Adopting Vulnerability Principle as the Panacea for Security Policy Monitoring

Prosper K. Yeng[1], Stephen D. Wolthusen[2], Bian Yang[3]
Department of Information Security and Communication Technology, NTNU, Gjøvik, Norway[1,2,3]
School of Mathematics and Information Security, Royal Holloway, University of London, Egham, United Kingdom[2]

***Abstract*—Despite the adoption of information security policies, many industries continue to suffer from the harm of non-compliance. Some of these harms include illegal disclosure of customers sensitive data, leakages of business trade secrets, and various kinds of cyber-attacks. The impact of such harm can be enormous.To avert this, monitoring the compliance of information security policies (otherwise known as use policies) have been adopted as a strategy towards enhancing security policy compliance. One of the main essence of use policy monitoring is to enhance security policy compliance so as to prevent harm. Ironically, the consequences of use policy monitoring can be detrimental. While proponents use utilitarianism ethics to argue that the monitoring of use policy is enhancing security policy compliance, the opponents of use policy skewed to deontological ethics to argue against the monitoring of security policy. Deontological ethics is of the view that monitoring of security policy intrudes on employees' privacy and tend to hamper on their work performance. There have not been any clear solution to this discourse. A survey was conducted to understand the extend of security policy monitoring. Vulnerability principle was therefore explored as the panacea towards enhancing the monitoring of use policy to satisfy all the involve stakeholders.**

Keywords*—Information security; vulnerability principle; ethics; security policy monitoring

I. Introduction

There exists a "a tag of war" between employers and their workers over use information security policy monitoring [11]–[14], [26]. Employers are threatened based on the fact that the employees have been entrusted with user access credentials and other company resources. So if the use of these assets are not monitored, the employer cannot be certain of the loyalty of the employees to be using the entrusted resources for the assigned duties.

Use policy monitoring involves observing the behaviour of legitimate users with various tools and technology. The ultimate goal is to detect and mitigate employees behaviours that deviate from the established policies. Data from monitoring of the policy can also be used in a reactive manner. It can serve as evidence for penalizing disloyal employees. Use policy monitoring can also exonerate suspected but innocent employees in a dispute scenario which has to do with abuse of use policies.

There have been various instances where employees inadvertently or deliberately cause problems for the companies based on their empowerment with access credentials and resources. For instance, an employee in a drug manufacturing company sent an email to update its customers but unfortunately, all the customers' email addresses were entered in the "TO" field of the email system [11]. Apparently, each of the customers got to know of the other customers who were using the drug [11]. The company was subsequently found guilty of breach of privacy and was heavily fined [11].In addition, employees' conduct can result in the exfiltration of sensitive data, in unauthorised sharing or disclosure of the company's trade secretes. Employees' actions and inaction has been a gateway to multiply cyber-attacks which are mostly costly to the healthcare providers [2].

Based on these repercussions, many companies have adopted monitoring to track how employees comply with established information security policies, standards and guidelines [11], [13], [16]towards preventing harm from employees. Averagely, 80% of organizations are monitoring use policy compliance. And resent survey indicates that more than 90% of financial companies uses various methods in monitoring use policies [1]. Utilitarianism ethical theory is believed to be in support of use policy monitoring to prevent harm to many parties in a company [21].

On the contrarily, deontological ethics support the claim of employees against the monitoring of security practice. According to the opponents, monitoring of use policies can have psychological and physical harm to employees. Especially, overzealous monitoring of use security policies are invasive to employees' privacy. Excessive monitoring of use policies could involve video monitoring of toilets, bathrooms and dressing rooms. As this is very dehumanizing, deonthological ethics heavily frown on such monitoring and believe that employees have a reasonable level of expectation of privacy at work places [11].

Various solutions have been professed but none of them have the ability to completely mediate in this "tag of war". So a review was conducted to understand the problem area towards proposing a lasting solution.

This introduction is followed by a background section which provides understanding of the ethical theories that were used in this study. A section which clearly defines the research problem, objective and scope was also presented. The background section is followed by the method section which describes the approach of the study. This was followed by presenting the current use policy monitoring methods and devices were identified. Additionally, the benefit and advert effect of monitoring these policies were also explored. Finally, vulnerability principle was used to develop a framework with a discussion that is deemed fare to all the involved stakeholders.

II. Background

Ethics provides a set of standards for behavior that helps us decide how we ought to act in a range of situations [3], [4], [6]. In a sense, we can say that ethics is all about making choices, and about providing reasons why we should make these choices. Ethics is defined as an aspect of philosophy which deals with the nature, criteria, sources, logic and rationality of moral judgement [3], [4]. It establishes some standard ways of behaviour to enable one to decide how to act in different scenarios. Ethics is basically based on moral and cultural values to establish the moral behaviours or customs within various groups. Some ethical behaviours such as murder, theft, assault and arson are universal and unacceptable [3], [4].

