or any other matter that (…) this is a factor that should have been weighed against the loss of trust and confidence in favor of the defendants"[140]. This aspect is important because Air New Zealand argued that it had lost trust in their employees after the internet misuse. The Court recognized the value of the defendants as professionals who had invested more than 30 years at the company. Dignity or other human rights were not studied in this case, despite being covered by media,[141] and the possible humiliation of the defendants.

In conclusion, the New Zeland employment institutions have predominantly adopted the Anglo-American approach but with the notable exception of those who have taken some steps towards a more realistic view of the CMWC dynamics by taking into account factors such as the workplace culture. This may open the door to progressive employment case law in the future. Progressive in the sense that it understands the dynamics between employees and communication technology, which is changing rapidly towards a more techno-savvy workforce[142].

C Human Rights framework.

---

[138] At [3]

[139] At [3].

[140] At [41].

[141] Anonymus "Air NZ to appeal decision on employees' internet use" The New Zealand Herald (online ed, Auckland, 4 jul 2006).Retrieved from <http://www.nzherald.co.nz>

[142] "Generation Y individuals,(…) represented more than 72 million prospective employees internationally (…) They are not only technologically savvy; they are also good at multitasking and are at ease with working in a global environment (…) [They]had continual and expanding access to information through technology": Mitchell, Above n 33, at [2 and 26].

When employers access employees' CMWC it can contain personal information even sensitive data, for example; marital status, religious belief, ethical belief, color, race, ethnic or national origins, disability, age, political opinion, employment status, family status, and sexual orientation[143]. All of this information is prone to be used to discriminate against the employee. Human rights law has been applied to this issue when dealing with matters of discrimination or when there is a loss of dignity as a result of a Privacy Principle breach.

In *Hammond v Credit Union Baywide*[144] the HRRT set out that "the reasons why the information privacy principles were enacted by Parliament in the Privacy Act. The unrestrained use of personal information can cause devastating, if not irreparable harm to an individual." [145] This case was explained above, and the remedies the Tribunal established are contemplated in the Human Rights Act[146].

The Human Rights Act and its concepts of dignity and injury of feelings were applied by the ERA in *Linnell v Les Mills International Ltd* [147] but in general it has not played a main role. This is despite some cases media coverage (e.g. *Air New Zealand Ltd v Bisson*) posing a threat to an individuals dignity. Furthermore, it is not necessary that the case is covered by the media, the sole fact that disciplinary procedures based on CMWC misuse, involves a group of the employee's coworkers (Human Resources, IT staff, Managers) is enough to humiliate an individual.

Another piece of legislation that addresses human rights is the Bill of Rights [148] however this provision does not included the right to privacy. Petra Bulter explained:

> The absence of a right to privacy in the Bill of Rights Act has led to uncertainty surrounding privacy concerns and how those concerns are to be addressed by the courts. While the courts have not had difficulty in recognising privacy as an important

[143] Human Rights Act 1993 s 21.

[144] *Hammond v Credit Union Baywide,* above n 103.

[145] at [188]

[146] Human Rights Act s 89.

[147] *Linnell v Les Mills International Ltd,* above n 132.

[148] Bill of Rights Act 1990.

> value in the abstract, there has been difficulty in identifying when privacy interests matter, and how they are to be balanced against other rights and interests[149].

To summarize, the lack of dialogue between the privacy and Human Rights framework has led to the implementation to the Anglo-American approach. By not recognizing privacy rights in the Human Rights framework, law-makers are giving it a value equitable to other renounceable rights such as property rights. If employees' privacy is a property right it can be subjugated by employers' property of the networked infrastructure even in cases when dignity may be affected.

V Principles That Should Govern the Electronic Surveillance of Employee's CMWC

As analyzed in the above, in New Zealand employment and privacy law institutions are aligned with the Anglo-American view. Under this approach "workers wave goodbye to their right to privacy as soon as they log onto their workplace computer"[150]. It is feasible to say that New Zealand as a jurisdiction suffers from the same due to its replication of the Anglo American approach when dealing with the issue of employee protection from abusive surveillance at the workplace. Ciocchetti described

> (1) Workplaces exist for work purposes, (2) employers provide technology and pay wages in return for performance and (3) liability issues override the instinct to enhance employee privacy interests[151].

As in United States, in New Zealand this "property-rights approach leaves employees without common law or statutory remedies against abusive monitoring of CMWC"[152]. Research has demonstrated that "U.S. is lagging behind Europe in balancing workplace

---

[149]Petra Butler "New Zealand Journal of Public and International Law Special Issue - 21st Birthday of the New Zealand Bill of Rights Act 1990" (2013) 11 NZJPIL 213 at 245.

[150] Rustad and Paulsson, above n 3, at Abstract..

