University of Cyprus

DEPARTMENT OF BUSINESS AND PUBLIC ADMINISTRATION
MScHRM PROGRAM

IS MONITORING EMPLOYEE'S ONLINE BEHAVIOR BY COMPANIES ETHICAL?

CHRISTOFOROS TRIANTAFYLLOU

NICOSIA
DECEMBER, 2021

ACKNOWLEDGEMENT

I would like to thank my thesis advisor Dr. Seraphim Voliotis. Dr. Voliotis was always eager to help, making sure to impart to me valuable and thorough academic knowledge. My experience of having him as a supervisor left me with nothing but utmost honor, reaping the rewards of getting, apart from academic advice, a precious paradigm of professional expertise.

Contents

Introduction

In this paper, I will argue that for specific combinations of motives behind monitoring with specific types of monitoring, it is not unethical that companies monitor employees’ online behavior. I will first review the international literature in order to find a plausible conceptualization of Privacy and a structured theory of Workplace and Business Ethics. Based on these findings, I will be constructing a test of ethicality. Against these issues, I will be testing different motives and types of online behavior monitoring, again found in the International Literature, in order to find out which ones manage to pass the test and are considered ethical. Lastly, I will propose the findings in the form of a proposition describing which combination of motive and type of monitoring fulfils the requirements of the ethicality of the test, arguing at last that there exist certain cases which monitoring employee’s online behavior is ethical.

Literature Review

Privacy

When studying the international bibliography, it would be a rather rare phenomenon to spot academic analyses of monitoring and surveillance without thorough examinations of the topic of privacy and its ethical or moral realm. Despite its frequent appearance on a plethora of academic papers, it would be false to assume that there is a consensus on how different academics comprehend the term privacy. As a result, conceptualizing privacy can be characterized as a challenging task. This difficulty of reaching a theoretical consensus regarding the general direction that this conceptualization should take, is according to Rössler occurring due to the multiple fields that can be directly related to the adjective "private". Specifically, "…actions, situations, states of affairs and states of mind…" can be private (Rössler, Privacies – Philosophical Evaluation, 2004). In what follows, I will outline the most important theoretical attempts that have been made to conceptualize what privacy is. In this outlining, I will attempt to spot certain limitations of each attempt provided and by the end of this section, I will provide the one direction of privacy that I consider the most appropriate for the purposes of examining the ethicality of companies monitoring the online behaviour of their employees.

Before presenting the most important attempts made in regard to privacy, let me begin with the consequence of the fact that the plethora of different fields which can be characterized as private, causes the task of formulating a generally acceptable conceptualization, to complex one. The main consequence of this complexity is the mere fact that the main theorists of privacy have attempted to escape from the trap of trying to formulate a definition of privacy on the basis of specific sets of personal data that cannot but considered intrinsically private. On the contrary, the theories that are presented in this review are essentially following a different tactic. A tactic which pays no attention to specific categories of personal data that have the necessary and sufficient characteristics of getting the adjective "private" next to them. This I because such is the subjectivity of what might be private and what not, that it would have been impossible to exclude personal domains from the category of data that inherently defines privacy. The tactic which is followed by the theories that are presented here, has a more functionalistic character since it pays attention to the reasons which privacy must be protected. Accounts in favor of this tactic have been offered by both Rössler and Schoemann and they both support the shift of focus on what they refer to as the "value of privacy" whenever there is an attempt to conceptualize it, instead of allowing endless amounts personal affairs or states of mind decide what is and what is not private (Schoemann, 1984). With that said, all the theories presented here, will be essentially making use of this functionalistic tactic.

In an attempt to analyze what privacy is, several theorists have argued that privacy should be identified with intimacy. The main argument in favor of identifying privacy as intimacy comes from Inness. According to Inness, the core of what one conceives as privacy sensitive is motivated by love or care and is more generally strongly related to relations of intimacy (Inness, 1992). It is true that we somehow relate privacy to things that are strongly associated with intimacy or that we feel that there is an encroachment of our privacy whenever someone finds out an intimate personal secret of ours. However, Palm suggests that even though intimacy may be an important part of what we define as private and privacy sensitive, there are also instances of intimacy without privacy concerns (Palm, 2007). For example, a person might feel that an infringement of her political beliefs consists as a violation of her privacy, even though political beliefs have no association with love, care or more generally intimacy. The same applies with other universally acceptable as private matters like personal notes on work tasks, classroom notes or even shopping lists. As a result, a theory which identifies privacy with intimacy would be incomplete and would most certainly cause problems to an analysis of workspace privacy.

Another analysis of what privacy is sources from conceptualizing privacy as premised on and originating from the concept of human dignity. The proponents of such theories suggest that a potential infringement of privacy would necessarily invoke to an infringement of personal dignity (Bloustein, 1964). The question which arises once this theory comes up for discussion, is whether a replacement of the term privacy with the term dignity will actually offer the conceptual inside of the term private. For example, at a moment in which an actual intruding of privacy takes place, subjects can still act in a manner which preserves their dignity. For instance, if there is an accidental leak of an employer's personal e-mails in a particular workspace, the employer may face the consequences of such an intrusion of privacy by maintaining their dignity. As Palm better puts it, "Dignity seems to concern how individuals behave and respond to certain circumstances. An employee may adjust to excessive surveillance or other forms of exploitation with dignity i.e. in a certain manner" (Palm, 2007). Clarifying, the mere fact that there can be times that while privacy is lost, dignity is maintained, conceptualizing privacy as originating from dignity would not stand.

A proposed theory which sustains objections and can successfully propose what privacy is, declares that the value of privacy is to be found at autonomy. According to Rössler, the main proposer of this definition, "…privacy, is valued for the sake of individual liberty and autonomy. Unless privacy is secured, individuals are unable to develop themselves in accordance with their own chosen life-plans (however rough and imprecise these might be) towards a life that is personally rewarding" (Rössler, 2005). In effect, looking at privacy as premised on autonomy means to allow that each individual has the unquestionable ability to be able to solely control specific aspects of their life's which extent both to the physical and to the non-physical realm. Specifically, direct admission to physical spaces and intellectual access to personhood through having the control of who possesses information about themselves are all explanatory of how privacy identifies with autonomy (Rössler, 2005).