Ethics is categorized into three main areas [3]. The are meta-ethics, normative ethics and applied ethics. Meta-ethics deals with the source of the ethical principle as to whether it is a social invention or will of God. Normative ethics propose standards and principles that regulates the right and wrong behavior. Applied ethics investigate specific areas and special controversial issues, for actual application of ethical principles and standards. Such special areas include abortion, capital punishment, voluntary euthanasia and animal rights.

In addition to proposing ethical principles for regulating good and bad behavior, normative ethics also deals with evaluating moral judgement of which both meta-ethics and applied ethics are less concern about. In this light, this study concentrates on surveying for roles in which corporate institution can play to enhance security practice. Primarily, normative ethics is categorized into consequentialist theories, deontological and virtue theories.

A. Deontological Ethics

Deontological ethics deals with the fulfilment of duties and obligations of people in any given setting. As a result, deontological ethics is also known as duty-based approach [5], [6] which is a kind of normative ethics where the principles and standards tend to guide and assess the choices of people with their given duty on what they need to do [6]. Each one is expectant to fulfill their respective duties irrespective of the outcomes [6]. So a good ethical behavior require an individual to perform their given duties in the rightfully prescribed manner, irrespective of the repercussion. A system of rules are provided in deontological ethics with consistent expectations for those in the same domain [5], [6]. For instance, if a behavior is judged to be morally right, that encompasses all people in related situation and these are basically the laws established in various jurisdictions.

B. Consequentialist Theories

Consequentialist theories (also known as utilitarianism) deal with the consequences of individual's behavior. Primarily, some actions would always result in good or bad outcome [5], [6]. So the best ethical decision would be the choice of action that provides the most good or causes the least harm. Consequential theory is counterrally to deontological ethics since deontological ethics does not care about the consequence of an action aside the obligation for one to perform his or her duty, irrespective of the outcome [5], [6]. An aspect of consequentialist approach concerns itself with the common good where our actions should be guided by contributing towards the common good of the people. So the best society for instance should be based on the general will of the people towards producing what is best for the people [5], [6].

The virtue approach deals with the adoption of outstanding human characteristics which can motivate an individual in a given context. A person with good character might have attained some virtues in society. It normally concentrates on moral characteristics instead of rules(deontological) or consequences in (consequential ethics) [5], [6].

C. Vulnerability Principle(VP)

According to Robert Gordin, all kinds of ethical principles can be drawn from vulnerability principles (VP) [32], [41]. In moral responses, others (vulnerable people) depends on the moral agents. Moral agents ((which is also called vulnerable agent) has a degree of autonomy and the capacity for independent and reasonable self-determination. Moral agents have the ability to determine what they want and how they want to go about their way of life. They can influence their choices by taking measures to grantee the materialization of their decision. The employer is the moral agent in the context of workplace. On the contrary, the dependence are not entirely in control of what happens in their affairs. Dependants have limited choices and lack a complete ability to control their affairs. Employees are the dependants, moral patients or vulnerability patient in workplace scenarios.

The dependants are really vulnerable to the actions and choices of the moral agents. The concept of vulnerability in ethics is a situation in which a dependant (otherwise called moral patient) is susceptible to injury or harm in some way [32], [41]. Human beings are emotionally and psychologically susceptible to loss and grief, to neglect, to abuse, to lack of care, to rejection, to isolation, and humiliation at various work places [31], [40]. The VP has therefore placed a responsibility on moral agents to act in a manner that will prevent putting vulnerable people or dependence at risks and to protect them against harm or injury [32], [41]. Stakeholders in a company including employees, board of directors, share holders and the society at large can be vulnerable in various ways including man-made threats, threats of nature, omissions or neglects of others and through the actions and in-actions of others [32], [41].

Vulnerability results in a state of helplessness and dependency [7], [32]. Helplessness is the inability to help one self while dependency is being subordinated, conditioned, subjected, reliance or living at another's cost. In both situation, the harm through vulnerability is as a result of the inactions than actions [8], [32]. To be harmed means for the patients to be made worse than the earlier state by direct acts of agents or by the inactions of the agents who may fail to protect the patient from the threats [32].

In the context of information security, the employer can be vulnerable [32], [41]. Employees are normally given authorized access to the company resources such as physical assets, network, data, software and hardware. In this case, a kind of autonomy has been entrusted into the employees [11], [12], [26], [32], [41]. So the employees can then decide what and how they can use their access right for, if there are no

established use policies. Even if there are, the employer is still vulnerable if the employer has no means of determining the compliance of the use policy [11], [12], [26], [32], [41]. On the other hand, if compliance monitoring of use policy is established, the employee can become vulnerable if the monitoring is excessive. In the implementation of use policy monitoring, ethics is concern with protecting the vulnerable in the company against others that have the power or are in position and have the upper hand. And that is the basis of this study. How can employees, customers and share holders among others who found themselves vulnerable, can be protected from harm in the context of security practice which involve monitoring of the security policies. This study explored VP to develop an ethical framework towards enhancing security practices while satisfying the ethical needs of all the vulnerable partners.