[151]Ciocchetti, "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring.", above n 95, at 9.

[152] Rustad and Paulssos, above n 3, at 100.

monitoring against the privacy rights of employees"[153]. The difference is that Europe is the protection of employees' human dignity allows a broader scope of action against treating people in intrusive ways[154].

Currently the Privacy Act is being amended, therefore it is now suitable to formulate recommendations regarding electronic surveillance at the workplace in order to protect employees from abusive electronic surveillance. These recommendations if applied would lead to a better systemic response rather than a case by case solution. This section aims to offer a solution that balances both the employees' privacy rights and employers' interests.

A Dignity as an Umbrella based on the European Approach.

"Human dignity means that an individual or group feels self-respect and self-worth. It is concerned with physical and psychological integrity and empowerment"[155]. This link between privacy and dignity has been explored for decades. Edward Bloustein wrote in 1978 that "privacy is so integrally and inextricably linked to personal dignity that it remains an ultimate or final value of tremendous social importance"[156]. In concordance with this, the most widely-recognized values served by protection of privacy break down into two broad categories, those relating to autonomy and democracy, and those relating to dignity and personal wellbeing[157]. The link to the workplace has been acknowledged by the Council of Europe Committee who enacted the Recommendation CM/Rec (2015) which establishes that:

> Respect for human dignity, privacy and the protection of personal data should be safeguarded for employment purposes, notably to allow for the free development of

[153] At 11.

[154] Rothstein, above n 38, at 383

[155] Hammond v Credit Union Baywide, above 103, at [158].

[156] Edward Bloustein "Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory" (1978) 2 GaLRev 429, at 442.

[157] Oliver Hazel "Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out" (2002) 31 IndLJ 321 at 322

> the employee's personality as well as for possibilities of individual and social relationships in the workplace[158].

Recognition of employee's human dignity when dealing with CMWC surveillance has its root (but is not exhausted to this), in acknowledgement of employees as human beings and not merely as a means of production. Rothstein explained that at work, human dignity "is denied by treating the employee as a mere factor of production with capacities and vulnerabilities (…) ignoring both the worker's individuality (…) and human potential (…)"[159]. Especially when in modern societies, "for many people work involves connectivity, immediacy, and a blurring of boundaries between work and non-work"[160]. In alignment with this reasoning, the European Court of Human Rights (EHRT) set out that the ambit of "private life" includes the right to develop relationships with other human beings in activities of a "professional or business nature"[161]. The EHRT added that it is in the professional arena where "the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world"[162]

In general, European communities "employ the notion of human dignity in determining the outcome of workplace monitoring issues"[163]. These countries see monitoring as an intrusion into a person's autonomy or intimacy[164], as emerges from Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace[165]: "the location and ownership of the electronic means used does not rule out secrecy of communications and correspondence as laid down in fundamental legal principles and constitutions." The Canadian Supreme Court has also adopted this concept,

---

[158] Recommendation CM/Rec (2015) 5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (s) 3

[159] Rothstein, above n 38, at 382-383.

[160] See the theory of "The Boundary permeability": Daantje and others, above n 31, at 157.

[161] *Niemietz v Germany* (1992) 16 EHRR 97 (ECHR) at [29].

[162] At [29].

[163] Isajiw, above n 37, at 15.

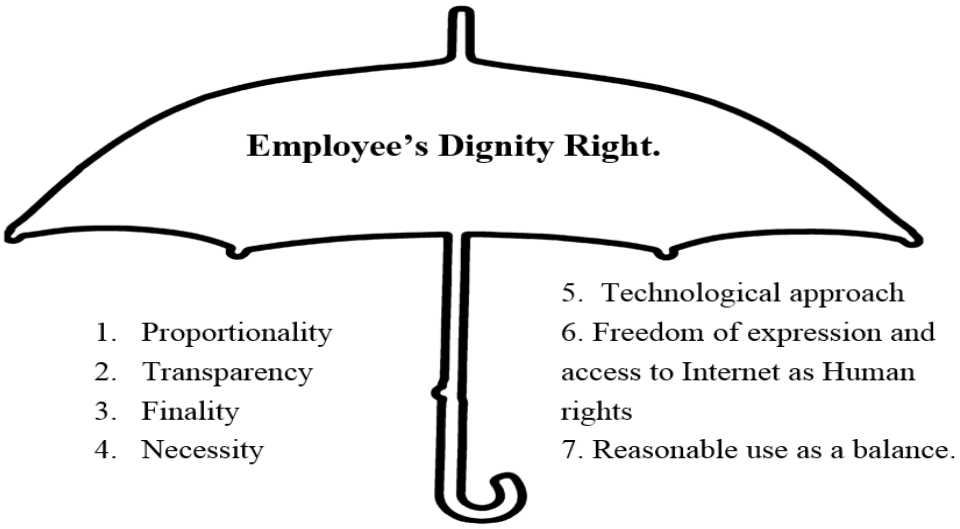
[164] At 15.