Undeniably this autonomy-based theory has also been subject to criticisms. One of the main criticisms against premising privacy on autonomy, concerns the dichotomy between private and public or the so-called problem of privacy in public. In effect, the following of the autonomy-based route for privacy, results in the allegedly paradoxical conclusion that privacy also exists in non-private physical domains, namely public places. Specifically, allowing that for the sake of autonomy-based privacy, a subject should have full control of who possesses information about themselves can be problematic if it does not only apply to a physically private domain. To demonstrate, this syllogism will allow subject X to demand full control of whether subject Y will possess information about the color of subject's X trousers, even though subject X decided to wear her trousers and have a walk at a public road. According to Fried, there is a so-called designated area which operates as framework in which privacy is to be protected. "…This designated area, whose content may differ considerably from society to society, would include intimate or sensitive information, and exclude the so-called "public" sphere from its scope of protection" because including the public sphere to this framework will compromise the rights of others to observe and their freedom to know what happens around them

(Fried, 1968). As a matter of a fact, the autonomy-based theory of privacy does not leave the public domain outside the designated area in which privacy should be protected and therefore can be objected on the basis that allows non-private dimensions to be protected for the sake of privacy, being like this paradoxical.

A response to this objection and to objections that are generally coming from the private and public dichotomy discussion, comes from Helen Nissenbaum. Nissenbaum's paper "Protecting Privacy in an Information Age: The Problem of Privacy in Public", analyzes in detail the shortcomings of the propositions which characterize as paradoxical all definitions or references that allow privacy to have any relationship with instances that take place in the public domain. According to Nissenbaum, theorists who object to the autonomy-based definition in the sake of the private and public dichotomy paradox support that "…information drawn from public spheres, either privacy norms do not apply, or applying privacy norms is so burdensome as to be morally and legally unjustifiable" (Nissenbaum, 1998). In response, Nissenbaum correctly argues that the rapid evolution and advancement in information and communication technology along with the enhanced facilitation of collection, storage and analysis of personal information, have resulted in an alteration in the general meaning of what public is. Further empowering Nissenbaum's view, Regan argues that most contexts which are considered public by the traditional legalistic or philosophical private-public dichotomy, are in reality private ones (Regan, 1998). For example, even though workspace contacts may be established in a professional setting, the actual relationships may be of a private nature. Also, "The domain of work also contains private elements in that employees keep personal belongings in drawers and lockers, and they may personalize their workstation with pots, plants and images" (Brey, 2005). Further illuminating at the limitations of the view in discussion, DeCew observes that “The public/private distinction has sometimes been taken to reflect differences between the appropriate scope of government, as opposed to self-regulation by individuals. It has also been interpreted to differentiate political and domestic spheres of life. These diverse linguistic descriptions capture overlapping yet non-equivalent concepts. Nevertheless, they share the assumption that there is a boundary marking off that which is private from that which is public.” (DeCew, 1997). Her observation further enhances the opinion that the dichotomy is falsely applied as an objection to the narrowness of the autonomy-based theory’s designated area’s boundaries. In fact, there are private moments which take place in public domains and by not specifically excluding public sphere instances, the autonomy-based definition correctly explains privacy, irrespective of where its appearance takes place. All in all, this objection fails to refute the autonomy-based theory and therefore the theory still holds.

As a matter of a fact, the proposed autonomy-based theory, given that it focuses on control that a subject has upon matters that fall under their own personal physical or intellectual realm, decontextualizes privacy. This decontextualization means that judgements concerning potential intrusions of privacy are not based on special places, objects or technologies but on the general relationships which bind them (Palm, 2007). In this context, the concept of private is not fluid or subject to easy change. However, basing the definition of privacy solely to the social relations without having any particular reference to a specific context, entails the danger of opening up the definition so much that every little detail of our everyday reality which concerns us *qua* subjects, will eventually fall under the category of being private – and every interaction with it, will be counted as an intrusion of our privacy. For instance, let us take a look back at our example of subject X’s choice to wear red trousers for morning walk, and subject Y's unauthorized but still completely acceptable freedom to have access to that information.

In this case, I propose that the autonomy-based theory can be slightly modified by adding some extra characteristics to it in order to ensure that is specific enough and does not allow certain examples that nobody would accept as private to be counted as private. In particular, privacy can be identified with autonomy as described above and in addition, a subject's privacy amounts to whatever seems reasonable. To clarify, reasonableness can be found, by first taking the effects of their actions on other persons and their interests into account (Tunick, 2000). To take these into account means that, following the Neo-Kantian constructivism, moral agents are concerned with identifying principles that no reasonable and rational individual could have reason to object to. As Scanlon puts it, "One would be unreasonable by not giving weight to other peoples' moral claims. Most importantly, one is required to take the interest of others into account irrespective of whether these are explicated or not" (Scanlon, 1998).

To sum up, I have provided what I consider to be the most important conceptual analyses concerning the concept of privacy. I have explained and illustrated the limitations of each analysis separately and I have showed why privacy should be explained with the autonomy-based analysis. Overall, Privacy functions for the safeguarding of autonomy. Autonomy is the level of control that each subject exercises on matters that concern themselves both physically and intellectually. The extent of privacy is decided by the principle of reasonableness which is in turn decided by considering the interests and actions of potential third subjects. For the purposes of this paper, I will be using this particular syllogism.

Workplace Ethics

A central part of any analysis which concerns the morality of companies surveilling the online behavior of their employees can account for workplace ethics. In the more general realm of the morality behind businesses, business ethics account for discussions and examinations that concern the business world and have direct implications to morality. The purpose of theorists under the umbrella of business ethics is to present normative or prescriptive arguments which will not just describe the morally challenging situation, but also prescribe or guide towards a particular course of action. Some suggest that Business or Workplace Ethics are no different in nature than Medical, Environmental or Animal Ethics and classical ethical theories suffice in prescribing the course of action in morally challenging situations in a workplace. Others disagree and suggest that the uniqueness of the business world needs a normative business ethical theory. In this section, I will pay attention to existing ethical and business ethical theories which attempt to normatively provide answers to potential moral dilemmas. My aim is to examine each theory carefully, list its limitations and choose which theory applies best for the purposes of this paper. More specifically, the aim of this section is to reach a decision on which particular theory is best to be used in order to examine the ethicality of companies monitoring the online behavior of their employees.

