63 *ALSB Journal of Employment and Labor Law*
Volume 11, No. 1, 63 – 103, Winter 2009

# Dignity in The Workplace: An Enquiry Into the Conceptual Foundation of Workplace Privacy Protection Worldwide

by

Avner Levin*

## Introduction

Perhaps you are a parent to a small child, and perhaps your child is in daycare. You would probably appreciate the ability to check on your child during the day, for example by accessing a video camera through a website established by the daycare. Suppose now that you work as an early childhood educator. How would you perceive a camera that monitors you constantly and broadcasts your images via the world-wide-web? Is such monitoring the prerogative of the employer? Are employees precluded from protesting such, and other, devices that appear to invade their privacy? Is there a concept of privacy for employees, and if so, what is its conceptual basis? These are all questions with which employees, employers, legislators and the courts are wrestling with in a number of jurisdictions around the world.

The child-care monitoring scenario is of course not hypothetical. Many parents have monitored their children, at home with their care-givers, via what are now generically called 'nanny-cams'. And the scenario is not hypothetical with respect to other child-care providers as well. Whether for-profit or not-for-profit, private or regulated, such monitoring is already available at many child-care centers. Monitoring employees of course is not limited, nor did it begin, in the child-care sector or with the development of new technology such as web-cams. Employers have always had an obvious economic interest in ensuring employees work for their pay, and have always had a variety of monitoring techniques at their disposal, from human supervisors to punch clocks. Contemporary monitoring takes these and a variety of additional new forms, from software installed on computers to track key-strokes and internet access, to geographical positioning systems (GPS) located in vehicles such as delivery trucks or police cars, to biometric measures, to radio frequency identifiers (RFID) implanted in employees and GPS implants as well. It would seem, however, that the advent of new technology has not only added to the arsenal of monitoring tools at the employer's disposal. It has significantly changed the nature of monitoring so that arguably legal doctrines that were sufficient to regulate monitoring are no longer up to the task.[1] Telephone calls, for example, have been monitored by employers in a variety of ways ranging from supervisors listening in, to continuous recording, to a log of numbers called, depending

* Associate Professor, Ted Rogers School of Management, Ryerson University.

[1] Some of the ways in which it is argued that monitoring has changed thanks to developments in technology are that it is easier to collect, use and process data (initially often even for non-monitoring purposes) and that it is now technologically possible to survey all employees all the time, in an imperceptible manner. See Mark Jeffery, *Information Technology and Workers' Privacy: A Comparative Study: Part I: Introduction*, 23 COMP. LAB. L. & POL'Y J. 251 (2002).

on the industry and position of the monitored workers.[2] With the introduction of new telephone technology, such as Voice Over Internet Protocol (VOIP), forms of monitoring that employers have only been able to use with respect to particular workers (mainly due to associated costs) will now be easily and readily available with respect to all workers.[3] As VOIP is phased in to workplaces, workers fear they will find their privacy, in the area of telephone conversations, phased out, unless existing case law with respect to telephone monitoring will be successfully modified to address such newly created privacy concerns. A conceptual basis for such concerns is required, one that will withstand technological changes.

It has long been argued in North American jurisprudence that such an adequate basis is to be found in the idea of reasonable expectations. Worker privacy is based on the reasonable expectation of privacy that workers have in the workplace. Where no reasonable expectation exists then no privacy exists, and where some reasonable expectation of privacy exists then some measure of privacy should be protected by the law. The idea that employees have, or should reasonably have, no expectation of privacy in the workplace is ubiquitous and obviously a useful tool in the hands of employers. It resonates well with the US tort of Intrusion of Seclusion and with Fourth Amendment jurisprudence, which constructed the test of reasonableness with respect to the activities of the US government against its subjects,[4] a test which has been logically extended to the workplace of public employees,[5] and which would seem to equally apply (the test, not the constitutional protection) to the private sector workplace as well. Significantly, the test whether workers, and individuals in general, enjoy a reasonable expectation of privacy is decided not only by examining the expectations of society in general in a particular situation (e.g., do members of society expect video surveillance inside washrooms), sometimes termed the 'objective expectations', but by examining the specific expectations of the individual in the particular situation in question (e.g., would the worker, given a bulletin circulated by the employer to all workers informing them of the new cameras installed in their washroom, expect privacy in that location), sometimes termed the 'subjective expectations'. No reasonable expectations of privacy can exist where no subjective expectations of privacy have existed to begin with.[6]

---

[2] A worker at a customer service call centre is probably subject to continuous monitoring and recording. Other employees may not even be aware that their calls are monitored in some way until they are presented with, and asked to account for, that long-distance call made from their extension…

[3] For a discussion of the legal implications of VOIP see Peter Swire, *Katz is Dead. Long Live Katz*. 102 MICH. L. REV. 904, 911-912 (2004).

[4] Katz v. United States, 389 U.S. 347 (1967). For a critique of the opinion that *Katz* should best be understood as establishing a 'reasonable expectations' test, and that perhaps better privacy protection could be achieved by legislative means see Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution* 102 MICH. L. REV. 801 (2004) as well as the ensuing discussion in Swire, *supra* note 3, Sherry Colb, *A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures,* 102 MICH. L. REV. 889 (2004) and finally Orin Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire,* 102 MICH. L. REV. 933 (2004).

[5] O'Connor v. Ortega, 480 U.S. 709 (1987).

[6] Katz, *supra* note 4, 361. For some differences between the tort law construction of reasonable expectations and the constitutional construct, see Lior Strahilevitz *A Social Networks Theory of Privacy,* CHI. L. & ECON. PAPER NO. 230 (Working Paper, 2004), 13-14, available at http://ssrn.com/abstract=629283.

However, the idea of employees enjoying only reasonable expectations of privacy, and the elasticity of the notion of reasonable expectations as subject to easy change by means of technological changes and subsequent unilateral employer notifications, as could be assumed that will be done in the context of VOIP for example, raise questions whether it is the appropriate concept to govern the analysis of privacy in the workplace. Interestingly, when the judges of the Ninth Circuit were informed that key-monitoring software has been installed on their computers they rose as one to rebel and demand its removal.[7] The existing legal doctrines that would impart great significance to the fact that the judges should have had no reasonable expectation of privacy in state-owned computers, certainly once they were informed of the software's presence, seemed to play little if no role in the judges' reaction. Rather, it seemed to have been motivated by the judges' sense of dignity, self-respect, and the feeling that these important attributes have been violated. Evidence, some anecdotal, as this story from the Ninth Circuit, and some more strongly empirically based, as discussed below, seems to indicate that such other concepts might be equally useful, if not more so.

This paper examines one such concept as a basis for privacy in the workplace, the notion of dignity.[8] I will first discuss dignity and its implications for the idea of privacy. Dignity has been offered (in North America) and largely already exists (in Europe) as a conceptual foundation for the employment relationship in general. The dignity of workers will therefore be the topic of the second section of this paper. In the third section, I will shamelessly capitalize on excellent comparative work already done on workplace privacy protection across many jurisdictions worldwide. Finally, the paper concludes whether, on the basis of the comparative work done, dignity is a concept that illuminates workplace privacy, and if so, to what extent. I begin, therefore, with an examination of dignity as a conceptual basis for privacy.

## Privacy as the Protection of Dignity

The idea that privacy protection is essentially the protection of an individual's dignity (whether worker or not) is not a novel idea,[9] although it has yet to curry favor in the eyes of some of the more prominent contemporary privacy scholars.[10] An individual, and specifically an employee's, privacy, can be violated in many different ways (some of which are mentioned above) and can correspondently enjoy the protection of distinct sources of law such as a constitution, the common law (e.g., tort law) and legislation (e.g.

---

[7] Andrew Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions,* 65 L. & CONT. PROB. 125, 128 (2002)

[8] Building upon the work of (among others) Lawrence Rothstein, *Privacy or Dignity: Electronic Monitoring in the Workplace,* 19 N.Y. J. INT'L. & COMP. L. 379 (2000) and Peter Isajiw, *Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Propriety Interests of Employers,* 20 TEMP. ENVT'L. L. & TECH. J. 73 (2001) that will be discussed in greater detail below.

[9] See e.g., Rothstein, Isajiw, *supra* note 8.

[10] For example Daniel Solove has recently proposed a taxonomy of privacy in which the notion of dignity does not play a major role ('dignitary harms', which privacy protects from, are mentioned however.) Daniel Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477 (2006). On the other hand, see Robert Post, *Three Concepts of Privacy*, 89 GEO. L. J. 2087 (2001) and more recently Dan Burk, *Privacy and Property in the Global Datasphere,* MINN. LEG. ST. RES. PAPER NO. 05-17 (Working Paper, 2005), available at http://ssrn.com/abstract=716862.

information protection statutes).[11] Discussions of privacy are therefore often conducted according to the respective areas of law which govern the different forms in which privacy can be violated. In Canada, for example, federally regulated employers may not use the personal information they hold on employees for purposes other than for which it was collected (with limited exceptions) according to federal legislation.[12] Other Canadian employees, depending on the province in which they work (as will be discussed in greater detail below) do not enjoy such statutory protection, although, as all other Canadians, they enjoy constitutional protection from unreasonable searches, which may apply in certain circumstances (e.g., to employer actions required by law) to such employer actions as video surveillance.[13] Finally, a specific tort addressing the invasion of privacy does not yet exist in Canada, and so Canadians, and by extension employees cannot commence private legal action against their employers for invasion of privacy.[14]

Such discussions typically miss out, however, on factors that are common to all these examples of privacy invasion and tend to focus instead on other issues, such as whether a particular form of privacy invasion (e.g., neighbors spying on neighbors with binoculars) is subject to the law or not. I will attempt here, however, the opposite – to discuss privacy in terms of a conceptual basis – dignity – that would be common to invasions of privacy in an employment relationship context regardless of the many forms these invasions may take, and the different areas of law under which they may fall.

An analysis attempting to determine such a conceptual basis for privacy attempts, actually, to answer the following question: What societal value(s) is protected by means of the protection of privacy? Such an analysis assumes therefore that privacy is, at best, a secondary good, serving values of more importance, and although it is important to take note of this assumption it is important to note as well that as such it is uncontroversial. Few doubt, in other words, that privacy, an important value as it may be, ultimately serves other, more important values. I have chosen to focus on one such value, the notion of dignity, yet there are of course others, such as for example liberty (i.e., freedom from government) or autonomy.[15] Interestingly, and this observation will hopefully become clearer as a result of the examination of employment privacy protection in several jurisdictions below, it seems that by and large jurisdictions focus on different values as being the most prominent ones to be protected by privacy. For example, American privacy protection seems to focus on protecting liberty, while European privacy protection seems to focus on protecting dignity.[16] Similarly, different areas of law protecting from specific forms of privacy invasions seem to base that protection on the particular values that privacy serves. For example, legislation protecting information is

---

[11] See Solove, *supra* note 10.

[12] Personal Information Protection and Electronic Documents Act (PIPEDA), Schedule 1, Principle 4.2.4

[13] Canadian Charter of Rights and Freedoms, § 8.

[14] Although some Canadian provinces (e.g., British Columbia) have enacted legislation to allow for private legal action for invasion of privacy.

[15] For a detailed list, see Ronald Leenes & Bert-Jaap Koops, *'Code' and Privacy or How Technology is Slowly Eroding Privacy, in* ESSAYS ON THE NORMATIVE ROLE OF INFORMATION TECHNOLOGY, (L. Asscher ed., 2005). The authors discuss the protection of personal information through technology. See also *infra* note 17. For an interesting discussion of privacy and other values, in the context of South African law, see J. Neethling, *The Concept of Privacy in South African Law,* 122 SALJ 18 (2005).

[16] For more on this comparison see Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground,* 2 UOLTJ 357 (2005); James Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L. J. 1151 (2004).

largely justified as the manifestation of the value of autonomy, by putting control over such information largely in the hands of the individuals to which it relates.[17] I will argue therefore that in the area of employment, largely regardless of jurisdiction, the protection of the secondary social value of privacy serves to protect the more fundamental value of dignity. Throughout the discussion it will therefore also be useful to keep in mind that, as a fundamental value, dignity is susceptible to harms by means other than privacy, and that some privacy invasive measures may harm dignity directly and not only through their invasion of privacy.[18]

The origins of the idea that privacy protection is the protection of dignity can be traced back to the seminal article by Brandeis and Warren, "The Right to Privacy".[19] Brandeis and Warren's article, perhaps due to its title, has been widely used to advance the argument that a constitutional right to privacy exists in the U.S., and what appears at times to be forgotten is that Brandeis and Warren were actually discussing the emergence of the tort of the invasion of privacy, and arguing that European Aristocracy (i.e., the celebrities of the time) should be allowed their privacy (their "right to be let alone") in an era when new media were popularly perceived to erode this privacy and consequently the majesty and status of the Aristocracy to a level where, heavens forbid, commoners might be confused to think themselves and the Upper Classes one and the same. The battle of the Aristocracy to protect their lives from prying eyes has no end in sight, and neither does the battle of their contemporaries, celebrities in general.[20] The justification for such privacy protection has been, since the beginning of these battles, that it protects the dignity of the besieged individuals, their sense of self-worth, their social standing, their reputation, their desire to avoid scrutiny, their desire to avoid unnecessary humiliation and their identity.

Understood and defined in such a manner dignity is first and foremost a social value, conceptually distinct from other values that privacy may protect, such as an individual's liberty (mentioned above, which can be understood to be in its essence a political value). To protect dignity is to protect a certain social status, a certain image of an individual that society holds. The protection of dignity consequently is the enforcement of certain relevant social norms.[21] Therefore, an individual's dignity does not necessarily suffer from government actions as much as it potentially suffers from the thoughts and perceptions of other members of society, and if the goal of privacy protection is ultimately the protection of dignity, then it is clear that privacy must be

[17] In jurisdictions where such legislation is largely absent, such as the US, attempts have been made to justify personal information protection on other concepts, by treating personal information as property and therefore a commodity to be sold on the 'information market'. See Paul Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055 (2004) as well as Jerry Kang & Benedikt Buchner, *Privacy in Atlantis,* 18 HARV. J. L. & TECH. 1 (2004) for a discussion of property and dignity as alternative foundations for personal information protection. Another suggestion has been to analyze privacy through social networks theory. See Strahilevitz, *supra* note 6.

[18] That is why some, e.g., Rothstein *supra* note 8, prefer to distinguish between privacy and dignity, arguing that workers will be better served by an emphasis on dignity, rather than privacy, in the workplace.