[165] Article 29 Working Party *Working document on the surveillance of electronic communications in the workplace* (WP 55, 2001).

asserting the employee's reasonable expectation of privacy over his personal information stored in company-owned equipment.[166]

A human dignity encompassed approach is the central piece or theme of this paper's proposal. Dignity is an umbrella under which the principles that should govern surveillance at the workplace are overarched by. In other words, the primary aim of these principles is to protect the human dignity of employees and balance it with the interests of the employer to achieve their economic goals.

The following data protection principles are derived from the Directive 95/46/EC[167] and should be complied with when considering the processing of personal data that is involved in such monitoring[168]. These principles are considered additional to the principles set out in the Privacy Act 1993, meaning that together they constitute a complete framework to addressing these issues. The next section of this paper is inspired by the European concept that links privacy rights with human rights as oppose to the Anglo American tradition of relating privacy rights to property rights. The image below illustrates this concept:



[166] "While the ownership of property is a relevant consideration, it is not determinative" *R. v. Buhay*, 2003 SCC 30, [2003] 1 SCR 631, at [22]; *R. v. Cole*, 2012 SCC 53, [2012] 3 SCR 34 at [55].

[167] Directive 95/46/EC on Data Protection [1995] OJ L 281//1

[168] At Art 28.

1 Proportionality

Any intrusion into an employee's privacy at work "should be in proportion to the benefits of the monitoring to a reasonable employer, which, in turn, should be related to the risks which the monitoring is intended to reduce"[169]This principle is translated into the following requirements 1. Drafting the policy: The company CMWC policy should be tailor made according to the type of work and the degree of risk, which the particular company and employees position faces.2.Collectiong information: Personal data collected through surveillance should be relevant and not excessive with regard to achieving the purpose specified. 3. Technology proportionality.

(a) Drafting the policy

To date, proportionality has been not fully applied by both the employment and privacy law institutions. In the case of the employment institutions, threshold 103A of the Employment Act establishes "what a reasonable employer would do" when applying disciplinary procedures[170]. However, this test has not as yet been used to measure the actual substantive spirit of CMWC policies. One way to measure the proportionality when drafting a policy is to analyse if the intrusion into employees CMWC corresponds to the final aim of the business. In other words, if this monitoring was not conducted would it place the core purpose of the company at risk? For example, if the company's aim is to achieve high productivity and in actual fact employees are producing favourable results, would it still be a sufficient cause to intrude into their CMWC Personal data collected through surveillance?

(b) Collecting information: Personal data collected through surveillance should be relevant and not excessive with regard to achieving the purpose specified

This principle has to do with the Principle 1 of the Privacy Act[171] and the "reasonableness of the collection" through surveillance. To illustrate this point, a recent and controversial case *Barbulescu V. Romania[172]* addressed by the European Court of Human Rights

---

[169] The Hong Kong Office of the Privacy Commissioner *Privacy Guidelines:Monitoring and Personal data at work* (December, 2004) at [2.1.3] Retrievable <http://www.pco.org.hk.>

[170] Anderson and Hughes, above n 114, at 800.

[171] Privacy Act, s 6.

[172] *Bărbulescu v. Romania* (2016)13 EHRR 29 (Section IV, ECHR)

(ECHR), deals with a workplace without a policy of internet use. In this case Barbulescu was ordered to create a Yahoo Messenger account for business purposes additional to his personal account. The employer surveilled Barbulescu's communication with his fiancé via IM personal and IM professional account and dismissed him on the grounds of using workplace resources for personal purposes. "The employer dismissed him presenting as evidence the transcription of Barbulescu private messages"[173]. Barbulescu then argued that e-mails and IM "were protected by Article 8 of the Convention as pertaining to "private life" and "correspondence"[174].

The ECHR considered that the surveillance was proportionate and within the scope[175]. This paper supports the dissenting opinion by Judge Pablo Pinto de Albuquerque. The Judge explained that the surveillance was disproportionate because the employer not only accessed the corporative account but also the employee's personal account:

> The employer was aware that some of the communications exchanged by the applicant were directed to an account entitled "Andra loves you", which could evidently have no relationship with the performance of the applicant's professional tasks.[176]

A good practice for employers then would be to give employees the option to mark some of their emails as personal, and avoid intrusion into the content. The employees would have a privacy expectation over these emails. Regarding the intrusion of the employer into Barbulescu's personal account, this action is *prima facie* a breach of employees' privacy and even a criminal offence in some jurisdictions. Using the same reasoning to the above case is *Case note 229558*[177] addressed by the Privacy Commissioner in New Zealand.