As mentioned above, many theorists believe that classical ethical theories suffice for normatively analyzing the dilemmas which are created in the business world. Such a classical theory is consequentialism. Consequentialism as a theory is generally based upon two relatively basic premises. The first premise claims that “the only thing that is intrinsically good, or good in itself, is well-being. Other things may be good, of course, but only because they are conducive to well-being (or utility, as it is sometimes expressed).” The second premise claims that “the only relevant factor in deciding whether any action or practice is morally right or wrong is its overall consequences, viewed impersonally. The agent is morally obliged to perform any action, no matter what, if and only if it has the best consequences or, as it is also put, if and only if it maximizes the good” (Ellis, 1991). Judging the consequences of any action can either take the form of a future prediction, supposing that the action has not taken place yet, or the form of a value judgement, supposing that the judgement occurs *ex post*. For the purposes of Workplace Ethics, there will be no need for prescriptive action if the actions in question have already occurred. Therefore, all judgements made regarding the overall maximization of the overall good are no more than mere predictions concerning the future. In effect, one of the main shortcomings of consequentialism is that these predictions about the future are most of the times outside the framework of human capacity. Once the discussion comes to workplace ethics, this limitation is rather maximized since most moral problems are situated in complex and very structured contexts in which predictions cannot be easily made, and if made, they will be very vulnerable to be proven inaccurate. In other words, due to the “web of fiduciary, legal and contractual duties” in which every employer and employee is obliged to work within, the so-called maximization of the overall good is very difficult to be predicted and also is mostly compromised so much that the overall good becomes each case’s minimal ideal. (Donaldson & Dunfee, Integrative Social Contracts Theory, 1995). Other than that, one can argue that in the context of monitoring employees, consequentialism can be extensively problematic. Specifically, justifying any action as long as its consequences add value to the overall utility, suggests that the whole discussion on whether monitoring employees *qua* action, is irrelevant. Instead, in the framework of consequentialism, the discussion should be replaced according to the consequences of monitoring employees. However, in this paper I am primarily concerned with the ethicality of the action as an action and adopting consequentialism will essentially elliminate the value of the action *qua* action and focus on other variables. In this context, it seems that consequentialism is a rather unpopular choice for handling the prescriptive guidance of workplace moral dilemmas.

Another alternative from classical ethics is Kant's Deontology. The Deontological school of thought comes into sharp contrast with consequentialism as it pays no attention whatsoever to the consequences of any particular act. Kant's Deontology emphasizes that the key in evaluating whether any kind of act is morally permissible, is the duty of any agent and the rights of any victim. In other words, the focus moves completely away of the action's consequences and solely concentrates on the action's specific characteristics – especially the ones who are directly related to the actions motivating principles (Donaldson, 1991). This so-called aged-centeredness places so much emphasis on the specificity of each subject's own subjectivity that the whole theory receives criticism of not having the ability of being universal. This particular limitation causes Kant's Deontology to lose so much credibility from a normative perspective, because if each case is to be examined separately from other cases, since motives are by nature dependent on their agent's subjectivity, then there is no normative theory at all. Interestingly enough, this problem "…is aggravated in business contexts, where promissory commitments, contracts and, what is more fundamental, the maze of legal and behavioral assumptions constituting a modern economic system such as capitalism, inform virtually all economic rights and obligations." (Donaldson & Dunfee, 1995). Deontological ethics presuppose the existence of certain duties of agents that are obligatory to be followed. In the altar of preserving one’s dignity, a deontologist risks the chance of one’s categorical obligations causing the world becoming a morally worse state of affairs—at least, “worse” in the agent-neutral sense of the word used by consequentialists (Larry & Moore, 2021). As a consequence, even though Kant's Deontology has important implications for corporate problems and economic actors in general, “it must be filtered through so many intermediate obligations and assumptions that its direct application to many business problems” that make it impracticable for workplace ethics (Donaldson & Dunfee, 1995).

It is evident, that classical philosophical theories of ethics do not suffice for providing adequate prescriptions for the course of action in workplace ethical dilemmas. Another alternative that has to examined is the so-called Stakeholder Theory. According to Freeman, Stakeholder Theory is a conglomeration of theories which interpret corporate moral responsibility in terms of weighing and balancing the rights and duties of corporate stakeholders (and not just stockholders) such as employees, customers, suppliers, local townspeople, and stockholders (Freeman, 1984). By putting weight in every possible player of the game the feeling of justice is preserved. However, justice does not identify with morality. The most important limitation of Stakeholder Theory is the fact that it lacks the very normative foundation both for assessing the ethical validity of the interests of stakeholders, as well as for identifying and prioritizing the rights and duties of affected stakeholders. In other words, “Stakeholder theory provides managers with convenient rules of thumb for mapping moral obligations, but it nonetheless lacks the normative sophistication necessary for making precise moral distinctions in moral dilemmas” (Donaldson & Dunfee, 1995). This structure-less format does not allow the Stakeholder Theory to take the place of an adequate normative workplace ethical theory and has to be abandoned.

For a number of different reasons that are to be analyzed, there is a specific proposed theory which designs a quite specific normative framework which realistically provides ethical guidance for the workplace world. This theory is proposed by Donaldson and Dunfee and it is called Interactive Social Contracts Theory. The last part of this section will be devoted to the detailed analysis of this theory.

To begin with, there is a need to understand a foundational assumption which binds all moral agents and all types of different ethical structures: There are “limits on the ability of general moral theory to model the full range of accepted moral convictions and there are limits on the conceptual ability of individual moral agents to discover and process morally relevant facts.” (Donaldson & Dunfee, 1995). This is called “bounded moral rationality” and differs from one ethical context to another. In the context of business ethics, it is plausibly argued that the high element of artifactuality which is present in the construction of any economic or business concept, causes workplace ethics to be subject of strongly bounded moral rationality. According to Donaldson and Dunfee, this strongly bounded moral rationality aids towards the explanation of at least three different features of business ethics: “1. Moral norms governing socio-economic interaction vary enormously. 2. Moral preferences relative to economic institutions and transaction environments shift significantly over time. 3. Using abstract, universal concepts of ethics to solve specific ethical dilemmas in business is notoriously difficult.” (Donaldson & Dunfee, 1995).

Still, it is obligatory for any normative framework, that there is a conceptual consensus between all agents who participate in this economic normative framework, for a hypothetical “macro” social contract that all agents will be bound by in order to then establish all those “micro” contracts that will be open to variance, since business and workplace affairs are strongly bounded to moral rationality. This hypernorm is based in two assumptions concerning moral agents: 1. Desire to satisfy their economic interests, 2. Wish to participate in economic systems which represent their cultural and economic values (Donaldson & Dunfee, 1995). The main advantage of Integrative Social Contract Theory is that it recognizes the diversity which exists between different economic affairs by allowing that the creation or abolition of micro social contract norms to depend upon the informed consent of all members of each community, as long as it does not come to conflict with hypernorms. Lastly, in order to avoid the limitation of the absence of structure or weighting that the Stakeholder Theory avoids, Integrative Social Contract Theory obliges the participating moral agents to follow certain priority rules between the micro social contract norms in order to avoid conflicts between mutually exclusive norms. In this context, the normative framework which is developed by Donaldson and Dunfee can be summarized into the following terms:

1. Local economic communities are to be allowed moral free space to generate obligatory ethical norms for their members through microsocial contracts.
2. Norm-generating microsocial contracts must be grounded in consent, buttressed by the rights of voice and exit.
3. In order to be obligatory for members of the community, a microsocial contract norm must be compatible with hypernorms.