D. Problem Definition, Objective, Study Scope and Approach

The issue at hand is depicted in Fig. 1 where the vulnerability patient (moral patient) suffers harm from both deontological and utilitarianism decisions which stemmed from the moral or vulnerability agent. The background is that employers need to monitor their employees on adherence to information security policy [11], [12], [26]. From utilitarianism ethical point of view , security policy monitoring is acceptable, so long as it serves the common good principle [6], [11], [21], [26]. But this mostly clashes with deontological ethics [21], [26]. Deonthological ethics stand against information security monitoring when the monitoring tend to cause harm to employees [21], [26]. So in such a contention, which ethical method can mediate to bring lasting solution to this discourse? The founding principles of utilitarianism ethics has been criticised [6], [11], [21], [26]. As it promotes common good, utilitarinism ethics can trample over the fact just to achieve its common good principle [5], [6]. This is ethically wrong [5], [6].For instance, if video cameras are mounted such that the monitoring invades workers privacy, so long as the monitoring prevents thefts, protects the customers, the business and the society at large, utilitarianism ethics does not care of the privacy issues of the fewer employees in the company [5], [6], [11], [21], [26].

Deontological ethics mostly restricts the extend of monitoring to prevent employees' privacy invasion and causing other harm to employees but some of these provisions does not satisfy the employers [6].

Vulnerability principle consists of moral agents who have the moral responsibility to protect vulnerability patients [32]. Vulnerability patients can be identified among all stakeholders (such as workers, employees and customers) in the company [8], [32].

In order to mediate and profess a lasting solution on use policy monitoring issue, one needs to understand the problem domain in all of its facets.For instance, what are the methods or tools used for monitoring? What are being monitored specifically ? How is the monitoring conducted? How does these kind of monitoring benefit the employers, employees and other stakeholders and society at large? What are the negative consequences of the use policy monitoring? Whom does these monitoring negatively affect and what solutions have already been proposed?

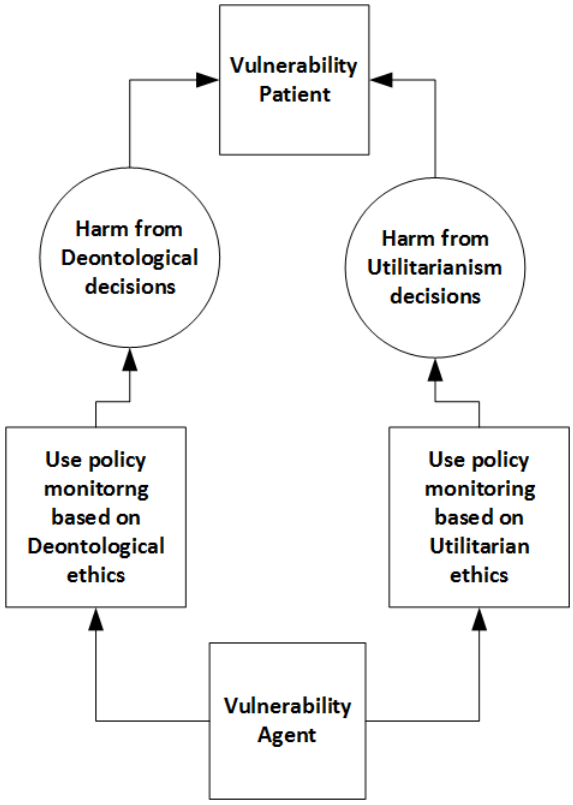

Fig. 1. Impact of use Policy Monitoring Decision in the Context of VP.

This survey therefore explored to answer these questions and propose and effective solution. VP was hence adopting in defining an effective approach to solving the discourse in use policy monitoring.

III. Method

A literature search was conducted in Google scholar, IEEE Explore, ACM Digital Library and Elsevier, for ethical dilemmas in monitoring information security policies of employees. Key words including employee, information security policy, monitoring and ethics were combined with Boolean functions of AND, OR and NOT, to enhance the effectiveness of the search strategy. The dilemmas in use policy monitoring, with respect to utilitarianism and deontological ethics were analysed. A solution for use policy monitoring was therefore proposed.

IV. Findings from Literature Survey

They findings in the survey were organised in this section to answer the outlined questions(section 2.4) as follows.

A. What are the Methods or Tools used in the Monitoring?

In recent time, various methods, techniques and devices are used in monitoring the compliance of use policies. Employers can conduct monitoring of the use polices within or outside their organizations, with different kinds of hardware and software tools. Some of these tools include video surveillance systems such as Closed-circuit Television(CCTV) and IP

cameras [13], [14], [26]. Both of them transmit video to their defined destinations but while CCTV converts the video signals into television usable format, the IP cameras converts its video signals into packets that can be transmitted via data network. Employees are also being tracked through their work badges [13], [14], [26]. In the badge tracking,time spent and entries into various locations by the employees are monitored [13], [14], [26]. Additionally,logs of physical accesses with access cards are stored and can be analysed to determine the security practice of the use policy [13], [14]. Internet monitoring, email monitoring, keystrokes, voice recording and biometric devices are some of the devices and techniques used in monitoring within the workplaces. In exploring for observational measures towards profiling healthcare staffs' security practice, Yeng et al also identified that the logs of electronic health records are mostly analysed to monitor health care professionals' behaviour within the hospitals [2].