---

[173] At [7]: "The transcript also contained five short messages that the applicant had exchanged with his fiancée on 12 July 2007 using a personal Yahoo Messenger account; these messages did not disclose any intimate information"

[174] At [36] : "The Court further held that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage".

[175] At [60]

[176] *Bărbulescu v. Romania*, above n 172, at 28 per Judge Pinto de Albuquerque dissenting at [19].

[177] *Case note 229558*, above n 82.

(c) The technology proportionality

Technology, as is stated in the Background of this paper, has itself the capability to increase the Panopticon effect at the workplace[178], an example of this is keystroke software. In order to observe the proportionality of the monitoring the employer should avoid the use of highly invasive technology such as keystroke software[179]. This technology is capable of working without being noticed by the employee. "When employees become aware that their employer is monitoring their computer, either before or after the fact, the negative repercussions on morale and dignity[180].This concept is developed further below when studying the "technological approach".

2. Transparency

Transparency as a principle has to be taken into account before, during and after the surveillance is conducted. After the collection of CMWC information it means that the employer has to provide his workers with a readily accessible, clear and accurate statement of his policy with regard to e-mail and Internet monitoring[181].Basically, it is not enough to comply with this principle merely because the employer has a CMWC policy at the workplace. Some requirements are covered by Principle 3 of the Privacy Act[182] but those are not enough to protect employees. In order to be transparent the policy has to contain the motives, legal and management related to monitor CMWC. The policy has to establish how the surveillance would be done specifying the type of technology used for that purpose

[178] "[U]ser experience and understanding of the technology, both the hardware and software, can impact their perception. For example, the utilization of passwords by some systems may reinforce the notion that the material is protected(…)": Because these Scott D'Urso "Electronic monitoring and surveillance in the workplace: Modeling the panoptic effect potential of communication technology, organizational factors and policies" (Doctor of Philosophy Theses, The University of Texas at Austin, 2004) at 27

[179] "Desktop and keystroke technology can also flag sexually-charged or violently keywords or content traveling over the company network and/or keep track of the number of times an employee hits delete or edits a document": Ciocchetti, above n 96, at [54-55].

[180] At 55.

[181] Article 29 Working Party,above n 165, at 14

[182] Privacy Act, s 6.

(e.g. Blocking specific websites or by alerts)[183]. Additionally, it has to be disseminated among employees, by offering training and E- learning tools that help employees to understand what information may be collected from their CMWC.

This positive practice would require the explicit consent of the employees[184] on a different document from the general employment agreement. In other words, it is not enough to have an Internet usage clause inserted in the employment contract. As is shown in the Background of this paper, employees who experience the Panopticon effect at the workplace may suffer from non-clinical paranoia or lack of self-esteem[185] because they think they are not trusted by the employer. Considering this, it is appropriate to communicate to employees the legal reason (e.g Industry regulatory provisions) why the surveillance is actually being conducted in order to mitigate the impact to those effects by monitoring. Transparency also demands employers to have their policy up to date in accordance with changes in the technology involved and the "scope of nature of the monitoring itself"[186]. Communication of these changes to employees is necessary. After the surveillance is conducted the employer should inform employees if they hold their personal data and what kind of data they hold, this is similar to what Principle 6 of the Privacy Act establishes[187].

3. Finality

[183] In United Estates "Fifty-seven percent of the managers surveyed in the 2001 AMA survey reported that their organization uses "blocking" software to prevent phone calls to restricted or inappropriate phone numbers, and 40% reported blocking of Internet connections to unauthorized or inappropriate websites.":

[184] In the European Union Opinion 8/2001 hold that "consent of workers must be freely given and fully informed and employers should not rely on consent as a general means of legitimising such processing." D'Urso "Electronic monitoring and surveillance in the workplace: Modeling the panoptic effect potential of communication technology, organizational factors and policies", above n 175, at 6.

[185]Regarding self-esteem and the panopticon effect See Jason Snyder "E-mail privacy at the workplace: A Boundary Regulation Perspective", above n 4.

[186] Watt, above n 62, at 147.

[187] Privacy Act, s 6: "(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled (a) to obtain from the agency confirmation of whether or not the agency holds such personal information."

This principle means that data must be collected for a specified, explicit and legitimate purpose and not gathered in a way that is incompatible with those purposes. In New Zealand this aim is covered by Principle 1 of the Privacy Act[188]. It establishes that the agency should have a lawful purpose to collect information. However, as illustrated above this notion is wide and does not offer a complete protection to employees. It would be an ideal paradigm if legal sources established explicitly and exhaustively what is a lawful purpose and not to leave this concept to an employer's discretion.