4. Priority rules compatible with principles 1-3 must be employed to resolve conflicts among competing, mutually exclusive microsocial contract norms.

(Donaldson & Dunfee, 1995)

Overall, Integrative Social Contract Theory does not require agents to carry out predictions about the future, which are beyond their human capacity. Moreover, It allows the existence of a relatively high amount of variance between each community but demands a standard compatibility with universally agreed hypernorms, allowing it to refrain from being either too agent-centered or too universal and distant from the strongly bounded to moral rationality which characterizes economic and business affairs. Finally, it predicts the potential problems that conflicting micro social norms will generate if they are mutually exclusive and suggests their prioritization. In this context, Integrative Social Contracts theory provides an adequate normative framework that will sufficiently aid any potential moral agent in the workplace be guided towards a specific course of action. Indeed, it manages to avoid the exposition to the same limitations that traditional philosophical or business ethics theories had. As a result, Integrative Social Contracts theory is the best possible theory to apply when examining whether it is ethical on behalf of companies to monitor their employees' online behavior.

Monitoring and Surveillance

Before moving forward to the central part of this paper, the last section of this Literature Review to the discussion of workplace monitoring. The analysis of whether it is ethical on behalf of companies to monitor their employees' online behavior should before commencing analyzing, refer to how previous academic analyses have accounted for specific examples of workplace monitoring. To this brief section which follows, I will attempt to outline the reasons behind surveilling employees and the different types of surveillance as listed in the international bibliography.

The motives of company surveillance can be separated into two categories: employee-based surveillance motives and company-based surveillance motives. According to the literature, employee-based motives mainly concern monitoring of efficiency and performance. Specifically, companies tend to align worker performance with organizational goals and compare workers to each other in terms of work performance and efficiency. The data that is collected from this monitoring is often used for predicting optimum staffing level, skills, and capability combinations (Ball, 2003). Along with the monitoring of performance, companies sometimes surveil their employees in an effort to monitor their workplace behavior, deter and control abuse of employee relationship (Miller & Weckert, 2000). Moreover, especially companies which possess production methods that involve several medical hazards, carry out monitoring and surveillance in order to protect their employees from hazardous exposure. In countries where the Health Insurance System is run privately by insurance companies paid by the employer, some companies request genetic information from their employees and carry out long-term surveillances of genetic screening (Sorsa & van Damme, 2005).

Company-based motives, concern motives which are directly related to the company’s assets, except employees. Specifically, companies sometimes surveil in order to “protect work premises, stock and means of production” (Miller & Weckert, 2000) and “To protect property against damage, misuse and theft” (Fairweather, 1999). Apart from that, companies sometimes surveil in order to have evidence in potential suits that their premises and workplace environment complies with the regulatory framework or that it promotes certain public considerations (Palm, 2007).

As long as the different types of surveillance are concerned, international bibliography refers to a number of different kinds. In effect, companies' main aim in selecting the exact methods that they will be using in order to monitor their employees is no else than to satisfy the aforementioned motives of surveillance. For instance, their need to monitor their employees' performance level is either satisfied by specifically performance measuring computerized technology that is placed at the employees' computers (Garson, 1988) or takes place by actual observers through real-time computer screening observation (Forester & Morrison, 1990). Monitoring interpersonal employee behaviour or measuring skills, abilities and special strengths or weaknesses is sometimes done through the monitoring of e-mail (Severson, 1998) or the monitoring of social media (Ghoshray, 2013). Finally, a method which surveys show that is even favourably seen by several workers (Loch, Conger, & Oz, 1998), allows camera surveillance in the premises in order to spot who are the free-riders and who are the hard-working ones (Merz Smith, 2004).

To sum up, I have outlined what I consider to be the main motives of surveillance and the different types of surveillance which companies use in order to monitor their employees. In what follows, I will attempt to answer to the question of whether it is ethical for companies to monitor their employees' online behaviour. My answer will consist of a proposition that will consider the preceding selected definition of privacy along with the preceding selected normative business ethics theory to normatively decide upon the ethical permissibility of the question. This whole philosophical discussion will be concerned with the motives and types of surveillance of this last section.

Discussion

Terminological Analysis

Prior of beginning addressing the question contextually, I will be paying some attention to the terminological aspect of each element of the topic. Even though, this paper is purely philosophical and a detailed discussion of semantics will definitely fall out of its scope, clarifying what exactly each term that is used refers to will safeguard the discussion from any potential linguistic misunderstandings.

For the purposes of this paper, the term "monitor" refers to watching and checking something over a period of time in order to see how it develops, so that you can make any necessary changes (Oxford Dictionaries, 2021). In effect, monitoring implies an action which essentially requires the activity of observing and the characteristic of change. Monitoring is not an action which is occurring only once, but an action which necessarily repeats itself over time in order for the subject who is performing it to be able to track the development of the object that is monitored. Monitoring can take place with a number of different methods varying from real-time or recorded watching of camera footage to reading and analysing different kinds of digital footprint. However, the term monitoring does not alter reference or meaning depending on the methodology of observation, as long as, the crucial element of development is part of the equation. To be clear, if the monitored object presents a potential absence of any development or change of any form whatsoever, this does not in any case imply that what occurred has diverged from the reference of "monitoring". In fact, the subject's intention to track the development of the object in addition to the actual tracking occurring suffices for what is referred as "monitoring" even though there is no observed development.

Likewise, for the purposes of this paper, the term “online behaviour” refers to the functional and interpersonal behaviours of people whilst online (IGI Global, 2021). Here, the term “online” should be taken with caution. “Online behaviour” is unlimited to every interaction that a user has whilst surfing the web. Specifically, whenever I refer to “online behaviour”, I refer to all the actions which have the capacity of leaving behind a digital footprint. To be more specific, the user’s behaviour is online both when she responds to e-mails of colleagues or clients and when she just fills out fields of a large Excel file. In effect, for the purposes of this paper, the term “online” could have been replaced with the term “digital”, since I am only concerned with the ethicality of monitoring employees’ conduct via systems that will observe their overall digital conduct. In this sense, this paper is not concerned with the monitoring of employees’ digital behaviour whilst online on personal time, like Social Media posts or personal screen time at all. On the contrary, the normative analysis strictly concerns the monitoring of employees during working hours and different types of this monitoring will be extensively analysed in the next sections.