With the perceived advert impact of employees security violations, use policy monitoring is extended beyond the employers offices. Outside the office space, global positioning systems(GPS)chips and Radio Frequency Identification (RFID) chips are being used to track assets locations such as laptops, phones and vehicles used by employees [13], [14], [26].

B. What are being Monitored and How is the Monitoring Conducted?

The use policy monitoring methods and tools are mostly used to observe a broad scope of the employee security practices. Communication related activities such as keystroke dynamics, inbound and outbound email communications [11], text-messages, use of internet and such engines, use of social media sites and telephone use [11] are some of the employees' activities that are being tracked [13], [14].

Other employers go to the extend of secretly viewing, recording and reporting basically all the computer activities of employees [15], [16]. Some of the monitoring activities were noted to include hiring and using outside investigators. Some overzealous monitoring were identified to include video taps of employee dressing rooms [21], [22] and watching of attendance to bathroom at work [21], [22]. Other companies adopted these advance monitoring systems without the knowledge of the employees [15], [17].

C. What are the Purposes of these Monitoring?

It is often said that, "there is no smoke without fire", meaning that there are obvious reasons which trigger the monitoring of these used policies. Some of the main essence for monitoring use policy includes security and employee productivity [15], [18], [19]. Many industries claim to suffer from the harm of non-compliance of security policies by employees [11]. By virtue of their legitimate accesses to company resources, employees are required to apply their given resources in accordance with their provisioned security policies [11]. So if there is lack of monitoring, employees could cause the company to lose trade secretes or business processes to competitors [15], [18], [19]. Companies could even face legal consequences for negligence to monitor use policies of employees' practices which results in causing harm to others [15]. Aside these, the employers deem it unethical for workers to be downloading objectionable materials such as pornography, visiting unauthorised websites and downloading unauthorised software onto the company computing resources. Such misbehaviours waste company network and computing resources [9]. The monitoring of non-compliance such as emails coming from outside the organization can help protect the company against various threats such as viruses and social engineering attacks. Monitoring outbound emails can also help to prevent data exfiltration. Unauthorised sharing of sensitive data could be very costly to both the company and the data subjects involve [10].In terms of security enhancement, CCTV for instance helps to prevent unauthorised and inappropriate practices such as theft, fraud and other misuse of security policies [26]–[28]

Monitoring of use policy does not only help the employer, but have direct benefits to the worker as well [15], [20]. For example, an employee who is suspected of sharing trade secret can be exonerated through the review or audit of his emails if indeed the employee was wrongfully accused [15], [20]. Other Utilitarian considerations include monitoring which goes a long way to protect society as a whole in terms of job creation [21]. Aside security enhancement, the proponents of use policy monitoring trust that the monitoring is able to increase productivity, improve quality and service while decreasing cost [21], [24], [25]. Additionally, use policy monitoring has been considered to be effective in discouraging undesirable behaviours and enhances productivity [26], [29], [30]. From the perspective of utilitarianism theory, use policy monitoring is essential as it supports the protection of consumers, workers and the company at large [22], [23].

D. What are the Negative Effects of the use Policy Monitoring?

Various "fingers" have been pointed at the advert impact of monitoring use policies. From deontological point, employee monitoring is a fundamental breach of the workers rights and it causes privacy invasion, stresses, decrease in work satisfaction and is very dehumanizing [11], [12]. Employees might sign to abide by such monitoring decisions, but they will still have their resentments of the implications. Employees may feel that the monitoring of the use policy encroaches their privacy's. A related study also supported the argument and pinpointed that [26] monitoring of use policy invades privacy, of employees which results in mental and physical health. The proponents of use policy monitoring believed that monitoring affects creativity, autonomy, morale, productivity, work-life balance, organizational trust, job satisfaction and increased in job stress [12], [15], [26].In terms of privacy rights of employees, Deontological ethics emphasise that employee monitoring should never be allowed at work places [15].

E. What are Some of the Suggested Solutions?

Ford et al examined how monitoring of employees' security practice could be done without invading on their privacy. The study therefore proposed for frequent updates of the use policies by involving the employees while updating use monitoring decisions with emerging laws [13].