[19] Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[20] See e.g., Princess Caroline of Monaco's battle in Mark Thomson & Hugh Tomlinson, *Bad News for Paparazzi – Strasbourg has Spoken,* 154 UKNLJ 1040 (2004).

[21] This status, and these norms, may vary of course from one society to another.

protected within society first, and from government later.[22] To some degree of course, an erosion of liberties will result ultimately in the erosion of dignity, and to that extent government intrusions will be worrisome even for those concerned primarily with the protection of dignity. Certainly for Europeans, having suffered abuse at the hands of totalitarian governments through World War II and the ensuing Cold War, such concerns are never far from their mind. But for societies concerned with dignity the activities within society are potentially more problematic than the activities of the governing regime. When Brandeis and Warren were writing it was widely held, particularly in Europe, that such notions were of importance, and indeed only existed, with respects to the Aristocracy. Significantly, it has been Europe and its privacy protection regime that has been greatly instrumental in extending the notion of dignity from a value that is of importance only to some members of society to a value which is in essence a fundamental human right.[23]

The primary legal source that indicates that dignity enjoys such an esteemed status in Europe is the draft of the European Constitution.[24] Although at this time the political future of the constitution is in doubt and its ratification has been put on hold, the bone of political contention does not lie in those sections of the constitution that enshrine European human rights. It is therefore unlikely that dignity will lose its constitutional status in the upcoming constitutional revisions that will no doubt occur. The current draft of the European Constitution states that the EU is founded on the value of human dignity:

> The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.[25]

Further, the Constitution states that the EU's Charter of Rights is founded on the value of human dignity:

> Conscious of its spiritual and moral heritage, the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity; it is based on the principles of democracy and the rule of law.[26]

The Constitution devotes an entire Title within that Charter to dignity.[27] Last but not least, the EU Charter of Rights devotes a Title to Solidarity, and within that Title the right of workers to dignity is enshrined as well:

---

[22] Europeans accept government intervention as necessary for dignity protection in other areas as well, such as the regulation of forenames and surnames. Americans, and by and large Canadians, find the very idea incomprehensible. See Whitman, *supra* note 16, at 1215-1219.

[23] I should note that dignity is perceived as a human right in other jurisdictions as well. For example, South Africa, whose Constitution bases the rights it provides for on the fundamental value of human dignity in Section 1. The South African Constitution has been touted, in turn, as model for Scottish law. See Hector MacQueen, *Protecting Privacy*, 8 EDINBURGH L. REV. 248 (2004).

[24] Strictly speaking the draft is not a source of law. However, I thought it informative to examine the draft and its contemporary understanding of dignity on the assumption that it will become ratified, rather than rely solely on the current EU sources, such as the European Convention on Human Rights.

[25] EU Draft Constitution, § I-2: The Union's Values. For the draft version see http://europa.eu.int/constitution/en/lstoc1_en.htm.

[26] EU Draft Constitution, Preamble to Part II.

> Every worker has the right to working conditions which respect his or her health, safety and dignity.[28]

Once the Constitution is finally ratified and adopted by European Member States it is foreseeable that the protection of employee privacy will be primarily based on this worker-right-to-dignity, but it is equally important for the purposes of this paper to remember that the EU Constitution was drafted not only with the aim of setting human rights for future EU citizens and residents, but also on the basis of the established European consensus with respect to human rights. In other words, the right of workers to dignity, and consequently to privacy, already exists in Europe.[29]

Within this consensus there are of course distinctions between the Member States themselves, and even within Member States. For instance, privacy, as personal information protection, is understood somewhat differently within Great Britain, by England and Scotland. Although in terms of personal information both England and Scotland are subject to the same Data Protection Act which implements the EU Privacy Directive, and both England and Scotland are subject to the same Human Rights Act, which implements the European Convention on Human Rights and Article 8 in particular,[30] the two jurisdictions do have their differing opinions. English courts have rejected the idea, for example, that Article 8 creates a tort in privacy, or that it offers protection to individuals from other individuals (known as horizontal protection.) Instead, English courts have viewed the Human Rights Act as protecting individuals from government (vertical protection,) and have understood privacy as a 'freedom,' similar to the American understanding of liberty.[31] Scottish courts, on the other hand, have awarded damages for both 'the invasion of privacy and liberty,' and although there is presently no Scottish case law based on the Human Rights Act it appears the Scottish courts are prepared to apply Article 8 to protect individuals from others, not only from government.[32]

In the context of the workplace privacy protects of course not only personal information but potentially a myriad of other employee activities. Understood as protecting primarily dignity privacy could be taken to protect, for example, employees from location monitoring, video surveillance and computer and internet usage, to mention but a few. Note how dependent the notion of privacy is on the underlying value it attempts to protect. In Great Britain, for example, video surveillance of the public, in public places, is pervasive and routinely used by the various levels of government to such

---

[27] Part II, Title I. The European Charter also includes a right to 'respect for private and family life' in § II-67, and a right to 'protection of personal data' in § II-68.

[28] EU Draft Constitution, § II-91: Fair and just working conditions, (1).

[29] Even those who would advocate that the EU adopt a 'reasonable expectations' approach in order to determine the extent of a person's right to dignity acknowledge that such expectations cannot simply reflect, as they appear to in the US, an individual's expectations (which are subject to manipulation by others, e.g., employers), but that they must reflect some objective standard, e.g., a denominator common to all Member States. See H. Tomas Gomez-Arostegui, *Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations,* 35 CAL. W. INT'L L. J. 153, 195-197 (2005).

[30] Article 8 creates the 'right to respect for private and family life.'

[31] See Jonathan Morgan, *Privacy Torts: Out with the Old, Out with the New*, 120 LAW QUARTERLY REVIEW 393 (2004)

[32] See MacQueen, *supra* note 23.

extent that Americans label it a 'dragnet'.[33] Such video surveillance does not disturb members of society in Great Britain as an invasion of privacy, it would seem, since privacy in Europe primarily protects dignity, a social value, which is not threatened by such government actions. In the U.S., where privacy does primarily protect an individual from government public video surveillance is met with the predictable uproar. It is necessary therefore, in order to understand privacy as the protection of dignity in the workplace, to first understand the meaning of dignity in the workplace and in the context of the employment relationship.

## The Dignity of Workers

Although it is beyond the scope of this paper to conduct a detailed analysis of all the legal implications of the employment relationship, a short detour into employment law, if only for the purposes of clarifying some terminology as it is used here, is in order. All the jurisdictions discussed below recognize in some form that there can be a distinction for legal purposes between a person that performs some work for pay for another person, and a person that is in the employment of another person. Depending on various tests for the working person's independence and control over the performed task jurisdictions draw a distinction between (to use the common law terminology) an independent contractor, who is a person that, as can be surmised from the term, enters into contractual relationships while largely retaining independence and free will throughout the contract, and an employee, who is a person that is generally hands over control of their conduct to the party that pays them throughout the existence of a unique form of contractual relationship, known as an employment relationship, between them.[34]

The person who mows your lawn, cleans your house, or to return to an earlier example, takes care of your children can be therefore your independent contractor or your employee, depending on the outcome of these various tests. There are legal obligations that arise only when an employment relationship exists, hence the significance of these tests. In certain jurisdictions for example, employers must pay employees at least a minimum wage, provide employees with paid annual vacation or leaves of absence for medical reasons or for the purposes of raising children, and more. All of these arguably contribute to the dignity of employees, and when such employment standards do not exist, or when they exist in a diminished form (e.g., when workers and employers can largely 'contract out' of these standards), then the dignity of employees is diminished as well. This paper focuses however on another form of contributing to dignity in the workplace, through the provision of employment privacy standards, so to speak.

From the perspective of employment law, viewing workplace privacy as a potential addition to current employment standards raises several important questions. For example, should a privacy standard be one that employer and workers are able to contract out of? Should such a contractual term be an express term of the employment relationship, or could it be implied through employment practices and policies that are

---

[33] See for example Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L. J. 213, 222-223 (2002).

[34] These tests for the existence of an employment relationship are known within common law jurisdictions as the Control Test, the Fourfold Test, the Integration Test and the Permanency Test, all of which can and have been used by the courts in combination with each other.

largely dictated by the employer? To what extent are such contractual terms compatible with the notion of workplace privacy reflecting dignity as an inherent human right, or do they lead towards an analysis of workplace privacy in terms of the employment relationship parties' reasonable expectations as shaped by their contractual agreement?[35] It seems to me, for example, that an argument that there are reasonable expectations that withstand any particular contractual relationship, or that there are employment standards out of which employers and workers cannot contract out is actually better put in the language of human rights that workers are entitled to as individuals both within and without the workplace, so it is perhaps more significant for the purposes of this paper that there are legal obligations that exist when one person works for pay for another person regardless of whether they are in an employment relationship or not, such as health and safety obligations, and, I would argue, dignity obligations. The obligation of one person to respect another's dignity is based, according to such a view, on a premise that dignity is a value respected between members of society regardless of their social status, or the contractual or employment relations they have with each other.[36] For this reason I shall discuss the dignity of workers, a term that is broad enough to capture employment law's category of independent contractor as well as its category of employee, as well as other categories of individuals working, such as the hybrid category of dependent contractor and the category of those individuals that do not seek remuneration, namely volunteers. All are owed some measure of dignity while performing their tasks, and this dignity emanates not from their work necessarily but from their status as members of a society that respects them as individuals in the manner discussed above.[37] Indeed, it seems that in the context of employment employees often struggle to maintain the dignity that is theirs as human beings to begin with.

What are individuals entitled to, therefore, while working (and in the limited context of privacy that is discussed here), in order to maintain their sense of self-worth, to avoid humiliation, to preserve their reputation and to maintain their persona in their interaction with their employer and their co-workers? In the context of privacy, and setting aside employment standards in general, it seems that workers are entitled, first and foremost, to the recognition that their persona as a worker be kept distinct from other aspects of their lives, and that other aspects of their lives be kept distinct, and unknown to, their employer and their work.[38] Indeed, the term used in EU legislation,[39] and in the

---

[35] See Gomez-Arostegui, *supra* note 29 as well as Hazel Oliver *Email and Internet Monitoring in the Workplace: Information Privacy and Contracting Out,* 31 INDUSTRIAL LAW JOURNAL 321 (2002).

[36] As seen from the European example dignity may be respected due to its enshrined legal status as a human right, or it may enjoy diminished emphasis in other jurisdictions

[37] *Supra*, page 5

[38] This paper focuses on dignity at work, but the analysis is clearly applicable to the conduct of workers that is not directly related to their function at work (e.g., the length to which they grow their hair) as well as to their conduct while not working (e.g., to their personal relationships). Employers increasingly attempt to control such off-duty conduct, in effect arguing that the only persona of workers is their worker persona and that they are not entitled to other, non-work personas. The notion of dignity provides a conceptual basis for such an entitlement. See most recently Catherine Fisk, *Privacy, Power, and Humiliation at Work: Re-Examining Appearance Regulation as an Invasion of Privacy,* DUKE LEG. ST. PAPER NO. 101 (working paper, 2006) available at http://ssrn.com/abstract=893148.

[39] E.g., Article 8 of the European Convention on Human Rights, *supra* note 30.

legislation of Member States such as France, Germany, Spain and Italy that is commonly translated into English as 'privacy' is in fact literally translated as 'private life'.[40] The concession that workers 'have a life' outside work is one that is difficult for employers to make.[41] Indeed it is perhaps a notion alien to North American work ethics, since it is a common North American (ethical!) argument that workers should not exhibit aspects of their personal, private, non-work lives, while working.[42] Nevertheless, it appears to be essential to the establishment of dignity through privacy in the workplace. Note that the establishment of such a distinction between an individual's work persona and other aspects of their persona can be achieved by ensuring that the individual is in control over their persona, or by handing over control to the individual, but that such control is not necessary. Such control is often built into privacy principles that govern personal information. For example, European principles such as the requirement for an individual's consent, the right to correct information and monitor its usage and the right to challenge any significant decision made on the basis of the information all guarantee the dignity of the individuals to whom the data belong, and achieve this goal by handing over control over the information, at least to some extent, to the individual that the information is about.[43] Although handing over control to individuals may be a necessary mechanism to achieve meaningful privacy in the context of personal information it is not necessary (although it could be useful) for other aspects of privacy. This is particularly important in the context of employment where as has just been discussed the absence of individual control is often a prerequisite for the determination that an employment relationship exists. It is possible, in other words, for employees to maintain dignity by enjoying privacy through measures that are controlled and set in place by the employer.

It is now clearer why many of the measures introduced into the workplace thanks to technological advancement and employer initiative are indeed privacy-invasive. Measures such as video surveillance, computer monitoring and location positioning and certainly biometric measures are taken by workers to invade their privacy because they blur the distinction between their work persona and other aspects of their life, and in so doing harm (or can potentially harm) the workers' dignity.[44] What is entailed therefore by the notion of dignity in the workplace, protected by privacy, is that these and other measures be used in a way that will limit the intrusion of employers into the lives of their workers, to the extent that this is at all possible. In a sense, if employers exercise self-

---

[40] For more on the significance of these linguistic differences see Rothstein, *supra* note 8, at 383.

[41] An example of such a life, to return to the example that opened this paper, would be the need of workers to check on their children at daycare through webcams. These webcams cause workplace problems therefore not only for the daycare workers subject to them, but also to the parent workers attempting to access them while at work themselves.

[42] Which might of course explain in turn why North American workers enjoy less dignity than their counterparts in other jurisdictions, as discussed in the following section.

[43] These principles govern personal information in other jurisdictions, such as Canada and Australia, as well, and the mechanism used there is that of personal control over the information as well.

[44] These measures can be harmful to dignity irrespective of the damage done to workers' privacy. It is common in the EU to argue against purely technological or automated forms of monitoring, on the basis that as human beings workers are entitled to have other human beings supervise them, rather than 'cold' technology in the form of cameras and computers. See e.g., Jason Flint's discussion of Spanish case law in *Internet and Email Monitoring in Spain: How Far Can Employers Go?* 15 INTERNATIONAL COMPANY AND COMMERCIAL LAW REVIEW 315 (2004).

control in use of these measures then arguably workers will have no need to demand control.