Lastly, for the purposes of this paper, the term “ethical” refers to whatever passes the test of moral permissibility. The test of moral permissibility, tests: 1) Any activity of monitoring online behaviour to whether it intrudes the autonomy-based conceptualization of privacy while always taking into account the element of reasonableness; and 2) whether it violates at least one of the four terms of “macrosocial contract” of Integrative Social Contracts Theory. In what follows, each motive of monitoring along with each type of monitoring of online behaviour will be analysed by the consequences it causes on these two issues. The aim of this paper is to select from this list of different potential monitoring motives and activities of online behaviour, if any, the ones which are morally permissible, if “morally permissible" refers to successful completion of the two parameters described above. If any combination of specific motive and monitoring activity passes this test, then it can be plausibly argued that this particular combination necessarily constitutes an ethical way to monitor the online behaviour of employees and consequently the question of the topic is affirmatively answered. Respectively, if no combination can be spotted, the question of the topic is negatively answered. To clarify, finding a single, two or three combinations successfully completing the test does not in any case whatsoever suggest that it is ethical to monitor employees' online behaviour. Specifically, this suggests that it is ethical to monitor employee's online behaviour if and only if this or these particular combination or combinations of motives and types is followed.

Summing-up, this previous section concerned the terminological aspect of the analysis that is about to follow. The obligation to specifically clarify the semantics of each of the terms that will be used in this paper separately has been fulfilled and its fulfilment will mark what follows free from any potential linguistic misunderstanding.

Motives of Monitoring

Employers have reasons to monitor their employees. To decide upon the ethicality of these reasons, however well- or ill-intentioned may generally seem, close inspection is required. In this section, I will be closely looking at each particular reason separately. My aim is to analyse every motive of monitoring in regards to its need and test it over the two aforementioned parameters of ethicality. Namely, reasonableness and potential intrusion of privacy conceptualized as autonomy, and the terms of Integrated Social Contracts Theory's "macrosocial contract". This will allow the paper to decide whether a motive of monitoring can be considered ethical or not. Given the vast amount of motives and the even more vast amount of submotives that exist not just for monitoring but for any human action, this section will only pay attention to perhaps the most famous and larger category of motives in regards with monitoring. The one concerned with performance and efficiency tracking.

One of the most famous motives category for employee monitoring is the general tracking of an employee's performance and efficiency. Specifically, companies tend to align worker performance with organizational goals and compare workers to each other in terms of work performance and efficiency (Ball, 2003). Effectively, performance improves if potential mistakes are minimized and in order to spot those mistakes it can be argued that one has to monitor their employees. Other than that, employees can improve their performance by not just avoiding potential mistakes, but by also enhancing potential practices that they are doing correctly. Again, it is the employer's job to let the employee know how to keep doing something which increases her performance, and it will be impossible to do that without somehow monitoring the employee. Additionally, a crucial factor which affects performance rates, concerns productivity. By having a good idea of how an employee spends her time online, the employer can have an idea of productive and unproductive working intervals, as well as potential websites which aid procrastination instead of productivity. Lastly, monitoring employees can have an automatic effect on the productivity of employees simply because they know that they are being monitored. Specifically, employees tend to be more focused and less distracted in their work, if they know that they are being monitored, something which improves the overall efficiency and productivity of any firm (LaMarco, 2019).

In substance, the employee-based motive that is described above clearly concerns the tracking and the constant need of improvement of performance and efficiency.

Such a motive sources from the unquestionable need for employers to increase the profits of their firm. Monitoring of performance and efficiency can take up different technical forms which are in essence all concerned with the comparison of figures to predict optimum staffing level, skills, and capability combinations (Ball, 2003). Such outcomes can be calculated by monitoring digital footprint that will allow any employer to know how an employee uses her online time, what does she do and how she does it as long as work functions are concerned and how much working time she spends online without carrying out tasks which concern her job.

To decide whether this motive and irrespective of the type of monitoring that it will accompany it, is ethical or not, one has to test it against the parameter of the intrusion of privacy and Integrated Social Contracts Theory. Beginning with privacy, this is the right moment to remind ourselves that looking at privacy as autonomy means to allow that each individual has the unquestionable ability to be able to solely control specific aspects of their life's which extent both to the physical and to the non-physical realm. Specifically, direct admission to physical spaces and intellectual access to personhood through having the control of who possesses information about themselves are all explanatory of how privacy identifies with autonomy (Rössler, The Value of Privacy, 2005). In terms of observing and monitoring performance via digital footprints, there is no direct encroachment of privacy if the latter is conceptualized as autonomy. To clarify, the mere knowledge of an employee that she is being monitored does not necessarily prohibit her from controlling the specific life aspect of choosing how to carry out her working tasks, how much working time she will spend on unrelated to work websites or how productive she will decide to be on Mondays. What essentially violates this access to personhood and consequently privacy, is mandating the accesses of her online behavior. Strictly speaking, prohibiting employees to access specific websites or use specific methodologies to carry out their task because comparing monitored online data have suggested so, cannot but be considered as an encroachment of autonomy which results in an intrusion of privacy. In effect, according to the autonomy-based conceptualization of privacy, monitoring with the intention of improving performance does not intrude privacy, whereas actively interfering does. A potential refutation of what is argued here could be that the simple knowledge that the employee possesses that she is being monitored is enough to influence and consequently alter her decisions and choices, which will result in the violation of autonomy. However, in this case, this is not something which is directly related with the act of monitoring in-itself, but with the conceptualization of monitoring by the employee herself. As a result, a verdict that would judge the motive of calculating performance as unethical just because there are employees who allow their autonomy to be influenced by that mere knowledge, would be unfair.

It is very important not to omit that the autonomy-based conceptualization of privacy on its own does not suffice to judge whether there is a violation of privacy. In particular, privacy can be identified with autonomy, but a subject's privacy also amounts to whatever seems reasonable. To clarify, reasonableness can be found, by first taking the effects of people's actions on other persons and their interests into account. Then reasonableness is calculated by comparing one's own understanding of effects of one's actions and comparing and contrasting them with the former. In the case of monitoring with the intention of calculating and improving performance and efficiency, it can be considered reasonable for an employer to first advise, then warn and then take measures against employees who repeatedly ignore their employer's directions in terms of how they should spend their time online. Likewise, it can be considered unreasonable to prohibit the access to specific websites that are unrelated to the tasks an employee has to carry out. By the same logic, it can also be considered unreasonable to not prohibit specific Not-Safe-For-Work websites just because this will potentially intrude the autonomy of an employee. Clearly, an employee will need to conceptualize the effects of both active and passive monitoring on employers before reaching a decision in regards with reasonableness. However, as shown above there is enough argumentation to suppose that passive monitoring with sensible advisory character in order to improve performance and efficiency does not in any case intrude privacy conceptualized as autonomy and hence passes this part of the test.