Yearby (2013) considered various scanrios of use policy monitoring and suggested that , policy writing, policy updates and compliance should be a cross-functional team work. The

team should include, representatives from human resources, legal counsel of both employer and employees and the IT group, who can best advise on how the monitoring can be better conducted and the activities that will be monitored. The IT group can also advise on who will be monitored, and the data will be included in monitoring. Existing policies should be reviewed yearly to determine if the policy is in line with current procedures [15], [16].Janet et al also supported the idea and stated that policies, "once developed, need to be periodically reviewed to ensure compliance with evolving legal changes" [12]

A suggestion was offered for the adoption of communication in the design and implementation of monitoring systems to solve the issues originating from both deontological and utilitarianism [21]. This should be done by allowing the employees involve to give input in the monitoring design with regards to their preferences, The companies need to also communicate the monitoring activities to the employees and provide face-to-face feedback to employees. The feedback response should be considered in subsequent monitoring and the employees who provided the feedback should not be directly or indirectly punished based on their feedback [21].

Ethical orientation of both the employees and employers was proposed as a mediation to solving the divide [26]. It is believed that if both parties are "on the same page" regarding ethical understanding, there is therefore a high likelihood for them to reach fair decision which satisfies both the employer and employee [26].

F. Gap Analysis

With respect to the proposed solution by Ford et al., updating security policy monitoring procedures to catch up with current laws and concerns of employees is a step in the right direction. However, it in not only employees who are vulnerable in use policy monitoring. The consequences of use policy monitoring affects broad scope of actors including the society at large [11], [12], [26].

Similarly, communication and ethical orientation were respectively suggested by [12] and [26]. The suggestion can actually provide the parties involve in this argument, with ethical knowledge and an option for dialogue. But a better approach should be adopted to identify the stakeholders and subsequently identify the vulnerability agents and patients.

A complete identification of the stakeholders will lead to a fruitful discussion among stakeholders towards arriving at a better approach to monitoring the use policies. Yerby (2013) supported this identification of the stakeholders but the study did not specify the method that can be used to properly identify the vulnerability patients who are affected in the monitoring of the use policy [15]. The existing gaps has been depicted as shown in Fig 1. Moral Agents often opt for utilitarianism ethics, deontological ethics or both in developing use policies [11], [12], [26]. Any of the approaches can result in their respective harms (Harm from deontoligical decision or harm from utilitarianism decision). In such decisions, the vulnerability patient is the receiver of related harmsitem22,itemf,item32.

Therefore, using the vulnerability principle to identify the vulnerability patients in the decision making process and subsequently dialogue to finding a lasting solutions is what this study explored.

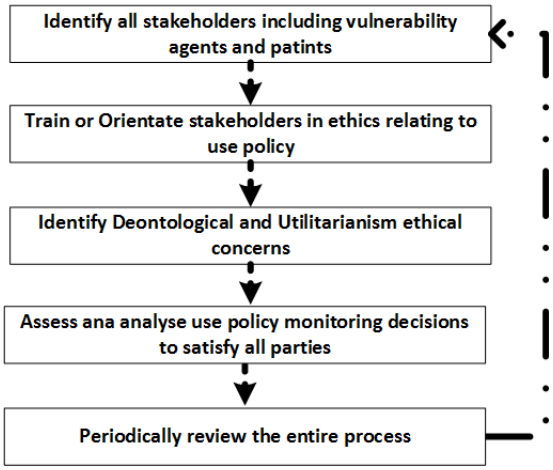

Fig. 2. Use Policy Monitoring Solution based on Vulnerability Principle.

V. Use Policy Monitoring Solution based on Vulnerability Principle

As shown in Figure 2, the vulnerability principle can be adopted in the following steps:

1) Identify what policies need to be monitored. This also involve, the identification of the monitoring methods and devices.
2) Identify all stakeholders who can be affected by the use policy monitoring. This includes technical teams, such as legal advisor of all vulnerable groups, and IT teams who will install the devices or perform the monitoring.
3) Train or orientate stakeholders with ethical principles [26]
4) Identify deontological and utilitarianism concerns [26]. This will help catalogue all issues in the use policy monitoring for consideration.
5) Identify vulnerable agents and vulnerable patients and how they are affected by the monitoring
6) Assess monitoring decisions and strategies and agree on reasonable monitoring methods which are acceptable to all stakeholders. This should include agreement on what data is to be collected or stored, what is to be video or audio recorded etc.
7) Periodically review the entire process for appropriate update of the monitoring processes [12].

VI. Discussion

Information security monitoring is vital in various organizations. But its implementation can tend to ironically suffocate the very business that it was mend to safeguard and cause various harms. This discourse of use policy monitoring is between utilitarianism ethics and deontological ethics. Utilitarianism is a proponent of use policy monitoring while deontological ethics tend to support employees in the argument against use monitoring policy due to its negative impact as outlined in section IV, subsection D. To find lasting solution to this

argument, a survey was conducted to understand the use policy monitoring domain. The results also provided guidelines to propose what is deemed as lasting solution. The tools, devices and methods were identified in the review as shown in Table 1. How and what are often monitored were also identified as summarised in Table I.

Biometric devices in this context are used for monitoring of employees' characteristics which relating to their conscious and unconscious changes of the employees' traits [33], [34]. Some of these characteristics include temperament, motivation, posture balance, brain activity, emotions and behaviour [33], [34].