It is now time to verify whether the notion of dignity is helpful in illuminating the different ways in which workers enjoy privacy, to a greater or lesser degree, across several jurisdictions. The following section will discuss workplace privacy protection in several EU Member States, as well as North America, Brazil and Australia, in order to determine whether a common theme of privacy protection as dignity protection can emerge from what little case law that exists on this topic.[45]

## Workplace Privacy Protection

The reviews that follow, while attempting to include as large a number of jurisdictions as possible within this paper in order to ascertain whether dignity is a useful concept in the analysis of workplace privacy, are by no means comprehensive. That is, they do not cover, for each jurisdiction, all of the forms of monitoring and surveillance that have been mentioned as examples above. Instead, each section dedicated to a distinct jurisdiction focuses on several forms of monitoring and surveillance, to the extent that case law or legislation or some other form of regulation exists with respect to these forms of monitoring. Such a focus does not mean that, since they are not mentioned in the section, other forms of surveillance are not in practice within the jurisdiction in discussion. It simply means that any attempt to measure whether their practice reflects dignity in the workplace is difficult in the absence of some form of regulatory guidelines as to their use.

### *The European Union*

As I mentioned excellent work has already been done reviewing workplace privacy protection in the EU and comparing it to other jurisdictions.[46] Within the EU, the status of dignity as a right that workers are entitled to is well entrenched in EU legislation, Member State legislation and the resulting case law and labor tribunal decisions. What is not so clear is the status of monitoring and whether surveillance is prohibited or allowed to some degree in the context of this worker right to dignity and of

[45] In light of the large number of workers that are under surveillance of some form or another the small numbers of complaints that have actually evolved into court or even tribunal decisions is somewhat perplexing. For some possible reasons see Hans-Joachim Reinhard, *Information Technology and Workplace Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law: Enforcement,* 23 COMP. LAB. L. & POL'Y J. 527, 529 (2002).

[46] The work of a research group based at the Open University of Catalonia (Barcelona, Spain) on Information Technology and Workplace Privacy has been published as a special issue of the COMPARATIVE LABOR LAW AND POLICY JOURNAL (vol.23, 2002) and will be referred to extensively below. In addition the work of another research group based at Tilburg University (The Netherlands) on video surveillance and workplace privacy, titled REASONABLE EXPECTATIONS OF PRIVACY? ELEVEN COUNTRY REPORTS ON CAMERA SURVEILLANCE AND WORKPLACE PRIVACY, (Sjaak Nouwt et al eds., 2005) is referred to as well. For a comparison of the EU to the US and Canada see Gail Lasprogata et al, *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada,* 2004 STAN. TECH. L. REV. 4, available at http://stlr.stanford.edu/STLR/Articles/04_STLR_4. For a brief overview of the US and some EU Member States see Jay Kesan, *Cyber-Working or Cyber-Shirking? A First Principles Examination of Electronic Privacy in the Workplace,* 54 FLA. L. REV. 289 (2002).

course Europe's information protection laws.[47] The European Constitution, if ever accepted, includes a right to the protection of personal information, as mentioned above, which states:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.[48]

Such a right, together with the workers rights mentioned above that are in the draft as well, would ensure strong legal protection to workers in terms of their workplace privacy.[49] For the time being, however, the EU Privacy Directive and the corresponding Member State legislation do not apply to the actions of surveillance directly (although the Working Party, established under Article 29 of the Directive, has issued guidelines with respect to particular technologies and forms of information processing).[50] They apply indirectly, because of the processing of the information produced by the different forms of surveillance.[51] It is this processing that falls under the jurisdiction of the directive, not the act of surveillance itself, and proponents of worker dignity wish at times therefore that the Member States would pass legislation curtailing surveillance directly.[52] As a result, Member States have largely been left to strike their own balance between workers' dignity, information protection legislation, and employer concerns. What follows is a review of some of these latest decisions, by Member State.

*France*

France is a bastion of workplace privacy, which may be somewhat surprising given that France was the latest Member State to implement the EU Privacy Directive

---

[47] For a general discussion of EU cases and the value of dignity see Whitman, *supra* note 16, at 1194-1196.
[48] EU Draft Constitution, § II-68, *supra* note 25. There is a similar right with respect to personal information in the hands of the EU itself, § I-51.
[49] Some Member States already have a constitutional right to personal information protection, and in that sense, again, the EU Constitution does not break new legal ground but rather reflect the current EU protection of human rights. See Joseph Cannataci & Jeanne Pia Mifsud-Bonnic, *Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty,* 14 INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW 5, 7-8 (2005).
[50] See for examples the guidelines on biometrics, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf. The guidelines specifically address the use of biometrics in the workplace for secondary purposes: "For instance when biometric data are processed for access control purposes, the use of such data to assess the emotional state of the data subject or for surveillance in the workplace would not be compatible with the original purpose of collection." See also Phillip Rees, *Hard to Put Your Finger On – Balancing Biometrics and Privacy,* 14 SOCIETY FOR COMPUTERS AND LAW MAGAZINE 1, 4 (2003) who mentions a decision by the Portuguese data protection authority that a biometric fingerprint system to ensure the punctuality of staff at a university was incompatible with the guidelines.
[51] See http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf for the opinion of the Working Party, established under Article 29 of the EU Privacy Directive.
[52] Whether such legislation is feasible, given the complexity of monitoring and its degree of variation both within the workplace and between industries, is another question.

with legislation that only came into force effective August 2004.[53] However, the surprise is diminished once one recalls that information protection and workplace privacy, while connected, are ultimately based on the distinct concepts of autonomy and dignity. The right to a private life (protecting dignity), until such time that the EU Constitution is ratified is protected in France through Article 8 of the EU Convention on Human Rights,[54] and through Article 9 of the French Civil Code.[55] This right has been implemented into strong workplace privacy protection through the French Labor Code.[56] Article L.121-8 of the Code prohibits the collection of worker information without prior notification. Once the information collected through surveillance and monitoring is taken to be personal (recall that this is the common understanding within the EU')[57] then the conclusion is that employers must notify workers prior to installation and use of any surveillance or monitoring device. Article L.120-2 further establishes that surveillance and monitoring must be proportional to, and justified by, their purpose.[58] Additional Labor Code Articles require that all actions taken by the employer (including surveillance) are to be taken in good faith, and in consultation with the workers' representative (e.g., a trade union).[59] These Articles of the Code establish that surveillance must be transparent, proportional and justified (or relevant) and many jurisdictions have attempted to implement these three principles within their system of privacy protection.[60]

Even France, however, recognizes that employers have legally the right, at times even the obligation, to survey and monitor the workplace. French case law, as in other jurisdictions, attempts therefore to balance, or limit this employer right, in light of the three principles governing surveillance and the fundamental right of workers to dignity, or a private life. The leading French case is the French Supreme Court's Nikon Case.[61] The Supreme Court found, based on Article 8 of the EU Convention on Human Rights, Article 9 of the French Civil Code and Article L.120-2 of the French Labor Code that employers are not allowed to read employee private e-mail (or other correspondence) even if the e-mail was sent using employer resources, and even if the act of using

---

[53] France did have its similar Computers and Freedom Act since 1978, which guaranteed certain information protection to workers as well. See also Claudia Faleri, *Information Technology and Workplace Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law: Public and Private Regulation,* 23 COMP. LAB. L. & POL'Y J. 517, 519 (2002).

[54] *Supra* note 30.

[55] Available on-line in English at http://www.legifrance.gouv.fr/html/codes_traduits/code_civil_textA.htm.

[56] For a discussion see Christophe Vigneau, *Information Technology and Workplace Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workplace Privacy: The French Law,* 23 COMP. LAB. L. & POL'Y J. 351 (2002).

[57] *Supra* note 51.

[58] The Code establishes these principles generally, with respect to any activity that restricts workers rights and freedoms.

[59] Articles L.122-35 and L.432-2-1 respectively. On the role of unions in workplace privacy protection see also Javier Aranda, *Information Technology and Workplace Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law: The Role of Worker Representatives,* 23 COMP. LAB. L. & POL'Y J. 533 (2002).

[60] See the discussion below of Canadian decisions, as well as Karen Eltis, *The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel: Should Others Follow Suit?* 24 COMP. LAB. L. & POL'Y J. 487 (2004).

[61] Arret 4164, Cour de Cassation – Chambre Sociale (2001), available on-line at http://www.courdecassation.fr/agenda/arrets/arrets/99-42942arr.htm.

employer resources for private purposes was in violation of an employer policy. This decision, while awarding employees with strong protection, has left employers somewhat at a loss, since employers are allowed to discipline employees for forbidden use of employer resources (even in France…) provided that the discipline is proportional to the harm caused by the unauthorized use.[62] It is not clear how employers are to distinguish personal from work-related e-mail, whether they are permitted to totally prohibit personal e-mail in order to avoid reading personal e-mail, and so on.[63] The extent to which the Nikon ruling applies to monitoring of other activities, such as internet usage, or monitoring in other forms, such as video surveillance, is also not clear. However, since the Supreme Court's starting point is that workers have a right to a private life even in the workplace (although there is no explicit such right in the French Labor Code) it seems that all employer activities in the areas of monitoring and surveillance are to be understood in essence as infringing on this right, and that they are therefore only to be allowed when justified by the employment relationship, or otherwise mandated by law (e.g., in the event of a criminal investigation).

Surveillance is justified in the workplace therefore, when it serves the employment relationship, i.e., when it is conducted for the purposes of assessing and evaluating employees. Workers must of course be notified and consent to the surveillance, in line with the principle of transparency, but it is clear that even the requirement that surveillance be justified prohibits, for example, surveillance in areas of the workplace that have little to do with employee evaluation, such as lockers and washrooms. Further, due to the implementation of France's information protection legislation in line with the EU Privacy Directive, workers' personal information is subject to additional restrictions even if the employer collected it in a transparent and proportional manner and for a justifiable purpose. For example, information cannot be stored indefinitely in an employer's data base. It must be kept only for a period of time that is appropriate given the purpose for which it was collected. E.g., information collected for the purposes of an annual evaluation must be destroyed upon completion of the evaluation. The principles of transparency and proportionality are strengthened by the information protection legislation, since it includes them as principles of personal information protection. These have proven particularly important where the justification of personal information collection is ultimately the termination of the employment relationship. The Social Chamber of the French Supreme Court has ruled that unless workers are notified, and consent to the use, of surveillance equipment for the purpose of their evaluation, which could lead to their termination, then the information collected by such means cannot serve as the basis for their dismissal.[64] Similarly, the Paris Court of Appeal ruled that an employer cannot use personal information gathered indirectly for purposes of dismissal, since employees were not notified, nor did they agreed to, the use of information in that way.[65] French courts have also been very cautious to accept

---

[62] For example, an employer was allowed to dismiss an employee that used the employer's internet access to gamble regularly. See Vigneau, *supra* note 56, at 357.

[63] For a discussion, see Vigneau, *supra* note 56, at 365-367.

[64] This in a case where an employee was caught stealing on tape. The tape was inadmissible since the surveillance was covert, although it would be admissible for the criminal proceedings. See Vigneau, *supra* note 56, at 372-373.

[65] An employer used a piece of software for sales, where every sale required an entry identifying the employee responsible, for purposes of customer service. The employer ascertained that one employee was

electronically stored personal information simply since it is easy to manipulate and alter, in such cases in order to support an employer's version of events.[66] Allocating this amount of power to the employee within the context of an employment of relationship would probably strike Americans, familiar with the 'at-will' doctrine of employment, as an abnormal doctrine of employment law.

Indeed, I would hazard to guess that American observers would be hard pressed to comprehend the manner in which French employment law has evolved in its protection of workplace privacy. It seems to me that the eventual ratification of the EU Constitution, with its emphasis on dignity, will only serve to entrench these French developments, which have so far been based on the idea of dignity in only an implicit manner, through the right of all individuals, workers included to a private life. Employers have been put in the position that their surveillance activities are secondary to the protection of worker rights, although even French law recognizes the legitimate purposes which surveillance in the workplace can serve, and that employers do have property rights in the resources and systems used by their employees. Employers must lift the burden, however, of justifying surveillance since the status of a private life as a worker right implies that workers are unable, even if they are willing, to contract out of this right, or to lose some form of reasonable expectation to such a right through the employer's unilateral actions. The contrast between the EU and the US could not be greater.

*Germany*

There are several reasons, unique to Germany, which have influenced the development of German workplace privacy. First, increased sensitivity is awarded in Germany, due to its totalitarian history, to databases of personal information, whether public or private. This sensitivity is conceptually based on the ideas of dignity and personhood as fundamental human rights that are protected in the German Constitution, and that have been developed in Germany, with the rude interruption of the Nazi regime, throughout several centuries.[67] The overriding principle of all such databases is that personal information collected must be kept to the bare minimum required for the purposes of the database. This principle applies to workplace databases as well. For example, German employers are not permitted to retain information on prospective employees once a decision regarding their employment has been made.[68] Beyond this emphasis on minimizing databases the familiar personal information protection principles apply. E.g., personnel records must be kept accurate, access to records is restricted only to those employees who require the records for the database's stated purposes, and

---

routinely absent from the lack of entries identifying that individual. The employer unsuccessfully attempted to dismiss the employee using the software log as evidence for the employee's absence. See Vigneau, *supra* note 56, at 373.

[66] Vigneau, *supra* note 56, at 374.

[67] For a discussion of these concepts in Germany see Matthew Finkin, *Information Technology and Workers' Privacy: A Comparative Study: Part IV: The Comparative Historical and Philosophical Context: Menschenbild: The Conception of the Employee as a Person in Western Law,* 23 COMP. LAB. L. & POL'Y J. 577, (2002).