The second part of this test refers to the Integrated Social Contracts Theory. For any emerging ethical norm, Integrated Social Contracts Theory, demands that it is authentic, legitimate and in case of conflicting norms, it is higher in priority than its opponent (Donaldson & Dunfee, Integrative Social Contracts Theory, 1995). More precisely, authenticity of a norm is granted if and only if the majority of a community complies with the norm irrespectively if it personally likes or dislikes the norm, given that there is an already established free moral space for the community to schematize its own norms and there is an already established consent from all members to be part of this community, having any right to voice their concerns and of course exit. Additionally, legitimacy of a norm is granted if there is no conflict of the norm to an existing hypernorm.

In the case of the motive norm of tracking performance and efficiency, if that norm is exercised passively and all its consequences have an advisory character, it is reasonable to claim that authenticity is granted. Of course, the ultimate decision of whether this norm is passes all the terms of the macrosocial contract will necessarily depend upon the majority’s voice and in order to ensure this majority’s voice, any employer who wishes to abide with workplace ethics and wishes to follow the normative directions that I present here, shall ensure that all the employees are asked whether they approve this specific intention category of motives. This can be done through surveys or internal interviews. Assuming that the employer also informs her employees once they accept the offer as part of their contractual agreement then one could argue that authenticity is granted. However, an issue that usually causes problems to the authenticity element of the equation and the case of monitoring-to-track-performance can be no exception, is the issue of members being forced or coerced to join or remain members of a community. Clarifying, in the case of having a number of employees disagreeing with the norm of monitoring in order to track performance, there is always the right to exit. This right will basically naturally grant the authenticity of all norms that a community follows, given that consent of all members ensures authenticity, and consent is granted if and only if the community has provided the members with the unquestionable right of exit and any originally consenting party has continued actively as a member of a community and has not exercised her right to exit, it means that she consents (Donaldson & Dunfee, Integrative Social Contracts Theory, 1995).

The issue remains though, because one has to calculate the opportunity cost of a member exiting or even voicing their concern as part of a community. Specifically, especially during the context of this current economic era, it is certainly a very difficult for employees to exercise their right of exit, in the face of the fear of unemployment. Especially in some countries of South Europe, it would be plausible to argue that a great number of employees are coerced not to exit their communities, something which makes the whole mechanism of the right of exiting and sometimes the right of voicing superfluous. Analogically, Hume puts it perfectly: “Can we seriously say that a poor peasant or artisan has a free choice to leave his country when he knows no foreign language or manners and lives from day to day by the same small wages which he acquires?” (Hume, 1953). As Donaldson and Dunfee put it, it would make no sense to suppose that the mere fact that there are some costs associated with a decision can be considered to limit a finding of consent (Donaldson & Dunfee, Integrative Social Contracts Theory, 1995). This claim has validity if and only if these costs are not at a point of highness in which coercion replaces consent.

To ensure the manifestation of the rights of exit and voice, along with ensuring that the majority of community members comply with the monitoring in order for tracking performance and efficiency, employers could make this monitoring optional. By asking employers once a month whether they consent that their digital footprints would be monitored by their manager, the employer safeguards that: 1) there is a right of what is equivalent to civil disobedience (a discontented member of any community, believing that a norm of that organization violated a hypernorm, could deny the legitimacy of the norm through her refusal to follow it); and 2) that a substantial majority of the members of any community, when coming face to face with the option of being monitored in order to track their performance, comply with this norm. One can plausibly assume that there is going to be a majority that approves the nascent norm of monitoring in order to track the performance and efficiency not necessarily out of fear of losing their job but because of their need to receive feedback and develop as employees. By giving an option to employees as described above, the employer basically manages to fulfill the authenticity prerequisite.

As long as legitimacy is concerned, in order to fulfill the legitimacy prerequisite there has to be an absence of a conflicting hypernorm. Specifically, if a hypernorm which explicitly prohibits the monitoring of employees in an effort to track their performance is spotted, then the microcosmic norm would be illegitimate. The only thing which naturally comes to mind are hypernorms which concern intrusions of privacy. However, this has been explicitly analyzed in the previous section, granting that there is a specific way of carrying out monitoring which does not violate autonomy-based reasonable privacy. As long as priority rules are concerned, this does not concern any employer, because there is no conflicting micro-norm that must be compared and contrasted with the norm of monitoring in order to track performance and efficiency.

Overall, I have paid attention at the motive of monitoring which is concerned with tracking performance and efficiency. I have tested it against two different questions: 1) If it violates the autonomy-based conceptualization of privacy, while having in mind the reasonableness parameter and 2) If it abides with the all the terms of the macro-social contract that is presented in Integrated Social Contracts Theory of workplace and economic ethics. Thus, I have concluded that as long as motives of monitoring are concerned, it is ethical to monitor employees' online behavior in order to track performance and efficiency as long as: 1) This motive of monitoring would have a passive character of tracking by ensuring that the consequences of this monitoring would have an advisory character; 2) That a monthly option is given to each employee not to consent to this monitoring due to the motive; and 3) That the majority of the firm's employees consent with this motive of monitoring.

Types of Monitoring

To fulfil their motives described above, different employees follow a plethora of different types of monitoring. The aim of the section which follows is to pay close attention to a number of different types of monitoring and test them against the two aforementioned parameters in order to decide which exact type of monitoring can be considered ethical. Following the same strategy as the previous section, in this section I will only be involved in commenting upon types of monitoring which have to do with the tracking of performance and efficiency of employees. Using this procedure, will allow me to afterwards combine what I have argued are the ethical motives with what I will be arguing here are the ethical types of monitoring (if any) in such a way that I will be proposing in what exact circumstance under which exact motives and under which exact methodologies, it is ethical for companies to monitor employees' online behavior.