The advert impact of these monitoring were identified to include privacy invasion, increment in stresses, reduction in work satisfaction and causing mental and physical health problems. Monitoring also affects employee creativity, autonomy and trust which have advert effect on their productivity.

From the view point of employees, aside privacy concerns, monitoring keystroke for instance can provide misleading reports of a user behaviour to management which may lead to needless employee sanctions. A keystroke monitoring system may not detect when an employee actually has a running stomach or a brief stretch from his seat. A court ruling in the European Court of human right in UK, supported this with the ruling that workers have reasonable expectation of privacy in making and receiving calls at work [11]. In a related ruling in the US, the judge noted that an employee does not surrender all privacy rights and therefore should not completely surrender that on a company's computer automatically [11].

In this dawn of digitization, most companies often leverage on the power of information technology to archive their business objectives. So employees are often entrusted with related resources such as access credentials, physical and electronic office places among others. Computing and other resources including laptops, phones, tablets, emails, internet, vehicles and many others, are often provided to the employees alongside with their usage rules and regulations [11], [12], [37]. The policies governing the usage of these resources is often important. So the use of these resources are monitored to prevent or detect misappropriation, misuse or abuse [11], [12], [37]. Inappropriate use of a company resources can have serious consequences on the company, on a third party or both [11], [12]. A company can collapse if its resources are wasted [11], [12], [37]. From utilitarianism point of view, this will not only affect the company and its investors, but the employees jobs will be lost and clients or the service receivers will be harmed [11], [12], [37]. Society will also be adversely impacted since the companies will not be in operation to pay taxes [11], [12], [37]. Trade secrets and business processes can be stolen. This can shift the business out of competition [37], [38].

Companies that deal with personal data also have the responsibility to efficiently protect this information [12], [14]. So companies can face serious legal challenges if their customers data is compromised or not used for the intended purpose. Based on some of these pertinent reasons, it is very sound to monitor use security policies for compliance to prevent utilitarianism ethical related harms. But some of these monitoring can be overzealous as employees believe that their reasonable expectation of privacy at their work places tend to be encroached.

Privacy concerns in organisations include but not limited to Intrusion and public disclosure of private facts [26], [35]. Intrusion occurs when there is a deliberate encroachment into one's private affairs [26]. This can be done physically or the usage of devices such as phone calls,taking one's pictures in his or her private place, opening one's personal mails, watching others with video a camera, recording voice messages and phone calls among others [35], [39]–[42]. Public disclosure of private facts involve unreasonable disclosure of the affairs of one's private life [26]. Employees feel that monitoring of all their activities is not right [26]. Even when employees consent to monitoring for security, performance, they are still much worried of their privacy [26], [35], [36].

Employees tend to be dehumanized if monitoring is excessive [35], [36]. Employees' privacy can be heavily compromised in monitoring use policies and this negatively affects their psychological and physical health [11], [12], [26]. Excessive monitoring prevent employees from working successfully, because employees tend to lose autonomy and the discretion to take useful decisions [11], [12], [26], [36], [37].

Critically, deontological ethics is not entirely against the monitoring of use policy. But the cause of contention is where use policy monitoring tend to cause harm to the vulnerable [11], [12], [26], [36], [37]. Ultimately, the advert impact of excessive monitoring of use policy does not affect only the employees. Ironically, it affect the employers too. For instance, psychological and and physical sickness of employees could translate into poor customer services or production in the business [11], [12], [26], [36], [37].

More to the point, one of the objectives of enhancing security is to safeguard the business. Deontological ethics also expects employees to be productive in their assigned duties. But the burden of overzealous monitoring can frustrate this. To find an everlasting solution contention, a reasonable monitoring of use policy need to be determined with the appropriate methods. Vulnerability principle which is the father of all ethical principles could be used in finding lasting solution to this discourse as outlined in Fig.2. In this regards, all those who are affected in the security policy monitoring are identified as the stakeholders [15]. In a typical company setting,the stakeholders can include the employer, employees, IT team, customers,lawyers representing the various group of stakeholders and labour officers [15]. Training or ethical orientation is then provided to bring the stakeholders upto the same level of ethical understanding within the scope of security policy monitoring. Ethical issues concerning utilitarianism and deontological ethics can then be identified. Based on the VP, the moral agents and vulnerable patients are identified under various scenarios. Using dialogue and effective communications [12], [26] backed with their ethical orientation [26], the use policy monitoring decisions are assessed and analysed to satisfy all parties. Periodically, the entire monitoring process should be reviewed to reflect changed laws.