[68] See Hans-Joachim Reinhard, *Information Technology and Workplace Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workplace Privacy: The German Law,* 23 COMP. LAB. L. & POL'Y J. 377, 395 (2002).

information cannot be disclosed to third parties unless required by law (e.g. for taxation or social security purposes).[69]

Second, some aspects of German workplaces are managed through the unique institution of the Works Council. Works Councils can exist at a workplace whether or not it is organized by a trade union. A Works Council is a committee established within the workplace, which represents all workers (including management) and which has the purpose of protecting human rights in the workplace. As such, issues of workplace privacy, to the extent that they can be understood as infringing on workers' right to a private life, fall naturally within the mandate of Works Councils. German law reflects this institution and grants workers, through Works Councils, a supervisory role over workplace privacy.[70] At the same time Germany does not have a labor code or tribunals dedicated to workplace dispute resolution, and it therefore has less case law on workplace privacy than other jurisdictions,[71] although issues that might seem trivial for North Americans have become, due to the role played by Works Councils, the subject of rulings, such as whether employers were allowed to introduce computers to the workplace at all![72]

The German framework of Works Council guarantees workers the ability to intervene when new technologies are introduced into the workplace in order to ensure that these technologies comply with the various German laws protecting personal information. Such intervention can take the form of supervision over the installation of technology, testing and examining the technology for compliance either by Works Council members or through external experts, and arbitrating complaints received from workers regarding the technology in question.[73] The exercise of its powers by the Works Council must reflect its mandate to protect the human rights of workers, in this case the right of workers to dignity and to a private life, yet despite these substantive measures, or perhaps as a result of their existence, German law offers little protection to workers in their use of employer resources for private purposes. These resources are considered the property of the employer and as such it is up to the employer to determine what form of private use is permissible. This is perhaps surprising in light of the status of the values of dignity and personhood in Germany mentioned above, yet the employer is free to set out the boundaries of private use through policies, or through an agreement reached with the Works Council.[74]

It goes without saying that where a policy or an agreement exists an employer must adhere to its contents. Yet German law does not dictate the contents of such policies or agreements beyond several general requirements, such as a notification requirement, the requirement that employers notify workers about surveillance (whatever its nature), or a requirement to respect the confidentiality of fiduciary relationships that the workers may be party to (e.g., if the worker is a lawyer or a physician).[75] Where private use of resources (e.g. e-mail) is allowed by the employer during work hours then the employer

---

[69] See Reinhard, *supra* note 68, at 395-396.
[70] See Aranda, *supra* note 59.
[71] See Reinhard, *supra* note 45. Another factor may be the existence of legislation on workplace privacy in Germany since 1972. See also Faleri, *supra* note 53.
[72] See Reinhard, *supra* note 68, at 382.
[73] See Reinhard, *supra* note 68, at 384-385.
[74] See Reinhard, *supra* note 72, at 386.
[75] See Reinhard, *supra* note 72, at 390-391.

will not be allowed to access the contents of such messages. But there is no such restriction in general, and an employer that does not allow the private use of resources is allowed to filter or otherwise screen messages for personal content.[76] As such, German practice resembles the American practice, where as discussed below employers are generally free to set their policies with respect to the use of their resources or the personal information of their employees as they please, but are then expected to adhere to these policies by state and federal regulators.

*Belgium*

It is worthwhile examining Belgium's workplace privacy, since it has had in place, for several years now, a national collective agreement governing the use of video surveillance cameras in the workplace.[77] The content of the agreement is of course of interest, but the notion of reaching a national collective agreement, through an institution in which both employers and employees are members, is of interest as well, and reflects the role which organized labor plays in the regulation of the workplace in Belgium. The agreement itself first establishes that it is in place to protect the private life of workers. In other words, video surveillance in the workplace in Belgium must respect the dignity of workers. Dignity is protected through measures built into the agreement which guarantee consultation between employers and workers upon the introduction of video surveillance into the workplace, and disclosure to workers of the ways in which video surveillance is to be used. Such disclosure must include the purpose of the proposed video surveillance, and the manner in which it will operate (e.g., the number, location, hours of operation, and technological capabilities of the cameras that will be installed). Further, employers are limited in the purposes for which they can use video surveillance to begin with. The agreement authorizes three purposes in general: health and safety, protection of the employer's property, and supervision of machinery. With respect to all three, employers must consult with workers if it appears that video surveillance for these purposes will impact on the workers' private life, and employers must aim to minimize this impact by ensuring that the surveillance is proportionate to the purpose it serves.

What is perhaps most interesting about the Belgian national collective agreement, however, is that it does allow for a fourth purpose, productivity, despite the obvious intrusion of what workers might view as their private life. The agreement allows for video surveillance of the production and the output of workers, albeit under several constraints. Such surveillance cannot be permanent (it can for the first three purposes mentioned above), and it must be obtained not only after consultation with the workers and disclosure of the surveillance to them, but in actual agreement between the employer and the workers as they are represented in the particular workplace. Despite these constraints, the allowance of video surveillance for productivity purposes in the Belgian national collective agreement is significant, since it presents an example in which the private life of workers is protected at work, while their productivity is measured at the same time. It is possible for employers to monitor and conduct surveillance on

[76] See Reinhard, *supra* note 72, at 391.
[77] The agreement is available in Dutch at http://www.cnt-nar.be/CAO/cao-68.doc. For the purposes of the discussion here I am relying on the English translation, available at http://www.eiro.eurofound.eu.int/1998/07/inbrief/be9807150n.html.

employees, for productivity purposes, even if the legal concept at the basis of the employment relationship is that workers enjoy a right to dignity and to a private life.

*The Netherlands*

Dutch workplace privacy has developed along lines similar to German workplace privacy, largely due to the existence of Works Council in Dutch workplaces as well. Generally, the Dutch enjoy a right to a private life from government through the Dutch Constitution,[78] and the equivalent of a constitutional right to a private life from other members of society through the European Convention.[79] As in the other Member States of the EU, the right to private life is not absolute, and can be the subject of a contractual relationship. In the context of workplace privacy, this would most often be, as it is in Germany, a contract between the employer and the Works Council. According to the Dutch Works Councils Act, Works Councils have the authority to approve permanent monitoring and surveillance systems of any form, hence the incentive for employers to reach such agreements.[80] Temporary forms of surveillance, such as a camera introduced into the workplace to investigate specific suspicions of theft, do not require the approval of the Works Council.[81]

As in Germany, the Netherlands information protection legislation does not dictate the content of the agreements reached between employers and Works Councils. Nevertheless, these agreements are expected to adhere to the guidelines for monitoring and surveillance in the workplace set out by the Dutch Data Protection Authority. These guidelines specify that monitoring and surveillance must be for a purpose that cannot be achieved differently, that is more important than the harm it would cause to the private life of workers, that surveillance must be proportionate to the purpose and measured, and that workers be notified of the monitoring.[82] Moreover, there exists some case law with respect to workplace privacy in the Netherlands. A lower court in Amsterdam determined that workers have the "freedom to be themselves" in certain circumstances, e.g., when they are changing cloths, despite the existence of a video monitoring system.[83] Unfortunately, most of the case law discusses situations where workers suspected of theft or fraud were monitored in order to obtain evidence to substantiate these suspicions, and the resulting question as to whether such evidence is admissible.[84] Ultimately, Dutch law is no different than the law of every other jurisdiction in recognizing that surveillance and monitoring is a legitimate way for employers to protect their property from unscrupulous workers. As such, circumstances in which certain workers are suspected of theft and surveillance ensues are not circumstances in which the private life of these workers is threatened.

Of more interest is an earlier Dutch case referred to as the KOMA case. KOMA decided to install video surveillance cameras for purposes of regular supervision and

---

[78] Article 10. An English version is available at http://www.oefre.unibe.ch/law/icl/nl00000_.html.
[79] Article 8, *supra* note 30.
[80] Sjaak Nouwt et al *Camera Surveillance and Privacy in the Netherlands*, *in* Nouwt et al *supra* note 46.
[81] Nouwt et al *supra* note 80.
[82] Nouwt et al *supra* note 80.
[83] Nouwt et al *supra* note 80. It is not clear what this freedom actually entails beyond the entitlement to freedom from supervision in certain work-related circumstances.
[84] Nouwt et al *supra* note 80.

quality control. These purposes are directly linked of course to the productivity of workers, and the trade union representing the workers commenced litigation. The trial court rejected the employer's argument that video surveillance is no more intrusive than regular supervision conducted by other employees.[85] It therefore rejected the argument that video surveillance could be used for regular productivity purposes, and required an additional interest that could be served only through the technology and not via regular means (such as the need to supervise in the course of manufacturing several locations simultaneously). The trail court's findings were upheld by the court of appeal, and the KOMA case is significant since it established that the right to private life, in the Netherlands, could not be infringed upon by technological means if the sole purpose of the proposed monitoring system was to ensure productivity.

*Spain*

Spain illustrates the simplicity of tarring the EU, and all its Member States, with the one brush of being a jurisdiction where only worker interests (i.e., dignity) are protected at the expense of employers. In fact the legal discussion in Spain, perhaps more so than in the other EU Member States, often leaves one pondering what appears to the Spanish employment tribunals to be a greater threat? Is it the threat to worker's privacy by monitoring that has been described as "distant, cold, incisive, constant, surreptitious and apparently infallible",[86] or is the threat to the employer's business by their workers' abuse of resources such as access to the internet.[87] To some extent this Spanish state of affairs reflects Spanish legislation. The Spanish Constitution protects privacy and the secrecy of personal communication in its Article 18.[88] However, the Spanish Workers' Statute was passed before the forms of surveillance discussed in this paper became prevalent. As a result it does not address (or forbid) new forms of monitoring explicitly. The Workers' Statute does recognize that workers have a right to privacy in their personal belongings and does mandate that any form of monitoring and surveillance must "pay due consideration to human dignity".[89] Similarly, Spain's Information Protection Agency has ruled that Spain's information protection legislation does not prohibit surveillance and monitoring completely, but allows it within limits.[90] It has been left up to Spain's courts and tribunals to find these limits and strike a balance between employers and workers, surveillance and dignity.[91]

Decisions so far in Spain have centered on monitoring of e-mail and internet use. Most decisions are at the regional employment tribunal level and at best therefore only tentatively indicate where Spanish law will settle. Generally, Catalonian courts have

---

[85] Nouwt et al *supra* note 80.
[86] Javier Aranda, *Information Technology and Workplace Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workplace Privacy: The Spanish Law,* 23 COMP. LAB. L. & POL'Y J. 431, 432 (2002).
[87] See Aranda, *supra* note 86, at 433-434 for statistics on such employee abuse.
[88] For an English translation of Article 18 available on-line see http://www.congreso.es/ingles/funciones/constitucion/titulo_1_cap_2_sec1.htm
[89] Aranda, *supra* note 86, at 440.
[90] See Flint, *supra* note 44.
[91] Note that the Workers' Statute protects dignity and not privacy, leaving the door open to impose restrictions on surveillance that are not limited to privacy concerns (e.g., that humans should not be watched over by machines).

adopted a North American tack, with an emphasis on the role of employer policies, employee notification, employee consent, and the reasonable expectations created as a result.[92] Most notably, in what is known in Spain as the Deutsche Bank case, the Catalonian court upheld the dismissal of an employee that sent hundreds of personal e-mails from work, in light of previous discipline and explicit violation of employer policy. This decision stands of course in contrast to the similar French Supreme Court decision in the Nikon case. The same Catalonian court, in a later case, upheld the dismissal of an employee that used e-mail to send resumes to prospective employers and insult their current employer.[93] The court also held that an employee sending an e-mail from a general account to another general account was not entitled to privacy in its contents, and that dismissal for excessive internet use is permissible.[94] On the other hand, the Barcelona Employment Tribunal set aside the dismissal of an employee that inadvertently infected the employer's system with viruses due to e-mail and internet personal use. The dismissal was based on the employer's examination of e-mail and internet use logs and the Tribunal ruled that such examination of personal entry logs (distinguished from work-related entries in the logs) is possible only when a court order has been granted, and on the basis of a reasonable suspicion of a serious breach. The Tribunal found that in general access to personal logs should only be allowed where a specific explicit and legitimate purpose requires it, the monitoring must be proportional, and the harm to the employee's privacy is at a minimum.[95]

This ruling of the Barcelona Tribunal is in line with decisions made by Madrid's Employment Tribunal. The Madrid Tribunal found for example that although employers have a right to access work-related correspondence, personal computer use is allowed as long as it is not excessive (by drawing an analogy to conventional telephone use), and that e-mail examination must preserve employee dignity (for instance, be conducted in the presence of employee or representative).[96] The Tribunal also issued its own decision confirming that a monitoring system that logs the websites visited and time spent creates personal information and is therefore subject to Spain's data protection laws (although not prohibited by them).[97]

With only one Spanish Supreme Court decision related to workplace privacy so far (confirming that employers have propriety rights in information systems, and can therefore control access to these systems, e.g., prevent trade union access)[98] it remains to be seen where Spain will find the balance between workers and employers. More importantly for the purpose of my discussion here, Spanish courts and tribunals are aware in their decisions of the tension between the conceptual bases of reasonable expectations and dignity for workplace privacy, a tension they have yet to relieve.

*Italy*

---

[92] See also Reinhard, *supra* note 45, at 528.
[93] For a discussion of the cases see Flint, *supra* note 44, at 316.
[94] Flint, *supra* note 44, at 317-318.
[95] Flint, *supra* note 44, at 318.
[96] Flint, *supra* note 44, at 317.
[97] Flint, *supra* note 44, at 317.
[98] Flint, *supra* note 44, at 319. Unions do have a role, however, but less so than other EU Member States in workplace privacy supervision, since they must be consulted, although their consent is not required, prior to the implementations of measures impacting workplace privacy. See Aranda, *supra* note 59.

The right to dignity in the workplace is a constitutional right in Italy.[99] Employers cannot advance their interests in any way that would harm "human dignity". In additional to the constitutional protection Italy is one of the first members in the EU to have had legislation protecting the privacy of workers in the workplace, as part of its Workers' Statute.[100] The statute was passed during a period of labor unrest in Italy, and its stated purpose is "the protection of the freedom and dignity of workers."[101] In practice, the statute boosted the power of trade unions and allowed them to organize many employers. With respect to monitoring and surveillance the statute states that any concealed monitoring or surveillance devices harm the dignity of workers.[102] Monitoring and surveillance may only be conducted with the agreement of the union in an organized workplace, or only with the authorization of the Ministry of Labor in the absence of a union.[103]

This constitutional and legislative balance has been expressed in specific regulations for workplace privacy established by the Italian Data Protection Authority (known as the Garante).[104] For example, the Garante has issued regulations known as Decalogue 2004 with respect to video surveillance in general.[105] A section of these regulations addresses workplace video surveillance specifically.[106] In general, workers are not to be monitored from a distance for productivity purposes. Video surveillance is permissible for health and safety, security, and crime prevention purposes, or when surveillance is required by the organizational or manufacturing process.[107] Images obtained for these purposes cannot be used for other purposes, such as productivity. Further, video cameras are not allowed in areas not intended for the performance of work, such as restrooms or locker rooms. In Italy, therefore, the right to a private life precludes the monitoring of workers by technological means for productivity purposes.

The framework established in Decalogue 2004 is based upon, and strengthened by, several Italian cases on video surveillance and workplace privacy. Several local trial

---

[99] Article 41. An English version of the Italian constitution is available at http://www.oefre.unibe.ch/law/icl/it00000_.html.