The need of companies to monitor their employees' performance level is either satisfied by specifically performance measuring computerized technology that is placed at the employees' computers (Garson, 1988). This usually takes the form of specific pre-designed Employee Monitoring Software, which usually comes as an up-to-measure for each firm separately. Moreover, the online activity of each employee can be tracked down and monitored by methods like Stealth Monitoring or Keylogging. Stealth Monitoring involves covertly using video monitoring technology not to record the screen of an employee, but to essentially record a user's digital activity (Stealthmonitoring, 2021). Quite similar is Keylogging, with which employers have the ability of covertly recording input signals into a computer from a keyboard so that the computer user is not aware. Keylogging can be accomplished by means of various methods - both software and hardware - ranging from low-level rootkits and operating system level API-based programs, to physical devices connected in-line with a keyboard’s connection to a computer and analysis of electromagnetic signals emitted by a target keyboard from up to 20 meters away (radware, 2021). Alternatively, monitoring takes place by actual observers through real-time computer screening observation (Forester & Morrison, 1990). The method of the self-explanatory Screen Recording along with the traditional method of CCTV cameras fall under this category. Finally, Monitoring interpersonal employee behaviour or measuring skills, abilities and special strengths or weaknesses which are closely related with performance and efficiency levels, is sometimes done through the monitoring of e-mail (Severson, 1998) or through the monitoring of Network Traffic of the company.

The first part of the dipartite ethical test which this paper follows, is the privacy conceptualized as autonomy part. This suggests to allow that each individual has the unquestionable ability to be able to solely control specific aspects of their life’s which extent both to the physical and to the non-physical realm. Specifically, direct admission to physical spaces and intellectual access to personhood through having the control of who possesses information about themselves are all explanatory of how privacy identifies with autonomy (Rössler, The Value of Privacy, 2005). One can plausibly argue that just from this manifestation, any particular type of surveillance which occurs covertly, that is without the employee having the knowledge that they are being monitored fails to pass the first parameter of the test. Effectively, by secretly monitoring an employee’s actions, the freedom of direct admission to personhood along with the freedom of having the complete control of both the specific aspects of their lives and who else, where and how has access to these specific aspects of personhood, is irreversibly harassed. Even if for the sake of the discussion, suppose that covert methods of monitoring pass the first part of the test, they would still fail to prove that they consist of a relatively reasonable method, since one can assume that employers, as part of calculating how consequences of their actions would have impacted other people, they would all agree that they would never wish under any circumstance whatsoever that their own online behavior shall be monitored by others. Again, even if reasonableness was still granted, any covert monitoring methods would immediately drop once the authenticity term of macrosocial contract of Integrated Social Contracts Theory came into context. This is because the authenticity term demands from the nascent norm to allow all members of any community to have the complete right of voice and buttressing rights of entry and exit. By not having any knowledge of being monitored, there can be no discussion of consent and apart from that there can also be no discussion about legitimacy, since the violation of the hypernorm of deceiving other people by willingly hiding information which concerns them would be universally unacceptable and most importantly impermissible. As a result, all covert methods of monitoring like Stealth Monitoring and Keylogging get immediately out of question.

As long as Screen Recording and CCTV cameras are concerned, the main difference is that in this case there is the element of informing all employees about the presence of these methods. However even if deceiving the employees gets out of the picture in these cases the freedom to freely choose who has access to personhood is once again violated. Specifically, CCTV cameras that will monitor all the movements of the employee will also monitor not-work related activities that inevitably occur during work. From what flavor of tea bag an employer uses, to how many times they are using the toilet to personal health characteristics like back-pains or itching, the employer inevitably has access to areas of personhood that an employee never consented that they should have. Likewise, Screen Recording will record the musical preferences of the employee, if the employee decides to use his computer to listen to music whilst working. Given that autonomy is not a problem, the unethicality still remains because it is unreasonable for an employer to monitor not work-related features of an employee's working hours. As a result, Screen Recording and CCTV cameras do not pass the test too, leaving us with only too options to test for moral permissibility.

The monitoring of the employees' online behavior by Employee Monitoring Software and E-mail monitoring are methods which are specifically designed for the monitoring of employees. Employee Monitoring Software and E-mail monitoring does not "see" a real-time recording of any employee's screen. Instead, it uses an algorithm which understands and categorizes different working activities of any company which designs such a software. These categories are then further compared and contrasted with their appropriate KPI's (Key Performance Indicators) as those are set by the company. In essence, the company does not have direct access to what exact activities consist of the online behavior of an employee, but sees an overall summary of what categories of activities an employee has taken part in over a larger period of time (Biz-Doctor, 2021). This way, there is no intrusion of autonomy whatsoever, since the choice of the employee to listen to what music he likes or spend as much time of a single day to specific tasks is granted. Apart from that, it comes out as a reasonable alternative to companies having full and direct access to their employees', since there are things that they have no reason to have access whatsoever. In the same way that the motive discussion moved forward, the only way to guarantee that the involvement of all employees to this particular norm will consist of an authenticated decision, is to grant that companies will not only inform their employees about the Employee Monitoring Software (How it works etc.), but also allow them not to consent and giving them the option to abstain from being monitored through this software. This will grant the buttressing rights of exit. Moreover, the organization of frequent focus groups or internal interviews will guarantee that the right of voice is safeguarded. Finally, the calculation of who consents and who does not will give the opportunity to companies to further test the ethicality of the whole claim, due to the fact that if the majority consents then terms 1 and 2 of the macrosocial contract of Integrated Social Contracts Theory are fulfilled. In effect, given the absence of any conflicting hypernorms which in this case is most probably granted given that any possible violated hypernorms will have to do with privacy intrusions which were handled in the previous paragraph, and in the absence of any mutually exclusive micro-norms that are violated, Employee Monitoring Software and E-mail Monitoring can be considered ethical types of surveillance if and only if they are open to the employee's choice and there are not covert.

Overall, I have argued that as long as types of monitoring are concerned, it is ethical to monitor employees' online behavior, if and only if this happens via pre-designed up-to-measure Employee Monitoring Software and E-mail monitoring, giving the full option to employees not to participate in that kind of monitoring, happening in a non-covert way and having a majority of employees following it.

The Proposition

In this paper, I have argued that monitoring employee's online behavior by companies is ethical if and only if:

1. The motive of monitoring and the type of monitoring would have a passive character of tracking;
2. The consequences of monitoring would have an advisory character;

3. The employees will only consent to participate in the scheme of monitoring if they wish to;
4. The majority of employees consent in the monitoring scheme.

Following the aforementioned premises and the discussion which preceded, I propose that monitoring employee's behavior by companies is ethical if and only if:

1. The motive of monitoring directly relates to the tracking of performance and efficiency and nothing else;
2. The monitoring happens via pre-designed up-to-measure Employee Monitoring Software and E-mail Monitoring;
3. All the Employees are priory informed, the majority has consented, and participation is optional.

