Privacy and Distributed Tactical Operations Evaluation

Dennis Andersson
Information Systems
Swedish Defence Research Agency
Linköping, Sweden
dennis.andersson@foi.se

Abstract— **In this study, thoughts on ethics of workplace monitoring are being applied to the very special domain of evaluations of tactical operations, such as military or crisis management exercises or operations. I try to find out if there are differences in the way we should regard workplace monitoring when it comes to this domain compared to standard workplaces such as offices, since the purpose of the surveillance is not to enforce discipline, but to evaluate the organizations' ability to conduct a tactical operation. The study focuses on issues such as privacy and informed consent and the main purpose of the investigation is to structure a consistent ethical standpoint when it comes to operations' evaluation by making parallels to related theories that I found correct and applicable. I conclude that is indeed reasonable to place other demands on crisis management workers than we would do on other work forces, and that it should therefore be easier to motivate workplace monitoring for the purpose of evaluating distributed tactical operations. I argue however, just as Miller does regarding police work, that upholding privacy can be a real problem when crisis management personnel are exposed to monitoring, even though it is intended for evaluation.**

Keywords - privacy, workplace surveillance, after-action review, crisis management

I. INTRODUCTION

The strive to develop and increase efficiency is, and has always been, an important force in society. Any organizational development assumes some sort of evaluation of the current state, to validate or verify the organizations' processes. Operational organizations such as the Armed forces, the Police and the Rescue services are not exceptions to this rule. Hence, evaluating their operations can be fruitful to yield understanding of how the organizations function, and thus a lot of effort is currently being put into developing methods and technology for such evaluations. In this sense, technology development is a door opener enabling a new spectrum of analyses; using video cameras, audio recorders, radar, position trackers and other sensor systems. From an ethical point of view, we need to investigate how those being evaluated react to the inherent analysis of their actions, which from an ethical point of view can be compared to the commonly discussed topic of workplace surveillance.

Workplace surveillance has been around since the early days of industrialization and is a powerful tool for the employer to ensure that the employees are performing the work they are hired to do. As technology progresses it becomes easier for the employer to increase the level of surveillance on the employees at the cost of an increased risk that they will experience the surveillance as a violation of their privacy. Kizza and Ssanyu [1] states that employees can get a reduced self esteem and become less creative by intrusive surveillance. In their article they present a number of arguments for and against workplace surveillance. I will return to the most relevant of their arguments later in this paper.

II. OBJECTIVE AND READING DIRECTIONS

In this paper I leverage on the work done on workplace surveillance by Kizza and Ssanyu [1] among others to direct the same questions to the question of monitoring crisis management personnel, where the purpose of the surveillance is not to enforce discipline, but to evaluate the organizations' ability to execute a tactical operation. The main purpose of this study is to structure ethical guidelines to consider for operations' evaluation by making parallels to related theories that I found correct and applicable.

The questions dealt with here would benefit from a larger empirical study of crisis management work, but that lies beyond the scope of this paper. Instead the study is focused on existing literature on nearby topics to yield some insight into the questions that need to be asked when conducting such an empirical study. To bring the findings in [1] closer to the crisis management domain, I take help from Miller [2] and his reasoning around the problems related to surveillance of police officers in their daily work. He argues that there really is a difference in what kind of surveillance you can expect a policeman to accept compared to for instance an office worker. The main contribution of this paper is the study of what privacy issues may arise when monitoring personnel in distributed tactical operations. The case studied here differs from the typical case of workplace surveillance, since the surveillance serves the purpose of validating and verifying processes and are therefore typically only in place for a limited time period, which was not the case in for instance Miller's much quoted study.

I argue, just as Miller does regarding police work [2], that upholding privacy can be a real problem when crisis management personnel are exposed to monitoring for the purpose of operation evaluation. In the following chapters I present my arguments before I finally structure my stand on evaluation of tactical operations. I start by defining some key

 ISBN: 978-1-61208-167-0

notions and describing the context around which my reasoning revolves.

III. Evaluating Distributed Tactical Operations Using After-Action Review

Evaluation of distributed tactical operations is here used to denominate the systematic practice of evaluating a tactical operation or exercise spanning across multiple locations [3, 4]. Originally, the approach was designed to evaluate military exercises; however it has also been successfully applied in many civilian domains, such as first responders in crisis management operations. In large and complex operations with many organizations, the after-action review (AAR) [5, 6, 7] can be more or less independently executed for each unit in the training audience. While these small group session AARs remain important, large-scale shared AARs receive more and more attention. In these overarching AARs, the evaluation focuses more on strategic command and control (C2) than the regular AARs that typically deal with issues on the operative level. Exactly where to put the efforts will depend on what kind of issues you want to highlight for the training audience.