[100] Statuto dei lavoratori (1970), available at http://www.unipa.it/cdl/lexall/dc1/70n300.htm.

[101] A discussion of the statute in English is available at http://www.eurofound.eu.int/emire/ITALY/WORKERSSTATUTE-IT.html. See also Claudia Faleri, *Information Technology and Workplace Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workplace Privacy: The Italian Law,* 23 COMP. LAB. L. & POL'Y J. 399 (2002).

[102] Article 4.

[103] Article 4. See also Aranda, *supra* note 59. However, see Faleri, *supra* note 101 for a critical discussion of the Workers' Statute.

[104] The regulations are based on Italy's comprehensive Personal Data Protection Code. For a discussion of the Code see Pierluigi Perri & Stefano Zanero, *Privacy Law – Italy: Lessons Learned from the Italian Law on Privacy – Part I,* 20 COMPUTER LAW AND SECURITY REPORT 310 (2004) and Pierluigi Perri & Stefano Zanero, *Privacy Law – Italy: Lessons Learned from the Italian Law on Privacy – Part II*, 20 COMPUTER LAW AND SECURITY REPORT 384 (2004). An English version of the Code is available at http://www.garanteprivacy.it/garante/document?ID=1219452&DOWNLOAD=true.

[105] An English version of the regulations is available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1116810.

[106] Section 4.1 of the 2004 Decalogue.

[107] See also Paolo Balboni, *Video Surveillance and Related Privacy and Data Protection Issues: The Italian Experience*, *in* Nouwt et al *supra* note 46.

courts have affirmed that distance monitoring of workers for productivity purposes is prohibited, and that monitoring of workers while they are not working (e.g., on a break) is prohibited as well.[108] The Italian Supreme Court (The *Corte di cassazione*) has affirmed that union agreement must be obtained prior to the installation of surveillance systems, in a decision known as the Banco di Sicilia decision.[109] Finally, and perhaps most significantly, the Italian Supreme Court has upheld the right to dignity and a private life even in circumstances where it would seem that the employer had a legitimate interest in infringing upon this right. In a case known as the Ledda case the court ruled evidence obtained via video surveillance inadmissible in a termination lawsuit.[110] The owner of a bar suspected a worker of theft, and subsequently installed a video camera to monitor the cash register. When the images captured the worker "in the act" the worker was dismissed on the strengths of the images. Although it would seem that the employer's protection of the employer's property is legitimate, and indeed is recognized as such by several other European jurisdictions, not to mention Decalogue 2004,[111] the court nevertheless ruled that the use of video surveillance was disproportionate(!), and therefore in violation of Article 41 of the Constitution.[112] This decision is reminiscent of the French Nikon decision and underlines the strength of the right to dignity in European jurisdictions.

*England*

England occupies a unique position with respect to other EU Member States regarding workplace privacy. The common law does recognize (yet) a tort of privacy.[113] As a result, under the common law the employer is considered to have the prerogative to act in the workplace as the employer sees fit since the workplace and its resources are understood to be the property of the employer. The employer is therefore free to monitor and conduct surveillance on workers by any means and for any purpose, unless the employer has entered into a contract (e.g., a collective agreement) to do otherwise. At the same time, English employers must comply with legislation that has been introduced as a result of England's membership in the EU. Three Acts important to workplace privacy are the Data Protection Act, the Human Rights Act, and the Regulation of Investigatory

---

[108] For a discussion of these cases see Balboni, *supra* note 107.

[109] See Balboni, *supra* note 107. Interestingly, there have been since that decision several contradictory lower court decisions as to whether the union's agreement overrules the refusal of individual workers to consent to such surveillance, particularly when the relationship between the union and the workers is adversarial, and it is the union seeking information on individual workers from the employer in order to determine whether these individuals are in violation of the collective agreement. See Faleri, *supra* note 101, at 417-418.

[110] See Balboni, *supra* note 107.

[111] The court's decision precedes Decalogue 2004.

[112] The court also found the installation of the camera was in violation of the Workers Statute.

[113] Litigation has focused on various celebrities such as the actor Michael Douglas or the model Naomi Campbell and the British media, not on workplace issues. For a discussion of the various cases see Lorna Skinner, *You're a Celebrity, Madam. So Do We Have a Right to Share Your Privacy in a Public Place?* 9 COMMUNICATIONS LAW 118 (2004); Stuart Goldberg, *The Contest For a New Law of Privacy. A Battle Won, a War Lost? Campbell v Mirror Group Newspapers Limited (2004) UKHL 22U,* 9 COMMUNICATIONS LAW 122 (2004); M.A. Sanderson, *Is Von Hannover v Germany a Step Backward for the Substantive Analysis of Speech and Privacy Interests?* 6 EUROPEAN HUMAN RIGHTS LAW REVIEW 631 (2004).

Powers Act.[114] None of the Acts forbid monitoring and surveillance in the workplace. However, they do impose some constraints over employers.

The most significant constraint imposed by the Human Rights Act is its introduction of a right to a private life.[115] The Regulation of Investigatory Powers Act is significant since it renders the interception of communications illegal unless both parties to the communication have consented to its interception.[116] Interception involves knowledge, at least partial, of the content of the communication, by a party which is neither the sender nor the recipient.[117] Monitoring of employee electronic communication traffic, therefore, does not necessarily constitute interception, so it is possible for employers to conduct such monitoring and surveillance legally. Employers are permitted, in addition, to intercept communications lawfully by the Act, provided such interception is reasonably required for the carrying on of the employer's business, and subject to regulations known as the Lawful Business Practice Regulations.[118] The Regulations generally permit interception to determine whether a given communication is private or business-related (the employer is not permitted to create a record of such communication in the event that it is personal) or otherwise, for an authorized business purpose. Authorized business purposes include the establishment of facts (e.g., faced with a customer's complaint), the compliance with any law, regulations or internal policies, quality control, training, and the maintenance of the information system.[119] In other words, the Regulations provide employers with sufficient grounds to continue and carry out monitoring and surveillance in the workplace without having to resort to obtaining the consent of their workers.[120]

Finally, the Data Protection Act authorizes the Information Commissioner to issue Codes of Practice with respect to the Act.[121] Although authorized by the Act the Codes themselves are not binding, although they are considered to be the expert interpretation of the Information Commissioner and will be granted weight as such by the courts if necessary.[122] The Commissioner has issued a Code of Practice with respect to workplace privacy known as the Employment Practices Code. It is to be read in tandem with another publication from the Commissioner, the Employment Practices Code: Supplementary Guidance.[123] The commissioner acknowledges that monitoring and surveillance, for any

---

[114] For a discussion of the acts see Mark Jeffery, *Information Technology and Workplace Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workplace Privacy: The English Law*, 23 COMP. LAB. L. & POL'Y J. 301 (2002).

[115] Article 8 (incorporated from the EU Convention). There has been some debate in England (and within the UK *supra* page 9) as to whether the Act offers, to borrow the English terms, vertical protection (from government only) or horizontal protection (from other individuals, e.g., employers, or the media in the event of celebrities) as well. See Basil Markesinis et al, *Concerns and Ideas About the Developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help)* 52 AM. J. COMP. L. 133 (2004) as well as *supra* note 113.

[116] Regulation of Investigatory Powers Act, § 3 (1).

[117] Regulation of Investigatory Powers Act, § 2 (2).

[118] Regulation of Investigatory Powers Act, § 4 (2). For a discussion of the Regulations, see Oliver, *supra* note 35, at 338-343.

[119] Lawful Business Practice Regulations, § 3.

[120] See also Jeffery, *supra* note 114, at 340-345.

[121] Data Protection Act, § 51 (3).

[122] Contrast their status with the authority of the Canadian Federal Privacy Commissioner, or lack of it, as discussed below.

[123] Both publications are available at http://www.ico.gov.uk/eventual.aspx?id=437.

purpose, is generally permissible under English law and specifically under the Data Protection Act, although it is the Commissioner's opinion that the right to a private life established in the Human Rights Act does apply to the workplace.[124] Interestingly, the Commissioner does not take the position that this right to a private life entails workers to the use of employer resources for private purposes. The right to a private life, in other words, does not create the right to use a telephone for a private call or the right to send a private email from work.[125]

Further, balancing the prerogative of an employer to conduct monitoring and surveillance with the right of employees to a private life and to the protection of their personal information does not preclude any particular form of monitoring or surveillance, and does not rule out any particular purpose for surveillance. Indeed, the Commissioner lists among the acceptable purposes the measurement of employee efficiency (i.e., productivity).[126] The private life and the protection of employees are ensured by other means which are listed in the Code and in the Supplementary Guidance. Generally, surveillance or monitoring will only be acceptable to the Commissioner if it has passed an internal assessment of its impact on privacy, which consists mainly of assessing whether the purpose justifies the intrusion, and whether there are alternatives ways in which to achieve the purpose.[127] Once a proposed form of monitoring or surveillance has passed such an assessment it can be carried out without the consent of workers.[128] Contrary to other EU Member States therefore, organized labor does not have a legal role in the establishment of monitoring/surveillance measures.[129] Nevertheless, it is the requirement of the Data Protection Act that workers be aware of any form of monitoring or surveillance that the employer has decided on.[130]

The employer can create such awareness by establishing policies with respect to the use of the employer's resources and to the monitoring and surveillance that exists to ensure such policies are complied with. The Commissioner offers several key elements that should be included in such policies, but more importantly, the substantive content of the policy (e.g., whether private use is allowed at all) is left to the employer.[131] Once employers decide upon a policy they should enforce it. A policy will not bind workers if in practice it is not enforced and workers are allowed to use resources in ways that are forbidden by the policy.[132] The Commissioner's approach with respect to policies and their role resembles the American FTC's approach in that respect, as is discussed below.

Of special interest is the section of the Code devoted to video surveillance.[133] Video surveillance of public places is both pervasive and popular in England.[134] In light

---

[124] EMPLOYMENT PRACTICES CODE, at 54.
[125] EMPLOYMENT PRACTICES CODE, at 64.
[126] EMPLOYMENT PRACTICES CODE, at 55.
[127] EMPLOYMENT PRACTICES CODE, at 57. Privacy Impact Assessments, or PIAs, are a common tool used in most of the jurisdictions discussed in this paper.
[128] EMPLOYMENT PRACTICES CODE, at 59. Consultation with workers is part of the assessment process.
[129] See also Aranda, *supra* note 59.
[130] SUPPLEMENTARY GUIDANCE, at 48.
[131] EMPLOYMENT PRACTICES CODE, at 64.
[132] SUPPLEMENTARY GUIDANCE, at 48.
[133] The Code discusses at length in additional sections electronic communications monitoring, the Commissioner's interpretation of the Lawful Business Practice Regulations, and in-vehicle monitoring (e.g., GPS).

of the degree to which public video surveillance is welcome in England the Commissioner has issued particularly forceful recommendations in the Code and its Supplementary Guidance. The Commissioner distinguishes between continuous and temporary surveillance, as well as between overt and covert surveillance. These distinctions follow the distinctions made by other EU Member States. Continuous surveillance is more intrusive – as such the Commissioner is hard pressed to acknowledge circumstances when such surveillance is acceptable.[135] Temporary surveillance is more acceptable, depending on its purpose, e.g., the suspicion of theft. Regardless, workers must be notified of all video surveillance, unless it is covert.[136] Covert surveillance in turn is also justified only in exceptional circumstances, e.g. criminal activity by workers on the premises.[137] Even in such dire circumstances covert surveillance is not to be carried out in locations that workers consider to be private.[138] These recommendations of the Code are forceful in light of the Commissioner's position that generally it is the prerogative of the employer to conduct surveillance and monitoring as the employer sees fit. The Commissioner seems to imply, in excluding such 'private' areas from covert surveillance, that workers are protected legally from surveillance by their right to a private life in such circumstances.[139]

### *Australia*

Canada and Australia are often compared in many areas of law, as two non-US, non-UK common law jurisdictions that have largely set on their own paths and at times have drawn closer to the EU as a result.[140] Similar to Canada, Australia appears to be caught currently in a debate over which approach to take to workplace privacy, the American or the European. Unlike Canada, however, Australia's Constitution (passed by the British parliament) established Australia as a federation but does not include a section focusing on human rights, similar to the Canadian Charter of Rights and Freedoms. Although Australia has passed legislation concerning various human rights the value of

---

[134] See the result of a survey conducted by the Information Commissioner, available at http://www.ico.gov.uk/eventual.aspx?id=5739. Note that the survey was conducted prior to the events of 7/7 in England.

[135] EMPLOYMENT PRACTICES CODE, at 68. See also SUPPLEMENTARY GUIDANCE, at 52. Surveillance of areas open to the public, i.e., to non-workers, is not considered to be workplace surveillance by the Commissioner.

[136] EMPLOYMENT PRACTICES CODE, at 68. See also SUPPLEMENTARY GUIDANCE, at 52.

[137] EMPLOYMENT PRACTICES CODE, at 69. See also SUPPLEMENTARY GUIDANCE, at 53.

[138] The Commissioner gives the examples of washrooms and private offices. Such locations should be put under surveillance only with the involvement of police. EMPLOYMENT PRACTICES CODE, at 68. See also SUPPLEMENTARY GUIDANCE, at 52.

[139] The Commissioner leaves the door open to overt surveillance of such locations, as well as allowing for the employer to influence through policy their reasonable perception as private, seeing as the Commissioner defines such locations as "areas that workers would genuinely and reasonably expect to be private." EMPLOYMENT PRACTICES CODE, at 69.