Given the fact that not each and every single motive of monitoring has been examined and also given the fact that not each and every single type of monitoring has been examined, one could accuse the scope of this study limited. However, in my defense, this study has paid attention to the most famous motives and the most famous types of monitoring employee online behavior. For any motives or types of monitoring that are not included in this study, there is a land of endless opportunity to develop and evolve the present theory in potential future studies. Sensibly, the procedure of combining a widely accepted conceptualization of what privacy is, namely autonomy with reasonableness in its limits, with a structured workplace business ethics theory, namely Social Contracts Integrated Theory, is what makes this study's contribution and what it essentially has to offer.

Conclusion

I have studied the ethicality of monitoring employee's online behavior by companies. To do that, I have constructed an ethicality test which tested different motives and types of monitoring against three different parameters: The potential intrusion of an autonomy-based conceptualization of privacy, the reasonableness of each context of privacy's limits and the terms of macro-social contract of Integrated Social Contracts Theory as analyzed by Donaldson and Dunfee. I have proposed that it is ethical for companies to monitor employees' online behavior if and only if the motive and type of monitoring successfully passes the three aforementioned parameters of the constructed ethicality test. In this context, from every example analyzed, I have proposed that it is ethical for companies to monitor employees' online behavior if and only if this is done via pre-designed up-to-measure Employee Monitoring Software and/or E-mail monitoring with the motive of tracking down the performance and efficiency of employees, informing them prior to their participation in the monitoring scheme, securing a majority of employees consenting and any potential consequences of the passive monitoring occurring having an advisory character. Even though there is an endless land of research opportunity for untouched from this study motives and types to be deeper analyzed, the procedure of this study is unique, reliable and most importantly supportive towards deciding if monitoring employees' online behavior is ethical or not.

Bibliography

Ball, K. (2003). Categorizing Workers: Electronic Surveillance and Social Ordering in the Call Centre. In D. Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.* New York: Routledge.

Biz-Doctor. (2021, December 11). *Types of Employee Monitoring* . Retrieved from Biz-Doctor.com : https://biz30.timedoctor.com/types-of-employee-monitoring/

Bloustein, E. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Posner. *New York University of Law Review 39*, 962-1007.

Brey, P. (2005). The Importance of Privacy in the Workplace. In S. O. Hansson, & E. Palm, *The Ethics of Workplace Privacy.* Brussels: P.I.E Publisher.

DeCew, J. (1997). *In Pursuit of Privacy: Law, Ethics and the Rise of Technology.*

Donaldson, T. (1991). Kant's Global Rationalism. In T. Nardin, *Traditions of Ethics in International Affairs* (p. Chapter 7). Cambridge: Cambridge University Press.

Donaldson, T., & Dunfee, T. W. (1995). Integrative Social Contracts Theory. *Economics and Philosophy*, 85-112.

Ellis, A. (1991). The idea of utilitarianism'. In Traditions of Ethics in International Affairs. In T. Nardin, *Traditions of Ethics in International Affairs.* Cambridge: Chapter 8.

Fairweather, N. B. (1999). Surveillance in Employemnt: The Case of Teleworking. *Journal of Business Ethics*.

Forester, T., & Morrison, P. (1990). Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing. *Harvard Journal of Law & Technology*, 299-305.

Freeman, E. R. (1984). *Strategic Management: A Stakeholder Approach.* Pitman Press.

Fried, C. (1968). Charles Fried "Privacy," The Yale Law Journal (Volume 77):475-93. p. 493/. *The Yale Law Journal 77*, 475-493.

Garson, B. (1988). *The Electronic Sweatshop.* New York: Simon & Schuster.

Ghoshray, S. (2013). Employer Surveillance versus Employer Privacy: The New Reality of Social Media and Workplace Privacy. *North Kentucky Law Review*.

Hume, D. (1953). Of the Original Contract. In C. W. Hendell, *David Hume's Political Essays* (pp. 43-63). Bobbs-Meryl.

IGI Global. (2021, December 12). *Dictionaries*. Retrieved from IGI Global: https://www.igi-global.com/dictionary/online-behaviour/20907

Inness, J. C. (1992). *Privacy, Intimacy and Isolation.* Oxford: Oxford University Press.

LaMarco, N. (2019, March 12). *Small Bussinesses:Managing employees: Employees*. Retrieved from smallbussinesses.chron.com: https://smallbusiness.chron.com/advantages-monitoring-employees-18428.html

Larry, A., & Moore, M. (2021). *Deontological Ethics.* Retrieved from Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/ethics-deontological/#WeaDeoThe

Loch, K. D., Conger, S., & Oz, E. (1998). Ownership, Privacy and Monitoring of Workplace: A Debate on Technology and Ethics. *Journal of Business Ethic*.

Merz Smith, E. (2004). Everything is monitored, everything is watched - Employee Resistance to Surviellance in Ontario Call Centres. *Department of Sociology - Queen's University Canada*.

Miller, S., & Weckert, J. (2000). Privacy, the Workplace and the Internet. *Journal of Bussiness Ethics*, 255-265.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy* , 559-596 .

Oxford Dictionaries. (2021, December 10). *Definitions*. Retrieved from oxfordlearnersdictionaries: https://www.oxfordlearnersdictionaries.com/definition/english/monitor_2

Palm, E. (2007). *The Ethics of Workspace Surveillance.* Stockholm: Royal Institute of Technology.

radware. (2021, December 11). *ddospedia*. Retrieved from radware.com: https://www.radware.com/security/ddos-knowledge-center/ddospedia/keylogging/

Regan, P. (1998). Genetic Testing and Workplace Surveillance: Implications for privacy. In D. Lyon, & E. Zureik, *Computers, Surveillance and Privacy.*

Rössler, B. (2004). *Privacies – Philosophical Evaluation.* California: Stanford University Press.

Rössler, B. (2005). *The Value of Privacy.* Oxford: Polity Press.

Scanlon, T. M. (1998). *What We Owe to Each Other.* Harvard: Harvard .

Schoemann, F. (1984). *Philosophical Dimensions of Privacy: An Anthology.* Cambridge: Cambridge University Press.

Severson, R. W. (1998). *The Principles of Information Ethics.* London: Routledge.

Sorsa, M., & van Damme, K. (2005). Ethical, Legal and Practical Aspects of Genetic Testing at Work. In S. O. Hansson, & E. Palm, *The Ethics of Workplace Privacy.* Brussels: P.I.E Lang Publisher.

Stealthmonitoring. (2021, December 11). Retrieved from stealthmonitoring.com: https://stealthmonitoring.com/security-blog/stealth-monitoring-at-a-glance

Tunick, M. (2000). Privacy in the Face of New Technologies of Surveillance. *Public Affairs Quarterly*, 259-277.