VII. Conclusion

Following the long standing debate on information security policy monitoring, a survey was conducted to understand

TABLE I. DEVICES AND METHODS OFTEN USE IN MONITORING INFORMATION SECURITY POLICIES

No.	Device/Method	Purpose
1	Video Cameras	Monitoring employees at the offices, dressing room, toilets or baths
2	Badge Tracking	Trackin og employees and their time spent at various locations in the office
3	GPS	Tracking and monitoring location of office vehicles
4	RFID	Monitoring and tracking location of office equipment such as phone, laptops,tablets, within and outside office
5	Log monitoring and log analysis	Profiling employees' behaviour through logging physical access and accesses through specialist application software. And also secretly viewing, recording and reporting all the computer activities of employees [15], [16]
6	Biometric monitoring	Monitoring the characteristics of staff such as mood changes, facial expressions, looks, etc
7	Keystroke	Tracking performance and detecting behavioural changes
8	Voice Recording	Monitoring voice communication to prevent unauthorised disclosure
9	Email, social media and SMS monitoring	Monitoring messages to prevent unauthorised disclosure
10	hiring and using outside investigators	To assess the nature of the employee in potential policy breaches

the problem domain. Employers are poised in monitoring employees regarding to how they apply security resources in their duties.However employees feel that the monitoring sometimes inflicts them with varying degree of harms such as privacy invasion, pyschological and mental stress and even tend to negatively affect their work performance. Deontological ethics took side with employees as there are some privacy laws against overzealous monitoring. The basic solution is to find a balance point of which security policy monitoring can be conducted in such a way that harm is not caused onto the stakeholders involve. Vulnerability principle was therefore explored to help in the mediation of this controversy in use policy monitoring. The process involve identifying all stakeholders, training or orientating the stakeholders with ethics relating to use policy, identifying deontological and utilitarianism ethical issues in use policy monitoring.This is followed with identifying moral agents and their patients, assessing and analysing use policy monitoring decisions to satisfy all parties. The process is reviewed periodically to catch-up with updated laws and concerns.

In following this process, all the parties in the use policies will be involved in the design of the monitoring process. Their challenges relating to use policy monitoring can then be identified and resolved. Use policy monitoring can then be reasonably conducted to meet the desire effectiveness of the employer without causing harm to employees. Empirical studies need to be conducted in future to assess and evaluate this proposed solution for practical use.

REFERENCES

[1] Indiparambil JJ. An empirical study on the detrimental effects of employee surveillance in India. International Journal of Research in Computer Application & Management. 2017;7(12):48-51.

[2] Yeng P, Yang B, Snekkenes E. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. In2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) 2019 Jul 15 (Vol. 2, pp. 397-404). IEEE.

[3] Whitman M. E., Mattord H. J. Principles of information security. 6th Edition ed: CENGAGE Learning; 2017. 728 p.

[4] Ruighaver A. B., Maynard S. B., Warren M. Ethical decision making: Improving the quality of acceptable use policies. Computers & Security. 2010;29(7):731-6.

[5] Nweke L., Wolthusen S. Ethical Implications of Security Vulnerability Research for Critical Infrastructure Protection. 2020. p. 331-40.

[6] Bonde S., Firenze P. Making choices: A framework for making ethical decisions. Retrieved from Web Accessibility Initiative website: http://www. brown. edu.; 2013.

[7] Trompeter C. M., Eloff J. H. A framework for the implementation of socio-ethical controls in information security. Computers & Security. 2001;20(5):384-91.

[8] Scully JL. Hidden labor: Disabled/nondisabled encounters, agency, and autonomy. IJFAB: International Journal of Feminist Approaches to Bioethics. 2010 Sep;3(2):25-42.

[9] Wang, S.C., Yan, K.Q., Liao, W.P. and Wang, S.S., 2010, July. Towards a load balancing in a three-level cloud computing network. In 2010 3rd international conference on computer science and information technology (Vol. 1, pp. 108-113). IEEE.

[10] Yeng, P.K., Yang, B. and Snekkenes, E.A., 2019, December. Framework for Healthcare Security Practice Analysis, Modeling and Incentivization. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3242-3251). IEEE.

[11] Patrick Dubicki,Submitted 11/27/2003Acceptable Use Policies and Workplace Privacy:Legal and Ethical Considerations,SANS Institute , 2003,1-14,2004, SANS, Access https://www.giac.org/paper/gsec/4079/acceptable-policies-workplace-privacy-legal-ethical-considerations/106512

[12] Ford J, Willey L, White BJ, Domagalski T. New concerns in electronic employee monitoring: have you checked your policies lately?. Journal of Legal, Ethical and Regulatory Issues. 2015;18(1):51.

[13] Walls, A. (2012a). Conduct digital surveillance ethically and legally: 2012 update. Gartner, Inc. Retrieved June 29,2012 from http://www.gartner.com/id=1965315

[14] Ciocchetti, Corey A. "The eavesdropping employer: a twenty-first century framework for employee monitoring." American Business Law Journal 48.2 (2011): 285-369.

[15] Yerby J. Legal and ethical issues of employee monitoring. Online Journal of Applied Knowledge Management (OJAKM). 2013;1(2):44-55.