[140] Hong Kong and South Africa are two other interesting jurisdictions. For South Africa, see Neethling, *supra* note 15. For Hong Kong see Joeson Wong Ka Yu, *Electronic Government and its Implication for Data Privacy in Hong Kong: Can Personal Data (Privacy) Ordinance Protect the Privacy of Personal Information in Cyberspace?* 19 INTERNATIONAL REVIEW OF LAW COMPUTERS AND TECHNOLOGY 143 (2005).

dignity does not enjoy within its legal system the same status it, or the right to a private life, enjoys within the EU Constitution and the constitutions of its Member States.[141]

Concerns raised by Australian employers are similar to concerns raised worldwide, e.g., loss of productivity due to new time-wasting capabilities of e-mail, instant messaging and internet surfing, vicarious liability and more.[142] As a result, Australian common law, which does not recognize a general right to privacy, and certainly does not recognize a worker right to use employer property for personal purposes,[143] allows employers to monitor employees within limits and does not require employers to notify workers of such monitoring. Australian workers do enjoy some statutory protection, however. Federal legislation includes the Privacy Act, part of which applies to the public sector, and part of which, known as the National Privacy Principles, which applies to the private sector as well. However, employee records are specifically exempt from the protection of the Privacy Act.[144] The Australian federal Privacy Commissioner has issued guidelines on workplace privacy (applicable to the public sector), but they have yet to be incorporated into legislation.[145] The guidelines call for clear policies, created through consultation, as to what forms of electronic activities are forbidden and what forms are acceptable. The policies should clearly describe how information is retained and who will have access to it. Finally, the policies should determine all this taking into account that "it is unlikely that pervasive, systematic and ongoing surveillance of staff e-mails and logs should be necessary… Policy or practice which leads staff to believe that their privacy in the workplace is not respected may be regarded as intrusive and oppressive and have a negative impact on morale and productivity."[146] Interestingly, these guidelines do not explicitly rely on, or even mention, the value of dignity, and generally seems to focus on addressing employers concerns e.g., productivity.

At the state level New South Wales has additional legislation that specifically addresses the issue of workplace video surveillance.[147] Covert surveillance is prohibited, unless authorized by a court order. Otherwise, surveillance is permitted provided cameras are clearly seen, signs are present notifying workers they are under video surveillance, and all workers must have been notified in prior to camera installation about the purpose and scope of the video surveillance. There are no further legislative restrictions on employers in their use of video surveillance, although New South Wales' Privacy

---

[141] Of course Canada's Charter does not include the values of dignity or private life either.

[142] It should be noted that some employers take the position that allowing some personal use of computers actually increases productivity. E.g., in the Alberta case discussed below (*infra* pages 45-46) above the library had actually allowed the employee to conduct on-line banking from his computer at work, reasoning that productivity would increase if the employee did not take time to physically go to the bank instead. Ironically, that decision allowed clearly personal information to be captured by the keystroke software installed on the employee's computer.

[143] Although the reality in Australia, as elsewhere, is that such use is tolerated in practice, and at times (although perhaps not sufficiently) even protected by collective agreements.

[144] The definition of employee records under the Privacy Act allows for information to be collected regarding performance and conduct, hence opening the door to monitoring activities. Privacy Act 1988, § 6 (1) Employee Record (e).

[145] The guidelines are available on-line at http://www.privacy.gov.au/internet/email/index.html.

[146] *Supra* note 145.

[147] The Workplace Video Surveillance Act N.S.W. 1998. Other states have legislation that addresses surveillance generally.

Commissioner has issued voluntary guidelines.[148] The guidelines call for employers to install cameras in consultation with employees about their purpose, their hours of operation, when and why information will be used, and how any disputes regarding the surveillance will be settled. Cameras should be operated ethically (e.g., not to zoom in on individuals for mere curiosity) and access to information should be restricted, although individuals should be entitled to access their own records, especially when the employee is the subject of disciplinary or legal action on the basis of recorded information. Records should only be retained for a reasonable period of time, and finally, cameras should not be installed in areas such as washrooms, showers and locker rooms. Although the guidelines and the legislation do attempt to balance employer interests with some of the more fundamental principles of personal information protection (such as proportional use, and right to access) they do not explicitly mention, nor are they explicitly based, on the notion that employees are entitled to such protection due to their dignity as human beings.[149]

The question remains whether existing Australian case law and employment tribunal decision incorporate the idea of privacy protection as dignity protection, and if so, to what extent. There is little case law to go on (as seen below, there is little case law in Canada as well). The Australian Industrial Relations Commission found that use of employer systems, even if only for collection of material (deemed offensive by the employer's policies) on an individual's computer could not, by definition, be private if it is conducted during work (and obviously, in violation of said policy).[150] Such a decision appears to strongly favor an American approach to workplace privacy, with an emphasis on the employer's property rights. While motivated perhaps in part by the nature of the material collected such a decision indicates that Australia is receptive to the idea that once employer interests have been recognized as legitimate (e.g., vicarious liability concerns) then the form of technology used to pursue these interests, or its degree of innovation is quite secondary and can in most cases be safely disregarded. Such an approach is in contrast with the European approach that is concerned primarily with the repercussion new technology has on the workplace, in terms of its erosion of dignity through a high degree of automation, widespread coverage etc., even if the goals it pursues have long been recognized as legitimate.

Other decisions, by the New South Wales Industrial Relations Commission, appear at least initially to contradict this line of reasoning, inasmuch that they overturned the dismissal of employees that downloaded offensive material to their homes or their personal e-mail at work. The Commission found that since these employees did not distribute the material they had a reasonable expectation that they were not engaged in indecent conduct (the cause of dismissal) and therefore that their activities were private (since indecent conduct requires an element of public awareness to the conduct).[151]

---

[148] CODE OF PRACTICE FOR THE USE OF OVERT VIDEO SURVEILLANCE IN THE WORKPLACE, available online at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/code_overtsurveillance.pdf/$file/code_overtsurveillance.pdf.

[149] Although from the prohibition of cameras in areas such as washrooms and lockers a concern for the dignity of employees can certainly be implied.

[150] See Karen Wheelwright, *Monitoring Employees' Email and Internet Use at Work – Balancing the Interests of Employers and Employees,* 13 JOURNAL OF LAW AND INFORMATION SCIENCE 70, 87 (2002).

[151] See Wheelwright, *supra* note 150, at 86-87.

However, the Commission did establish the test of 'reasonable expectation' in order to determine whether the employees were entitled to privacy in their activities, and did not base its determination on any notion of individual dignity that may have been compromised due to the monitoring of e-mail and internet activity. These decisions can be viewed therefore as being consistent with the American approach of the Australian Commission, despite having reached contradictory conclusions.

Generally, the Australian employment tribunals have been reluctant to read implied privacy terms into existing employment contracts, and few express terms exist.[152] Collective Agreements have not generally been used to regulate privacy issues although they legally can. The end result, so far, is that despite legislation that is at times a world leader in terms of addressing workplace privacy issues, the resolution of these issues is conducted utilizing concepts that emphasize employer concerns at the workers' expense.

***South America – Brazil***

Comparisons of Canadian or American jurisprudence often tend to focus on the EU, or on other common law jurisdictions such as the UK or Australia. It is therefore quite helpful to be able to incorporate the research done within Brazil on workplace privacy, particularly in terms of establishing the degree to which dignity can indeed be viewed as a universal human right in the context of the employment relationship, rather than a peculiar value which is the focus, (and would some venture the obsession?), of the EU and its Member States. An examination of Brazilian workplace privacy can therefore help ascertain the odd person out on the global stage in its treatment of workplace privacy, the US, or the EU.

An encouraging starting point in the search for dignity as a universal value is the Brazilian Constitution.[153] The Constitution states that Brazil is founded on "the dignity of the human person"[154] and goes on to expound on the obligations of the state to ensure the dignity of its citizens.[155] The Constitution further establishes individual rights to privacy, private life, honor and image,[156] and declares the secrecy of correspondence of data and telephone communications (among others) 'inviolable'.[157] Finally, the Constitution creates an individual right to *habeas data* allowing individuals access to information, and a right to correct information, held on them by government or other public bodies.[158] Interestingly, although the Constitution includes a long list of social rights in the workplace, the right to privacy or the right to dignity is not included.[159] The Brazilian Constitution, as can be surmised, is generally more detailed than corresponding common

---

[152] See Wheelwright, *supra* note 150.
[153] An English translation is available on-line at http://webthes.senado.gov.br/web/const/const88.pdf
[154] Title I, Fundamental Principles, § 1-III.
[155] E.g., Title VII, The Economic And Financial Order, Chapter I, *The General Principles of the Economic Activity*, § 170; Title VIII, The Social Order, Chapter VII, *Family, Children, Adolescents and the Elderly*, § 227.
[156] Title II, Fundamental Rights and Guarantees, Chapter I, *Individual and Collective Rights and Duties*, § 5-X.
[157] *Supra* note 156, § 5-XII. An exception exists for criminal investigations.
[158] *Supra* note 156, § 5-LXXII.
[159] *Supra* note 156, Chapter 2, *Social Rights*, § 7. Workers are protected, for the purposes of job security, against 'automation' and that may be interpreted eventually as protection from technological surveillance as well.

law documents it is more similar, for example to the Mexican Constitution than to the American or Canadian Constitutions (that are not always noted for brevity themselves). From the perspective of Brazilian privacy advocates these additional constitutional terms are invaluable, since Brazil has, up until now, not passed information protection legislation (where one might usually expect to find such information privacy principles as the right to access and the right to correction). The degree to which privacy protection is a priority for Brazilians, and therefore the degree to which privacy advocates and privacy concerns figure in Brazilian politics is also not clear.

Brazilian case law on workplace privacy is based of course on the Constitution, but does take into account what I have called the American approach, the realization that employers have interests that need to be protected through surveillance or monitoring in different forms. However, Brazilian case law also reflects the strengths of its organized labor, the reality that e-mail and internet monitoring may not yet be that common in Brazil, and perhaps most importantly, the contextuality of interpretation of key values such as dignity. As a result, the notion of reasonable expectations has not yet made many inroads into Brazilian decisions. For instance, it seems that even in instances where employees are notified of surveillance, consent to surveillance, and the employer monitors employees in accordance with the measures to which they have consented, the courts will not find that as a result the employees have no reasonable expectations of privacy, but attempt to find a balance between the constitutional right to privacy and the practical consent to surveillance.[160] Workers cannot contract out of their constitutional right to privacy, in other words.

As to the ultimate protection awarded to workers on the basis of such (constitutional, in Brazil) values as dignity, it is perhaps a sobering realization for North American advocates of dignity in the workplace that Brazilian workers in many industries have to undergo physical searches on a daily basis as they leave work, yet Brazilian case law has evolved to accommodate both the reality of physical searches and the constitutional right to dignity.[161] Although physical searches are known in some industries in North America one can only imagine the uproar that would ensue if employers, even largely non-unionized retailers suffering from inventory 'shrinkage', attempted to expand this practice. It is important to realize therefore, that although values and employment standards may share a common title across jurisdictions they are ultimately the product of a local culture and a local economy, perhaps even more so in a competitive global era.[162]

Another example where the contextual value of dignity, the strength of organized labor, and the legitimate interests of employers must be made to co-exist lies in the area of medical examinations.[163] Employers are legally obligated to medically test employees before hiring, during work, and prior to dismissal. The results of these tests, however,

---

[160] Joaquim Alvim & Roberto Filho, *Information Technology and Workplace Privacy: A Comparative Study: Part II: Information Technology and Workplace Privacy: The Brazilian Law,* 23 COMP. LAB. L. & POL'Y J. 281, 290 (2002).
[161] Alvim & Filho, *supra* note 160, at 290-291.
[162] Consider the wide range of practices within the EU itself with respect to information protection and the implementation of the EU Data Protection Directive by Member States both old and new. See also Richard Cumbley & Tanguy Van Overstraeten, *History Repeats Itself: Implementation of EU Data Protection Legislation in the Accession Countries,* 15 SOCIETY FOR COMPUTERS AND LAW MAGAZINE 3 (2004).
[163] Alvim & Filho, *supra* note 160, 296-298.

must not result in any discriminatory decision. Once the medical information is collected, however, it becomes difficult for the employer not to make discriminatory decisions on its basis, and indeed to distinguish between those decisions which discriminate and those that do not. In the absence of legislative guidelines the void has been filled by collective agreements, so that for example individuals carrying the human immunodeficiency virus have been guaranteed job security although some employers took the position (misinformed, of course) that dismissal of such individuals might be legal on the basis of their obligation to other employees. Implicitly, the strength of organized labor assisted in securing some measure of personal information privacy to workers in this example, and it is considered by workplace privacy advocates one of the more promising routes to ensuring workplace privacy protection worldwide, given the difficulties of tailoring legislation to suit particular needs.[164]

There are several Brazilian wrongful dismissal cases that suggest both reluctance on behalf of Brazilian courts and tribunals to admit monitoring-based evidence in such cases, and a requirement that employers, as in medical testing discussed above, use information collected through surveillance only for the purposes that were agreed upon with the workers.[165] The insistence that employers comply with their own policies is an important principle, and one that is enforced in many jurisdiction, including the US. The cross-jurisdictional difference lies, of course, in the degree to which each jurisdiction dictates the content of such policies and is not content to merely assume the role of policy enforcer while granting employers a free hand. In that respect, the Brazilian insistence that employers acknowledge the dignity of workers in establishing workplace surveillance measures is encouraging for the understanding of workplace privacy as based on dignity, the cultural-dependent value of dignity notwithstanding.

### *North America*

This section will discuss the three North American jurisdictions and their provisions with respect to workplace privacy. It is interesting, although anecdotal only in the context of this paper, to note how the development of workplace privacy in both Canada and Mexico has been influenced by US conceptions, and how this influence has undoubtedly grown due to the North American Free Trade Agreement. Canada has resisted US influence somewhat more so than Mexico, and is attempting to forge a conceptual middle ground between the US and the EU perceptions of workplace privacy. Mexico, in the meanwhile, appears to be looking for any ground at all, and is devoid of any meaningful privacy protection, whether to workers or to its members of society in general, as can be discerned from the following short overview.

#### *Mexico*

---

[164] See Jeffery, *supra* note 1.
[165] Alvim & Filho, *supra* note 160, at 287, 290, 294-295.

There is no explicit right to privacy or dignity in the Mexican Constitution.[166] Nor is there any protection in the Constitution from privacy invasive measures in the workplace, despite an extensive section in the constitution dedicated to labor.[167] It seems that the Framers of the Mexican Constitution in 1917 had more pressing matters to tackle.[168] Despite the Constitution's lack of explicit protection of privacy there does appear to be in Mexico legal action for Moral Damages, a tort that can manifest itself (among other aspects) as an injury suffered by a person to their honor, reputation and private life.[169] However there are no cases to date in which Moral Damages were claimed or awarded for a breach of privacy.[170] Mexico went through a public scandal in 2003 with respect to personal information in general, with the revelation that the personal information of Mexicans was sold to the US government by ChoicePoint, a commercial data broker.[171] At the time it was thought that the scandal would prompt Mexico to introduce personal information protection legislation in general. However, at this time Mexico still does not have such legislation in place.[172]

In sum, the personal information of Mexicans, and of Mexican workers in particular, is not protected by Mexican law. Employers, whether local or foreign, are free to act with respect to workplace privacy with impunity. In particular, workers are prohibited by the Federal Labor Act to use the employer's resources for any purpose other than the purposes intended by the employer.[173] In effect, employers have inserted explicit terms into their contracts of employment in which workers consent to whatever measures of monitoring and surveillance the employer intends to use.[174] Workers are therefore prohibited by law from private use of workplace resources, and employers are free to monitor and conduct surveillance on employees for any purpose. This situation is in all likelihood a direct outcome of the availability of workers and the lack of government regulation.