4. Necessity:

This principle means that the employer must assess if any form of monitoring is absolutely necessary for a specified purpose before proceeding to engage in any such activity[189]. The Working Party summarizes this principle in one question "Is it necessary? Could the employer not obtain the same result with traditional methods of supervision?"[190] For example, when employers argue that one of the objectives of conducting surveillance is productivity they should be able to demonstrate that productivity has not been achieved or was put on risk.

5. Technological approach

As presented in the Background of this paper, Technology has the capability itself to create the potential detrimental effects of the Panopticon. Therefore law sources should take into account the invasiveness level of some software like keystroke used to monitor employees. In other words, the issues of electronic surveillance is not only managed by enacting rules but also by adjusting the technology involved in this process to consider the employee's privacy interest.

This principle is closely related to proportionality and aims to restrict the excessive intrusion of electronic means into employees CMWC. The key of this principle is that technology is less invasive when it works on a prevention basis (blocking access to sites

---

[188] Section 6.

[189] Article 29 Working Party, above n 165, at 13

[190] At 4

by using firewalls)[191] rather than on a correctional one (monitoring all usage to be reviewed if misconduct suspected). For example, new technology such as "Access Panels" is relatively harmless towards employees' privacy. "These devices cannot sift through personal e-mails or listen in on private phone calls. They collect information on comings and goings and allow/disallow access"[192].

Hong Kong, whose position "may be a case of human rights protections making up for a lack of employment protections"[193] recognized this principle. The Privacy Commissioner of Hong Kong wrote a guide to offer "Alternatives to employee monitoring" and set out that "before committing to employees' monitoring, employers are strongly encouraged to give careful consideration to technology alternatives less privacy intrusive"[194]. The Commissioner suggest some technology options that are more "privacy friendly", for instance:

a. If the employers are worried about protecting its system against viruses and electronic threatens: The employer should consider " the installation of appropriate Virus checking software that enable employers to detect suspect messages without having to resort to opening and reading the contents"[195]
b. If the employer is interested in restricting downloading offensive or salacious material from internet there is "filter software" that helps employers to block all material and receive an alert when an employee intends to do it.
c. When companies are interested in preventing the disclosure of confidential information, there is software that detects some important words and phrases on employers command and gives the company alerts.

All of these mechanisms, and other technologies, have enough capability to minimize the need for surveillance.

---

[191] "Filters and firewalls not only prevent outsiders from gaining access to an employer's system - they also can be used to prevent employees from accessing information or Web sites unrelated to work. This firewall is designed to make employees more productive and stop non-work related activities during work hour": Ciocchetti, above n 96, at 25.

[192] At 40.

[193] Paul Roth "Privacy law reform in New Zealand: will it touch the workplace?" above n 68, at 4.

[194] The Hong Kong Office of the Privacy Commissioner, above n 169, At [2.1.3]

[195] At [2.3.1]

6. Freedom of expression and Access to the internet as a human right.

Freedom of expression is a fundamental human right enshrined in the New Zealand Bill of Rights Act 1990[196]. The Act specifies that this right "may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." On the other hand, access to the Internet is not yet recognized as a Human Right in New Zealand, although there has been some attempts to establish "Rights on the Internet"[197] it has not been accomplished.

The human dignity approach recognizes that freedom of Expression cannot be protected without protecting the means to exercise the right, which in the digital era is the Internet[198]. In Accordance with this reasoning, "user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression"[199]. Thus "the obligation to promote freedom of expression is coupled with the obligation to protect the right to respect for private life"[200]

Lastly, this paper is aligns itself with the Chief Human Rights Commissioner's view. In a recent speech he stated that:

> The Human Rights Commission will do everything it can to ensure New Zealanders know their human rights and responsibilities and to ensure that freedom of expression is protected. It is time to make sure that our government surveillance programs and businesses operating surveillance based business models are fit for the purpose of protecting our freedom and not eroding it. [201]

---

[196] Bill of Rights Act 1990.

[197] Gareth MP Hughes "Internet Rights and Freedoms Bill" Green Party of Aotearoa New Zealand <https://home.greens.org.nz/misc-documents/internet-rights-and-freedoms-bill>

[198] *Recommendation on measures to promote the public service value of the Internet* CM Rec16 (2007).

[199] *Bărbulescu v. Romania*, above n 172, per Judge Pinto de Albuquerque dissenting at [16].

[200] At 17.

[201] David Rutherford, Chief Human Rights Commissioner "Freedom of expression underpins NZ way of life" <https://www.hrc.co.nz/news/freedom-expression-underpins-nz-way-life/>

7. Reasonable use.

One of the expressions of the Anglo-American view is that what is in the work computer belongs to the employer, and if the employer has an e-mail and Internet policy forbidding all personal use, he can inspect any content on a laptop as well[202]. Policies that forbid all personal use are acceptable under this approach. To exemplify this point, the case of *Toleafoa v Vodafone*[203] was discussed in section IV (B) of this paper. The Internet policy stated "all messages generated on company systems were the property of Vodafone"[204]. The employee's breach of this policy by sending personal emails, among other reasons, was the argument that was the basis of the employee's dismissal.