[16] Peter.J., & Britton, S.M. (2001). Employer Monitoring Of Employee Internet Use And EMail: MEALEY'S Cyber Tech Litigation Report, 2, Retrieved June 1, 2020, from http://foleybezek.com/wp-content/uploads/art.InternetFile.pdf

[17] Business Wire, Inc.,2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse,American Management Association (AMA) and The ePolicy Institute, Retrieved June 1st 2020, From: https://www.businesswire.com/news/home/20080228005093/en/2007-Electronic-Monitoring-Surveillance-Survey-Employers-Combined

[18] Woodbury, Marsha Cook. Computer and information ethics. Stipes Pub., 2003.

[19] Oprea, Mihaela. "An Agent-Based Knowledge Management System for University Research Activity Monitoring." Informatica Economica 16, no. 3 (2012).

[20] Frayer, Charles E. "Employee Privacy and Internet Monitoring: Balancing Worker's Rights and Dignity with Legitimate Management Interests." Bus. Law. 57 (2001): 857.

[21] Alder, G. Stoney. "Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives." Journal of Business Ethics 17, no. 7 (1998): 729-743.

[22] Galvin, K. "Boston Hotel Worker Tells Senate of Video Invasion of Privacy'." States News Service 22 (1993).

[23] Barry, R. J. "Statement on behalf of Security Companies Organized for Legislative Action (SCOLA) before the senate labor and human resources subcommittee on employment and productivity." United States Senate 22 (1993).

[24] Alder, G. Stoney. "Employee reactions to electronic performance monitoring: A consequence of organizational culture." The Journal of High Technology Management Research 12, no. 2 (2001): 323-342.

[25] Bylinsky, Gene. "How companies spy on employees." Fortune 124, no. 11 (1991): 131.

[26] Palayoor, Alex Joy, and D. Mavoothu. "Ethical Orientation: A Solution for Workplace Monitoring and Privacy Issues."

[27] Watkins Allen, Myria, Stephanie J. Coopman, Joy L. Hart, and Kasey L. Walker. "Workplace surveillance and managing privacy boundaries." Management Communication Quarterly 21, no. 2 (2007): 172-200.

[28] Ball, Kirstie. "Workplace surveillance: An overview." Labor History 51, no. 1 (2010): 87-106.

[29] Sewell, Graham, and James R. Barker. "Coercion versus care: Using irony to make sense of organizational surveillance." Academy of Management Review 31, no. 4 (2006): 934-961.

[30] Miller S, Weckert J. Privacy, the Workplace and the Internet. Journal of Business Ethics. 2000 Dec 1;28(3):255-65.

[31] Mackenzie C, Rogers W, Dodds S. Introduction: What is vulnerability and why does it matter for moral theory?. Vulnerability: New essays in ethics and feminist philosophy. 2014:1-29.

[32] Morton Winston, The Vulnerability Principle Accessed on June 01, 2020 From: http://ethicsofglobalresponsibility.blogspot.com/2008/03/vulnerability-principle.html

[33] By Joydeep Misra,What is Biometric Monitoring? Accessed on June 03 2020 from:https://bridgera.com/biometric-monitoring-iot-digital-health/

[34] Brumback CB, Myers NA, Yuen SG, Park J, Diemer TS, inventors; Fitbit Inc, assignee. Biometric monitoring device with heart rate measurement activated by a single user-gesture. United States patent US 9,049,998. 2015 Jun 9.

[35] Lee S, Kleiner BH. Electronic surveillance in the workplace. Management Research News. 2003 Mar 1.

[36] Indiparambil, J. J. (2019). Review of Pros-Cons Cons Polemics of Workplace Surveillance : Survey Comparison and Analysis. International Journal of Current Advanced Research, 8(02), 17277–17283.

[37] Willey L, Ford JC, White BJ, Clapper DL. Trade Secret Law and Information Systems: Can Your Students Keep a Secret?. Journal of Information Systems Education. 2011 Jun 1;22(3):271.

[38] Keith, N. (2016). Cultivating practitioners of democratic civic engagement. Michigan Journal of Community Service Learning, 23(1), 15-36.

[39] Lisa Guerin, J.D,Workplace Cameras and Surveillance: Rules for Employers Accessed on June 10th 2020 From: https://www.nolo.com/legal-encyclopedia/workplace-cameras-surveillance-employer-rules-35730.html

[40] Bryant, J. (2005). Computer privacy ANNOYANCES: How to avoid the most annoying invasions of your personal and online privacy. The British Journal of Healthcare Computing & Information Management, 22(10), 25.

[41] Straehle C. Introduction: Vulnerability, Autonomy and Applied Ethics. InVulnerability, Autonomy, and Applied Ethics 2016 Oct 4 (pp. 7-16). Routledge.

[42] Donald C Dowling Jr, Proskauer Rose LLP,"Video surveillance in workplaces worldwide" Accessed on June 10th 2020, From: https://uk.practicallaw.thomsonreuters.com/9-203-3829?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1