*Canada*

---

[166] The Mexican Constitution is widely considered to be modeled on the US Constitution. For example, Article 14 of the Mexican Constitution is similar in content to the Fourteenth Amendment, and could perhaps provide therefore for privacy protection through its stipulation of Due Process. An English version of the Constitution is available at http://www.gob.mx/wb/egobierno/egob_1917_Mexican_Constitution.

[167] Title VI, Labor and Social Security.

[168] In a 1996 Amendment of Article 16 the Constitution does protect private communications explicitly, with an exception for law enforcement purposes. Article 16 itself is similar in content to the US Fourth Amendment.

[169] Mexican Federal Civil Code, § 1916. These can all be understood to be aspects of dignity which is not explicitly mentioned as a value in the Code.

[170] For a discussion of the Code see Jorge Vargas, *The Federal Civil Code of Mexico* available at http://www.llrx.com/features/mexcc.htm.

[171] See a brief report on the incident at http://www.privacy.org/archives/001128.html.

[172] Several drafts of such legislation have been submitted to the Mexican Congress. The latest Senate initiative is reported in English at http://www.senado.gob.mx/english.php?accion=nada&show=summary&lk=febrero_2006/02_summary.htm.

[173] Article 135, available at http://www.cddhcu.gob.mx/leyinfo/txt/125.txt.

[174] See Jorge Vargas, *Privacy Rights Under Mexican Law: Emergence and Legal Configuration of a Panoply of New Rights,* 27 HOUS. J. INT'L L. 73, 119 (2004).

The temptation is always great to cast Canada as a middle ground, actual or potential, between the two poles of the US and the EU approaches to privacy. To a large extent, in the context of personal information, this is a temptation to which one can happily yield.[175] It is not clear whether such a characterization is as correct in the context of workplace privacy, however. The Canadian Constitution, which divides jurisdiction between the federal and provincial levels of government, has been interpreted in a manner that finds most workers in Canada under provincial jurisdiction for the purposes of employment law. Specifically, as mentioned above, this interpretation has led to the conclusion that Canadian federal information protection legislation (PIPEDA)[176] applies only to those workers that fall under federal jurisdiction (among these are workers in the banking industry, telecommunication industry, inter-provincial transportation industry, such as airlines and railways, and more). This, even though the legislation itself applies to commercial transactions within provinces that do not have provincial information protection legislation that has been found substantially similar to the federal legislation by the federal government. Canada, therefore, is unlike the EU in this respect since the EU Privacy Directive has been found to apply to the workplace and has been implemented by the various Member States. Canada is also unlike the EU since its Constitution, even though it includes the Canadian Charter of Rights and Freedoms,[177] does not include an explicit right to dignity or to a private life.

The Canadian provinces have been largely left to their own devices with respect to regulation of workplace privacy, similar again to the US approach. Some provinces have extended protection to the personal information of workers through their private sector personal information legislation, while others have not.[178] Quebec, BC and Alberta all have in place such legislation, with provisions that extend to workers.[179] Interestingly, and I would argue significantly, the legislation of the western provinces permits employers to collect, use and disclose personal information on workers for the purposes of managing the employment relationship as long as the collection, use and disclosure are reasonable.[180] In other words, the legislation does not base the protection of workplace privacy on dignity. Quebec's legislation, at all its levels, however, is based on the protection of a person's private life.[181] It is difficult to establish a common ground to all provinces therefore as some tend to follow the US approach while Quebec quite naturally draws upon the EU (French) approach to workplace privacy.

On the other hand, in terms of employment law doctrine Canada does not resemble the US. The US is largely governed by the doctrine of employment 'at-will' (crudely put, the notion that both employer and employee may terminate the employment

---

[175] See Levin & Nicholson, *supra* note 16.
[176] *Supra* note 12.
[177] *Supra*, note 13
[178] Most multi-provincial employers appear to have opted for a single national workplace privacy policy that would comply with the requirements of these provinces.
[179] In Quebec: An Act Respecting the Protection of Personal Information in the Private Sector. In BC and Alberta: The Personal Information Protection Act (PIPA).
[180] PIPA §§ 15, 18, 21. (Alberta); PIPA §§ 13,16,19 (BC).
[181] The Quebec Charter of Rights and Freedoms applies to the private sector and includes a right to a private life (§ 5). Furthermore, under the Quebec Civil Code not only does every person have a right to privacy (established in Chapter III: Respect of Reputation and Privacy) but employers must respect the health, safety and dignity of employees (§ 2087).

relationship at will, subject to anti-discrimination legislation, and more significantly, without compensating each other).[182] Canada, both statutorily and in terms of its common law, is governed by the doctrine of wrongful dismissal, according to which (crudely put again) employees must be compensated for termination that is not based upon their conduct.[183] For the purposes of workplace privacy the distinction between these two doctrines signifies an American emphasis on the contractual aspect of the employment relationship, whereas Canada does appear to be more open to the possibility that workers have certain rights that cannot be contracted away.[184] In sum, Canada seems therefore to be caught in the middle between the American approach that emphasizes protection only for those expectations of privacy that are reasonable, that views the systems, the resources and the information generated by them in the workplace as the employer's property, and that allows the reasonableness of expectations to be shaped by unilateral notices and policies,[185] and between the general European approach that emphasizes the inalienable rights of individuals, including workers in the workplace, such as dignity, and its implications for the privacy protection.[186] Whether this is stable middle ground, or simply a temporary pause before Canada decides on its course, remains to be seen and perhaps ascertained from already existing Canadian case law and decisions.

However, as in the other jurisdictions surveyed here, there is little Canadian case law to go on. Canadian Privacy Commissioners (federal and provincial) have devoted some time to an analysis of video surveillance in general (e.g., in schools and public spaces) but due there are few findings on workplace privacy specifically.[187] The most significant case, in which the findings of the federal Privacy Commissioner were actually overturned by the Federal Court, revolved a railway employee's (and therefore a federally regulated) complaint about the installation of video surveillance cameras in the workplace.[188] The complaint appears to be the result of a disagreement between the worker's union and the railway over the installation of cameras, which led the employer

[182] The 'at-will' doctrine has been explained sometimes as an attempt to ensure employees are not caught in slavery resembling employment contracts. That may be, but in the vast majority of employment relationships today the doctrine clearly empowers employers.

[183] Strictly speaking workers must be provided with reasonable notice of such termination, or compensation in lieu of notice.

[184] E.g., the Quebec provisions *supra* note 181.

[185] For an analysis of Canada emphasizing the American approach see Marc-Alexandre Poirier, *Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?* 60 U.T. FAC. L. REV. 85 (2002).

[186] For more on the tension between Canadian and American employment law in the context of workplace privacy see Eltis, *supra* note 60.

[187] For example, see Ontario's Privacy Commissioner's guidelines on video surveillance in schools, available on-line at http://www.ipc.on.ca/docs/vidsch-e.pdf and on surveillance in public spaces, available on-line at http://www.ipc.on.ca/docs/video-e.pdf. The guidelines incorporate some common privacy protecting elements, such as the requirement that surveillance be used only in areas where it is necessary, and only for specific purposes, but the 'reasonable expectation' approach as well, advising that cameras not be placed in locations such as washrooms where school staff and students have a reasonable expectation of privacy. Also forthcoming is Robin Bayley & Colin Bennett, *Video Surveillance and Privacy Protection Law in Canada*, *in* Nouwt et al, *supra* note 46.

[188] Eastmond v. Canadian Pacific Railway 2004 FC 852. The case discusses the findings of the Privacy Commissioner, available on-line at http://privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp.

to install cameras unilaterally.[189] Section 5(3) of PIPEDA states that: "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". The Privacy Commissioner did not consider whether video surveillance constitutes the collection of personal information, and therefore established a four-part test to determine whether surveillance was reasonable: "Is the measure demonstrably necessary to meet a specific need? Is it likely to be effective in meeting that need? Is the loss of privacy proportional to the benefit gained? Is there a less privacy-invasive way of achieving the same end?"[190] In so doing the Commissioner did appear to strike a middle ground, constructing a test for (American) reasonableness using a European approach, emphasizing the need for the justification and proportionality of surveillance, yet not basing the findings on any notion of worker dignity.

The Federal Court, as mentioned, overturned the Commissioner's findings.[191] Significantly, the court noted that the railway did not intend to survey employees, but installed the cameras for other purposes (e.g., monitor unauthorized entries, prevent theft and more). The court found, in contradiction with the European approach, that the fact that cameras operate automatically actually serves to reduce the risk of privacy invasion, since it is not at all clear that tapes will ever be reviewed. It is only when individuals review the tapes, ruled the court, that personal information is considered to be collected. So although the court did not dispute the Commissioner's test, it did not answer the test's questions in the same way, and concluded in favor of the railway.

The Privacy Commissioner has issued other findings since this ruling, which are significant since they specifically address the need to balance employer concerns with worker dignity.[192] In a case involving the installation of surveillance cameras in the workplace by an internet service provider (presumably falling under federal jurisdiction – the point is not discussed in the findings) specifically for the purpose of monitoring employee productivity the Commissioner found that the cameras were unreasonable. Although the earlier test was not applied, and despite the fact that workers had been notified of the cameras and the employer's surveillance policy, the Commissioner found that there were other tools at the employer's disposal for monitoring productivity, and that the use of cameras harmed the dignity of all employees, particularly those that were considered to be productive and therefore for which cameras were purely invasive. The Commissioner concluded that video surveillance was unreasonable in the circumstances, since it harmed employee dignity unnecessarily, another example of what may turn out to be a unique Canadian combination of the reasonable expectations test with the value of dignity.

Finally, I should mention a recent decision from the Alberta Privacy Commissioner.[193] In addition to PIPA mentioned above Alberta has provincial privacy legislation which governs workers in the public sector.[194] A library employee complained

---

[189] And therefore a cautionary footnote to those advocating that workplace privacy can be achieved through collective bargaining.
[190] *Supra* note 188.
[191] The case is significant for Canadian privacy law since the court also decided it does not defer to the Commissioner's authority and expertise on privacy…
[192] Available on-line at http://privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp.
[193] Order F2005-03, available on-line at http://www.oipc.ab.ca/ims/client/upload/F2005-003.pdf
[194] Freedom of Information and Protection of Privacy Act, 2000 (FIPPA).

that the library installed keyboard monitoring software on his computer and in so doing collected his personal information in violation of Alberta's FIPPA. The library argued that the software was necessary for monitoring the employee's productivity, part of its operations and activities (a reason that allows a public body, under FIPPA, to collect personal information). However, it also argued, similar to the court's reasoning in the *Eastmond* Case, that no information was collected as long as it was not viewed by human beings. The Commissioner explicitly rejected that argument.[195] But the Commissioner did not completely adopt a European approach in his decision. The Commissioner found that the software was not necessary for the purposes of monitoring the employee and that there were other, less privacy invasive means, at the employer's disposal. In support of this finding the Commissioner emphasized that other employees were not monitored by installing software on their computers, and that only the complaining individual was targeted.[196] So Alberta's Privacy Commissioner, it would seem, would actually be more receptive to across-the-board monitoring, whereas for European information protection agencies monitoring and surveillance that is applied to the entire workplace is of the greater concern. Employers that wish to respect the dignity of workers generally and only target questionably performing individuals could therefore be caught between a rock and a hard place. If they monitor all employees they will be found not to respect their dignity (this seems to be the line of reasoning partially adopted by Canada's federal Privacy Commissioner), and if they monitor only those employees they suspect of under-performing they will be found to use means unnecessary for their purposes (a-la Alberta's Commissioner recent decision). This state of affairs clearly indicates that Canada is only in the initial stages of developing a coherent approach to workplace privacy.

*The United States*

It is often difficult for those immersed in American employment law jurisprudence to imagine that it is possible to construct an alternative approach to workplace privacy that will not be based on the determination of whether reasonable expectations to privacy exist or not.[197] Such an alternative construction has been described as requiring a paradigmatic shift, to emphasis that workers are human beings first, not merely workers that happen to be human.[198] In the meantime, there is no explicit right to dignity, privacy or a private life in the US Constitution.[199] Workers in the public sector enjoy some protection through the Fourth, Fourteenth, and at times First Amendment, yet it is worth recalling, that as with respect to the private sector workers discussed in this paper (that may only rely on tort law for their protection), these Constitutional protections boil down to a test of whether the workers had reasonable expectations of privacy. For example, a court in Ohio decided that school janitors had no reasonable expectation of privacy in their break room, and therefore that covert video

[195] *Supra* note 193, ¶ 9.
[196] *Supra* note 193, ¶ 28.
[197] See for example the renowned privacy scholar Alan Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?* 72 CHI.-KENT L. REV. 271 (1996).
[198] Joaquim Alvim & Roberto Filho, *Information Technology and Workplace Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law: Old and New Paradigms*, 23 COMP. LAB. L. & POL'Y J. 569, 573-574 (2002).
[199] Several states, such as California, do offer constitutional protection to privacy. See e.g., The California Constitution § 1 (1) of the California Constitution. See also Reinhard, *supra* note 92.

surveillance, initiated by the school principal, of the janitors taking unauthorized breaks was admissible as evidence.[200] Such action would most likely violate the workplace privacy provisions of the EU Member States surveyed above.