Under a Dignity-Based approach, policies establishing that all messages generated on company system are property of the employer are no longer sustainable. The working party explained that blanket prohibition on personal use of the Internet at the workplace may be "considered unrealistic as it fails to reflect the degree to which the Internet can assist employees in their daily life"[205]. In *Société Nikon France SA v M. Frederic*[206] the Court of cassation in France, held that an employer had no legal right to intercept and read personal e-mails "even if the employer supplied the computer and expressly provided that employees were not to use their computers for personal e-mail or Internet uses"[207].

Clauses that provide control of the CMWC exclusively to the employer neglect the fact that employees are human beings with personal interests. These interests may include maintaining personal relationships through communication. Additionally, it ignores the fact that New Zealanders work longer hours than the average of their peers in other

---

[202] Rustad and Paulsso, above n 3, at 94.

[203] *Toleafoa v Vodafone*, above n 119.

[204] At [46]

[205] Article 29 Working Party, above n 165, at 24.

[206] *Société Nikon France SA v M. Frederic* Cour de cassation [French Court of Cassation] 4164, 2 October 2001 reported in (2001) JTL n OIN211CC.

[207] At [3].

developed countries[208] and therefore spend more time at the workplace and have less time to attend to personal matters. Thus, "the path of online electronic surveillance law should strive for a balance between the employers' need to know and the right of employees to maintain a zone of privacy"[209].

V Conclusion.

Technology has radically changed the dynamics of the workplace, where average employees spent most of their time. In this present time of information age, even if employees are not at work technology such as smartphones and portable devices blurs the boundaries between their home and work life[210]. This fact accompanied by the demographic phenomenon of the Generations Y (born in the 80s') entering into the workforce, represents a change for organizations' climate worldwide[211]. Employees are reachable wherever or whenever. They are more techno-savvy[212] and hold a greater percentage of their interactions via CMWC.

At the workplace the employer is interested in achieving productivity goals and provides the resources (technology) to employees. This among other interests leads to companies monitoring employees' CMWC. Technology has now a second role, providing employers with multiple tools that allow them to retrieve employees' daily activity, every key stroke, every email or website visited. When surveillance is conducted invasively or in darkness the effect on the employee's morale can be devastating. This paper presented some applicable sociological theories like Non Clinical Paranoia. This theory established that the meta-message employees receive when they are under an invasive electronic monitoring (e.g Keystroke software) is basically that they are not trustworthy and need to be surveilled. The outcome of this in a workplace environment is the employee's lack of self-esteem and self-value.

---

[208] Paul Conway and Lisa Meehan *Productivity by the numbers: The New Zealand experience* (New Zealand Productivity Commission "Research Paper" September 2013) at 25; Staff Reporter "Kiwis work longer but produce less" *The New Zealand Herald* (online ed, Auckland,14 september 2013).

[209] Rustad and Paulsson, above n 3, at 101

[210] See Daantje and others , above n 31.

[211] See Mitchell, above n 33.

[212] At 38.

It is therefore pertinent to quote the principle of "mere means" by Kant which explains that human beings are rational beings, and should be treated "as ends-in-themselves" means respecting their rationality. Thus, we may never manipulate people or use people to achieve our purposes, no matter how good those purposes may be[213]. This is in brief the concept of Human Dignity.

Unfortunately in New Zealand dignity is a value that is not linked to privacy at the workplace. Legal sources in New Zealand place privacy rights alongside property rights. This is similar to the Anglo-American approach where rights can be changeable and renounceable for a wage. In other words, legislative and judicial bodies have failed to recognize that "workers do not abandon their right to privacy and data protection every morning at the doors of the workplace"[214]nor their dignity.

Although an employer's economic interests should be protected, employees as human beings cannot be valued less than a company's laptop. Dignity respect and a reasonable personal use policy for employees' CMWC will humanize the workplace while protecting the employer interests. A systemic change is required to provide remedies for cases of employer abuse in electronic surveillance. This is only the first step in developing an employment legal framework that respects employees' Human Rights.

[213] James Rachels *The Elements of Moral Philosophy* (4th ed, Mc Graw Hill, New York, 1986) at 114.

[214] Article 29, above n 165, at 24.