The US also does not have comprehensive federal workplace privacy legislation. Several states, such as Connecticut, Delaware, Indiana and Illinois have legislation on particular workplace privacy issues such as disclosure of personnel records, or the requirement to notify workers of monitoring and surveillance. West Virginia, for example, restricts electronic surveillance and in particular video surveillance and forbids it, regardless of its stated purpose, if it is carried out:

> in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, shower rooms, locker rooms, dressing rooms and employee lounges.[201]

This is a remarkable piece of legislation in that it appears to do away with the US common law requirement of reasonable expectations of privacy, and appears to provide privacy to workers based on their right as individuals to dignity. West Virginia, however, is the exception to the rule. On the whole there is no workplace privacy legislation at the state level in the US.[202] The US does have of course federal legislation that generally prohibits the interception of electronic communications.[203] However, the legislative definition of electronic communications excludes such communications that are made "in the ordinary course of business".[204] Therefore, it would seem that monitoring and surveillance in the workplace (to the extent that amounts at all to the interception of communication) is not curtailed. Furthermore, interception is allowed when one of the parties to the communication consents to the interception.[205] Such consent can be implied, e.g., from the conduct of workers that continue to work after having been notified that their communication is subject to surveillance and monitoring.[206] Due to the absence of legislation prohibiting or curtailing surveillance and monitoring in the workplace it is of no surprise that such activities are widespread in US workplaces. According to the latest survey from the American Management Association (AMA) 76% of employers monitor their workers' internet connections.[207] 55% monitor and retain e-mails. 50% monitor and review computer files, and 36% (that's one in three!) monitor keystrokes. Telephone use, which is anecdotally assumed by workers to be an area in

---

[200] Brannen v. Kings Local School District Board of Education, 144 Ohio App. 3d 620 (2001). For a discussion of the case and workplace privacy in the public education sector see Ralph Mawdsley, *The Law in Providing Education: School Board Control Over Education and a Teacher's Right to Privacy* 23 ST. LOUIS U. PUB. L. REV. 609 (2004).

[201] W. Va. Code § 21-3-20, Use of Video and Other Electronic Surveillance Devices by Employers Prohibited.

[202] See Faleri, *supra* note 53.

[203] Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

[204] 18 U.S.C. § 2510 (5) (a) (i).

[205] 18 U.S.C. § 2511(2) (c).

[206] For a discussion of the ECPA and US workplace privacy in general see Matthew Finkin, *Information Technology and Workplace Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workplace Privacy: The United States Law,* 23 COMP. LAB. L. & POL'Y J. 471 (2002); Sylvia Kierkegaard, *Privacy in Electronic Communication. Watch Your Email: Your Boss is Snooping,* 21 COMPUTER LAW AND SECURITY REPORT 226 (2005).

[207] The AMA's 2005 Electronic Monitoring & Surveillance Survey, available at http://www.amanet.org/press/amanews/ems05.htm.

which considerable private use is allowed, is also monitored. 51% of employers monitor the usage of telephones by workers in some way. Thankfully, only 15% review voice mail, and only 3% actually review all phone conversations.[208] Video surveillance for the stated purpose of combating theft and other illegal behavior is also used by 51% of employers. Video surveillance for productivity purposes is used by only 6% of employers.[209] 53% of employers use magnetic cards for access control, yet none stated that they use the cards for productivity purposes. Emerging technologies such as GPS and RFID are, as implied, emerging. Less than 8% of employers use these technologies for any purpose.

An equally interesting finding of the survey is how well US employers have learnt the lesson that, in the absence of legislation, the legality of their monitoring and surveillance activities will hinge on the existence of policies that shape the reasonable expectations of workers. With the exception of telephone usage on which the survey is silent, 80% to 90% of employers that conduct some form of monitoring or surveillance actually had a policy in place with respect to the use of the technology in question by workers. Roughly 25% of these employers have terminated workers on the basis of such policies. Notably, only 6% of employers have terminated workers for telephone abuse.

In light of these findings, it is worth noting that little reported case law exists with respect to workplace privacy in the US. The most significant case to date to offer direction to US employers has been ***Smyth v. Pillsbury***,[210] and it is significant since the court found that a worker had no reasonable expectation of privacy even though the employer had a policy in force stating the contrary, specifically that workers will not be terminated on the basis of their e-mails. Although ten years have passed since the ***Smyth v. Pillsbury*** decision, and although it was a trial court decision, it has not been appealed, nor has it been overturned or its scope narrowed in the few cases since. In ***Garrity v. John Hancock*** the court allowed the employer to dismiss the worker on the basis of violating the employer's e-mail policy.[211] A similar decision was reached in a more recent case as well, ***Thygeson v. US Bancorp***.[212] ***Thygeson v. US Bancorp*** is interesting, since the worker was targeted for monitoring and surveillance in order to substantiate a case for termination for cause, which under the employment contract would have allowed the employer not to pay the worker severance pay (Thygeson had worked for the bank for 18 years). Although the monitoring and surveillance was of one individual; although that individual's employment was subject to the employment-at-will doctrine; although as a result the employer did not even need to establish a cause for the dismissal itself and although the end result is targeted surveillance of an individual for a secondary purpose at best (the employer not having to pay severance) the court did not find the outcome an infringement of the worker's privacy. It is hard to imagine a similar outcome in any of the European jurisdictions discussed above.

## Conclusion

[208] It appears to me that these numbers will increase substantially as digital phone systems become more common in the workplace.
[209] It is my expectation that this number too will increase with the advent of digital video recording.
[210] 924 F. Supp. 97 (E.D. Pa. 1996)
[211] 18 IER Cases 981 (D. Mass. 2002)
[212] 34 Employee Benefits Cases 2097 (D. Or. 2004)

The comparative work I have surveyed above indicates that as an explicit human right that bears on workplace privacy dignity exists only within the European Union.[213] Its existence has enabled workplace privacy jurisprudence to develop in a different direction than the corresponding American jurisprudence, based on the notion that some measure of workplace privacy must exist as a minimal standard of employment out of which workers could not contract out, whether explicitly or implicitly through unilateral employer notices and policies. Brazil's Constitution and jurisprudence serves as an excellent illustration of this point, since although in practice many Brazilian workers likely enjoy less dignity at work than their American counterparts, according to the current state of Brazilian jurisprudence dignity is a value that out of which workers cannot contract out.

The practical implications of dignity as a basis to workplace privacy are also realized in the examination of the interaction of two concepts that are often conflated, namely the consent to privacy invasive measures and the notification of such measures.[214] Consent must be given by the worker, whereas notification is carried out by the employer. Yet the US perspective on workplace privacy has created some degree of confusion between the two. Since the American approach emphasizes the property rights of the employer in all workplace resources, and since at the same time workers can seek privacy protection primarily through tort law,[215] the reasonable expectations of privacy, which workers need to prove in order to succeed in litigation, are amenable to change through the unilateral actions of the employer. Coupled with the employment-at-will doctrine, the result is the US conclusion that workers that are notified 'mid-stream' of privacy invasive measures, and that continue to work, are in effect signaling their consent to these measures and relinquishing any reasonable expectations of privacy as a result.

As ideas, however, it is not at all clear that consent and notice are one and the same. Indeed, some notification is necessary for any meaningful consent, but consent does not follow automatically once notice has been given. In the EU for example, where dignity is perceived as the foundation of workplace privacy, mere notification is insufficient. Employers must obtain the consent of workers, often through their collective representatives, to the measures in question and a reasonable expectation analysis is rarely conducted.

The status of dignity within those countries such as Canada and Australia that have attempted to follow the EU's lead on privacy protection (at least in the realm of information protection) is not as well enshrined as it is within the EU. As a result, it is clear from the decisions surveyed above that workplace privacy protection is struggling within these jurisprudences to find a conceptual foothold and not be drawn in into the gaping American whirlpool of reasonable expectations as the 'be all and end all' of workplace privacy. Yet given the different foundations of the EU and the US it is not at all clear that a middle ground such as the one that has been tentatively struck in Canada in cases such as *Eastmond* between the two is tenable in the long run, and indeed the recent findings from the various Canadian Privacy Commissioners may seem to indicate

---

[213] See also Reinhard, *supra* note 92.

[214] For a discussion of the relationship between the two ideas see Roberto Filho & Mark Jeffery, *Information Technology and Workplace Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law: Notice and Consent*, 23 COMP. LAB. L. & POL'Y J. 551 (2002).

[215] Or in the public sector through the Fourth Amendment.

that the Canadian privacy safe keepers are aligning themselves with the EU and attempting to base their findings on the value of dignity, as opposed to analyzing the reasonable expectations in the workplace.

It is clear from the discussion of American jurisprudence that any construction of workplace privacy protection on the basis of reasonable expectations would be akin to building on quicksand. The doctrine knows no bounds, as a result of which several American states have introduced legislation to prohibit certain forms of intrusion by employers into private life.[216] Put differently, these legislative efforts are attempts to construct, on a state by state basis, a minimal standard of workplace privacy. It is most likely that the end result of these efforts, taking past American legislation on other areas such as personal health information into account, will result in a patchwork quilt of workplace privacy protection that will offer some, if less than satisfactory measure of privacy to employees.[217] The jurisprudential difficulty such a quilt faces is of course the lack of a conceptual and a coherent basis for the specific protections created by individual states. Dignity could, and indeed has been, advocated as such a basis yet it is clear that it will not overthrow the rule of reasonable expectations, and the doctrine of 'at-will' employment, overnight.

This predicament has produced calls for the creation of workplace privacy protection in the US, and in other jurisdictions as well, through collective bargaining and the power of organized labor.[218] One suggested model for workplace privacy protection is that of health and safety protection – the joint committee. Accordingly, joint committees for the protection of workplace privacy would be set up at places of employment, to be made up of worker and employer representatives.[219] These committees would then have the role of breathing life and details into invariably general principles of privacy protection that would exist as legislation, similar to the manner in which health and safety general principles (e.g., an employer's obligation to offer 'reasonable' health and safety protection) are translated into workplace reality on a daily basis by joint committees. The present reality of the labor movement in the US however is that of a fractured and beleaguered movement, unable to organize more than 8% of the present workforce.[220] It is possible that workplace privacy will become the rallying flag for a new organizational drive and a revival of American trade unions. Whether it is

---

[216] Although see Swire, *supra* note 3, at 928-930 who suggests that, at least in the area of constitutional law the doctrine of reasonable expectations should be based at least partially on the EU protection of a 'private life' as currently expressed in Article 8 of the European Convention on Human Rights and the EU jurisprudence that has developed subsequently.

[217] Suggestions have been made to regulate information protection in general in the US following scandals involving commercial data brokers similar to the Mexican one mentioned in the section on Mexico. See Daniel Solove & Chris Hoofnagle, *A Model Regime of Privacy Protection,* 2006 U. ILL. L. REV. 357 (2006). However even these latest suggestions would not result in a change to the patchwork quilt approach.

[218] Michael Ford, *Two Conceptions of Workplace Privacy*, 31 INDUSTRIAL LAW JOURNAL 135 (2002) discusses (employer) property and (worker) dignity as the two conceptions, and concludes that collective bargaining offers a resolution to the tension between the two. See also Aranda, *supra* note 59.

[219] A variation of this model calls for workplace privacy protection through joint committees that may already exist at the workplace for other issues, i.e., the EU's Works Councils. See also Faleri, *supra* note 53, at 520-521.

[220] Bureau of Labor Statistics, "Union Members in 2005" available at www.bls.gov/news.release/union2.nr0.htm.

plausible as well, and whether the American labor movement in particular will have the bargaining power to create such joint committees, or play any other substantive role in workplace privacy protection, remains to be seen.

Another suggestion, recognizing perhaps organized labor's relative lack of power in the US, yet remaining within the perception of the employment relationship as a contractual one (and an at-will contact to that) is based on principal-agent theory. According to this suggestion employers, acting as principals, and workers, acting as the employer's agents, may reach an agreement to the benefit of both parties regarding workplace privacy, providing such a contract would jointly establish workplace privacy policies which would be fully disclosed and to which both parties would adhere.[221] While such a suggestion is consistent with the theory at its basis, it is difficult to determine how exactly individual workers would obtain the necessary bargaining power to withstand the more powerful employer who is disinterested in managing the workplace according to principal-agent theory. Indeed, cooperation between employer and workers in the formulation and implementation of any workplace policies would seem to indicate some level of organization among workers, which in the US private sector simply does not sufficiently exist.

Another suggestion, and perhaps a more promising one, is for the independent privacy overseeing bodies (the various Commissions) to take a more active role in the protection of workplace privacy, on the basis of their mandate to govern information privacy, as they have appeared to have done in the EU.[222] Although this suggestion, again, would not go far in the US where there is currently no such body, and only a remote chance that such a body would be created in the future,[223] it might be more appealing to those jurisdictions, such as Canada and Australia, that do already have a Privacy Commission in place. A Privacy Commissioner could afford to take a balanced, consistent and principled approach to workplace privacy, balancing for example the employer's purposes that justify surveillance and monitoring with the workers' right to a private life by examining how relevant the proposed surveillance is to the purposes identified by the employer, and whether the monitoring is proportional to the purpose it purports to achieve.[224] Indeed the Canadian Federal Privacy Commissioner, and subsequently the Canadian Federal Court adopted exactly this approach in the *Eastmond* case discussed above, and it has been advocated for England as well.[225] It would seem that the provincial privacy commissioners, at least in those provinces of Canada that have private sector personal information legislation applicable to workplace privacy, are increasingly interested in workplace privacy issues as well.

---

[221] This is Kesan's suggestion. See Kesan, *supra* note 46, at 322-330.

[222] For an interesting discussion on how the various EU privacy authorities interact see Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807 (2005).

[223] Again, even leading privacy advocates have shied away from calling for the establishment of a body to oversee personal information protection. See Solove and Hoofnagle *supra* note 217. Although see Schwartz, *supra* note 17, at 2115-2116.

[224] For a detailed discussion of the principles of relevance and proportionality and their role in balancing surveillance with workplace privacy, see Christophe Vigneau, *Information Technology and Workplace Privacy: A Comparative Study: Part III: Recurring Questions of Comparative Law: Regulatory Techniques*, 23 COMP. LAB. L. & POL'Y J. 505 (2002).

[225] Oliver, *supra* note 35, at 350-352.

This paper has enquired whether the notion of dignity is at the foundation of workplace privacy protection, such that it is, in several jurisdictions worldwide as can be at best determined through case law, legislation and administrative decisions. The answer is that it is not, with the exception of the EU (and even then, one must allow for the differences between the individual Member States). In key jurisdictions such as the US dignity is unheard of, and in others such as Canada it is struggling to obtain a foothold in the limited jurisprudence that exists on workplace privacy. At the same time dignity has been advocated for as a strong and coherent basis for the protection of workers and their privacy. It seems to me that, notwithstanding the path chosen by the US, the historical development of employment and labor law has been increasingly moving away from a contractual basis and towards recognition of individual rights such as dignity. Dignity manifests itself in workplace areas, even in the US, such as health and safety, and employment standards. Perhaps the time has come for dignity to manifest itself in the area of workplace privacy as well.