VI BIBLIOGRAPHY

PRIMARY SOURCES

A Cases

1 New Zealand

Air New Zealand Ltd v Bisson EmpC Christchurch CC6A/05, CRC6/05, 17 June 2005
Allerton v Methanex [2000] 1 ERNZ 242 At 25
Armfield v Naughton [2014] NZHRRT 48, (2014) 9 HRNZ 808
Hall v Dionex pty LTD [2015] NZEmpC 29
Hammond v NZCU Baywide [2015] NZHRRT 6.
Harder v Proceedings Commissioner [2000] 3 NZLR 80, (2000) 6 HRNZ 173
Hook v Stream Group (NZ) Pty Ltd [2013] NZEmpC 188
Lehmann v Canwest Radioworks Limited Decision No 35/06, 21 September 2006 (Human Rights Review Tribunal)
Linnell v Les Mills International Ltd [2012] NZERA Christchurch 64
Safe Air Ltd v Walker EmpC Christchurch CRC 8/09 CRC 10/09 4 December 2009
Toleafoa v Vodafone New Zealand Ltd [2011] NZERA Auckland 488
Case Note 229558 [2012] NZPrivCmr 1.

2 Canada

R. v. Buhay, 2003 SCC 30, [2003] 1 SCR 631
R. v. Cole, 2012 SCC 53, [2012] 3 SCR 34

3 France.

Société Nikon France SA v M. Frederic Cour de cassation [French Court of Cassation] 4164, 2 October 2001 reported in (2001) JTL n OIN211CC.

4 European Court of Human Rights

Mauer v Austria (1997) 25 EHRR 91 (ECHR)
Bărbulescu v. Romania (2016) 13 EHRR 29 (Section IV, ECHR)
Niemietz v Germany (1992) 16 EHRR 97 (ECHR)

B Legislation

1 New Zealand

Employment Relations Act 2000.
Privacy Act 1993.
Criminal Act 1961.
Human Right Act 1993.

2 Austria

Arbeitsverfassungsgesetz [Federal Law Gazette 1974] (Austria)

3 Spain

El Estatuto De Los Trabajadores 1980 [Labor Act 1980].

4 United Estates

Electronic Communications Privacy Act of 2000 18 USC § 2515.

C International instruments

Article 29 Working Party *Working document on the surveillance of electronic communications in the workplace* (WP 55, 2001).

Directive 95/46/EC on Data Protection [1995] OJ L 281//1

European Convention on Human Rights 213 UNTS 22.

International Covenant on Civil and Political Rights 1966 (ICCPR).

Recommendation of the Council of the Organisation for Economic for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy an Transborder Flows of Personal Data" (OECD Guidelines).

Recommendation CM/Rec (2015) 5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.

Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

D Official Documents

1 New Zealand

Law Commission *Review of the privacy act* (NZLC R123, 2011)

Roger Procter *Enhancing Productivity: Towards an Updated Action Agenda (*Ministry of Economic Development, Occasional Paper 11/01, March 2011).

Paul Conway and Lisa Meehan *Productivity by the numbers: The New Zealand experience* (New Zealand Productivity Commission "Research Paper" September 2013)

The Office of the Privacy Commissioner. *Privacy At Work: A Guide To Privacy Act to Employers* (2008) Retrievable from https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf

2 Italy

The Garante per la protezione dei dati personali [Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 March 2007]

3 Hong Kong

The Hong Kong Office of the Privacy Commissioner Privacy Guidelines:Monitoring and Personal data at work (December, 2004) Retrievable <http://www.pco.org.hk.>

SECONDARY SOURCES

E Books

Aaron Crawford, Raymond Harbridge and Pat Walsh *Privacy in the workplace: the effects in the Privacy Act 1993 on Employment practices in New Zealand* (Victoria University of Wellington, Wellington, 1995).

Gordon Anderson and John Hughes *Employment Law in New Zealand* (2014 ed LexisNexis Wellington, 2014).

James Rachels *The Elements of Moral Philosophy* (4th ed, Mc Graw Hill New York, 1986).

M. P. Mack *A Bentham reader* (Pegasus, New York, 1969).

Noel Cox *Technology and Legal Systems* (Ashgate Publishing, Ltd, Hampshire 2006).

Phillippe Nonet, Philip Selznick *Law and Society in Transition: Toward Responsive Law* (2d ed, Transaction Publishers, New Jersey , 2009).

Richard Stanley Rudman *New Zealand Employment Law Guide* (2014 ed, CCH New Zealand, Auckland, 2014).

F Chapters in books

Robin Cooke "Tort and Contract" in Andrew Butler (ed) *Essays on Contract* (Law Book Company, Sydney, 1987) 222

Carl Botan and Mihaela Vorvoreanu "What Do Employees Think about Electronic Surveillance at Work? " John Weckert (ed) *Electronic Monitoring in the Workplace: Controversies and Solutions* (Idea Group Inc (IGI),London, 2005) 135

G Journals

Blake E Ashforth, Glen E Kreiner and Mel Fugate "All in a day's work: Boundaries and micro role transitions"(2000) 25(3) ASJC 472

Carl Botan "Communication work and electronic surveillance: A model for predicting panoptic effects " (1996) 63 Communication Monographs 293

Edward Bloustein "Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory" (1978) 2 GaLRev 429.

Petra Butler "New Zealand Journal of Public and International Law Special Issue - 21st Birthday of the New Zealand Bill of Rights Act 1990"(2013) 11NZJPIL213

Corey Ciocchetti "The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring." (2011) 48.2 AmBusLJ 285

Rebecca M Chory and others "Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses " (2015) 28(1) ER&RJ 23

Derks Daantje and others " Smartphone use and work–home interference:The moderating role of social norms and employeework engagement" (2014) 88 JOccupOrganPsychol 1

Linda Duxbury Christopher Higgins, Rob Smart, "Mobile technology and boundary permeability. "(2014)25 Brit J Manage 570

Karen Eltis "The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Case law in Canada and Israel: Should Others Follow Suit?" (2003) 56 Mcgill LJ 289

Larry O Gantt "Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace" (1994) 8 (2) Harv. JL & Tech 345

Oliver Hazel "Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out" (2002) 31 IndLJ 321

Peter J Isajiw "Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers" (2001) 20 TempleEnvtlL& TechJ 73

RM Kramer "Organizational paranoia: Origins and dynamics" (2001) 23 ResOrganBehav 1

Karen K Myers and Kamyab Sadaghiani "Millennials in the Workplace: A Communication Perspective on Millennials' Organizational Relationships and Performance" (2010) 25 JBusPsychol 226.

Sandra Petronio "Translational research endeavors and the practices of communication privacy management" (2007) 35 JACR 218.

Abdelbaset Queiri and Others "Generation-Y Employees' Turnover: Work-Values Fit Perspective" (2014) 9 IJBM 199

B H Raven " The bases of the power : Origins and recent developments " (1993) 49 JSI 227.

Michael L Rustad and Sandra R Paulsson "Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe" (2005) 7 UPaJIntlBus L 1

Lawrence E Rothstein " Privacy or. Dignity?: Electronic Monitoring in the Workplace" (2000) 19 NY SchJIntl&Comp L 379

Jason Snyder " E-mail privacy at the workplace: A Boundary Regulation Perspective (2010) 47 JBC266

Brian Tamanaha "A Vision of Social-Legal Change: Rescuing Ehrlich from "Living Law" (2011) 36 L&SocInquiry 297

Myria Watkins Allen, Kasey L. Walker "Workplace Surveillance and Managing Privacy Boundaries "(2007) 21 MCQ 172

H Unpublished papers.

Scott D'Urso "Electronic monitoring and surveillance in the workplace: Modeling the panoptic effect potential of communication technology, organizational factors and policies" (Doctor of Philosophy Theses, The University of Texas at Austin, 2004)

Daisy A Mitchell "Generation y information technology employees in the workplace: a qualitative study on how leadership motivates creativity and retention " (Doctor of Philosophy, Theses Capella University, 2015)

Marcus Roberts "Reforming New Zealand's Legislative Council: A Study of Constitutional Change, 1891 and 1912–1920" (LLB (Hons) Dissertation, University of Auckland, 2008.

James Watt "Electronic workplace surveillance and employee privacy: a comparative analysis of privacy protection in Australia and the United States" (LLM Thesis, Queensland University of Technology, 2009).

I Conferences

Paul Roth "Privacy law reform in New Zealand: will it touch the workplace?" (Presented to Third Biennial Labor Law Conference of the New Zealand Labor Law Society in Otago Universiy Dunedin , 2015).

Paul Roth "Privacy in the workplace" (Presented to Labour, Employment and Work in New Zealand Wellington,1994).

J News Papers

NZPA "Air NZ to appeal decision on employees' internet use" The New Zealand Herald (online ed, Auckland, 4 jul 2006).

Audrey Young"Entire NZ China trade board resigns" The New Zealand Herald (online ed, Auckland, 24 June 2011).

Staff Reporter "Kiwis work longer but produce less" The New Zealand Herald (online ed, Auckland, 14 September 2013).

K Internet.

Brittany Persen "Employee Monitoring: It's Not Paranoia—You Really Are Being Watched! (26 May 2008) PcMag <http://www.pcmag.com >

Charles Mabbett "Record damages awarded for cake photo breach" (2 March 2015) The Privacy Comissioner <https://www.privacy.org.nz/blog/cake-privacy-breach/>

Gareth MP Hughes "Internet Rights and Freedoms Bill" Green Party of Aotearoa New Zealand <https://home.greens.org.nz/misc-documents/internet-rights-and-freedoms-bill>