The concept of AARs was coined by the U.S. Army who, like many other organizations, conducted review sessions after each exercise and operation. It was formalized and labeled AAR in [5]. First responders and crisis management organizations often use the same methodology, sometimes labeling it hot wash or debriefing. There is nothing in the theory itself that defines how to capture data for preparing an AAR, but more often than not, the main source for data capture and input to the AAR process are human observers/trainers (OT). An OT can offer a subjective view of what happened during the operation, and can use his/her expertise to pinpoint interesting events for AAR discussion. However, technology is quickly gaining ground in this area as a complement to the human observers. Audio and video recordings combined with system logs and other sensory data can provide an undisputable ground truth that the AAR facilitator can use to provide a baseline for the audience to review and discuss. As technology advances, the quality and the quantity of this data increases as well, enabling more and more accurate and detailed reconstruction of the events.

IV. Reconstruction and Exploration as an Approach for Conducting AAR

Reconstruction and Exploration (R&E) [3, 4] is a formalized approach to, among other things, support an AAR after a complex chain of events, such as a military operation or a crisis management operation. The approach assumes both human observers and technical registration to collect information on the chain of events, very much like the practice that AAR facilitators are moving towards. The aim of the data collection is to gather enough data to enable reconstruction of the operations as a time-synchronized visual multimedia model. The model can be used to find system- and organizational problems and identify needs for improvement. However, it is important to note that not only negative feedback is captured and reported, it is commonly recognized that positive feedback is equally important to provide during the AAR session.

Some of the most common data sources used for R&E are observer reports (notes), video surveillance systems, handheld cameras, microphones, wiretapping, screen capture systems and GPS devices. Exactly what data sources are used will depend on what questions need to be answered or what hypotheses are tested during the exercise/operation. In some scenarios there are no predefined questions or hypotheses, in which case the AAR team will typically try to collect a data set that is as comprehensive as possible to be able to answer any questions that may arise during or after the operation. This all makes R&E-assisted AAR a very powerful and flexible way of evaluating exercises and operations, especially distributed ones where an OT can have a hard time getting a birds-eye view of the scenario until being presented the data in the exploration phase.

Kizza and Ssanyu [1] describes workplace monitoring as a dominance or power between workers and employers, where the purpose is to:

- Increase productivity,
- protect against theft,
- protect against espionage,
- performance review of employees,
- prevent harassment,
- find missing data,
- find illegal software or
- prevent personal use of company resources.

Data capture for the sake of R&E partly adheres to the fourth bullet, although the purpose of an AAR is usually to assess the performance of a process or an organization as opposed to an individual as was the case in [1]. This difference may be crucial to the training audience's acceptance of monitoring, but it becomes apparent that R&E could in theory be used for all of these 8 purposes too, which would incur reduced trust, both for the system and the OTs.

V. Crisis Management Work

A crisis is sometimes defined as something that threatens basic functionality and values of society or individuals. That is a too broad of a definition for this work, as it spans from natural disasters to personal tragedy. Instead I will only use the word crisis as the type of extraordinary event, disaster if you will, that affect society as a whole. More specifically I will focus on events that require interagency cooperation. Some of the most recent examples from the Swedish society include the 'Gudrun' storm in 2005 [8], the Indian Ocean tsunami in 2004 [9], the discotheque fire in Gothenburg 1998 [10] and the M/S Estonia disaster in 1994 [11]. The evaluation of this kind of events are often handled as special investigations by appointed authorities, in Sweden typically by the Accident Investigation Board, who tries to analyze what happened and clarify whether there were any mistakes or procedural errors that need to be fixed. Considering that you can never fully prepare for an extraordinary event, it is in reality impossible to guarantee that you will be able to recover all the data you need for this kind of analysis. When it comes to exercises on the other hand, the course of events

 ISBN: 978-1-61208-167-0

can be controlled, and collecting the right amount of data at the right time is a matter of thorough preparation. For this reason, R&E is best suited for exercises and well-planned operations as opposed to the chaotic environment that first responders typically are exposed to in a major disaster, and where R&E may be harder to apply.

Typical for this type of extraordinary events is that they put routines to the test and may even become impossible to apply. Ad hoc workflows may have to be created as well as spontaneous command and control structures that will help in dealing with the situation. To assess performance in this scenario is difficult as you cannot always foresee what the processes will actually be. R&E gives some support in this process as it offers a rich data set and is flexible in the way data is being used and analyzed.

VI. PRIVACY

There is vast number of known and used definitions of privacy, one of which was formulated by Warren and Brandeis in 1890: 'the right to be let alone' [12]. This definition is still in use, but not very suitable for privacy in the professional life, instead I will rely on the definition that Aiello and Klob used in their publications on workplace surveillance [13]: "Privacy is the ability for an individual to control the use of their own personal data, wherever it might be recorded".

By the definition above, every human has the right to control any information about them and to avoid being seen. The immediate consequence of that is that all non-controlled surveillance and monitoring must be regarded as an infringement on privacy which of course is a problem. The keyword in this definition is 'control' which calls for further investigation and interpretation.

VII. PRIVACY INFRINGEMENT ISSUES

In the following section I will show that infringement is a real problem in monitoring crisis management personnel for the purpose of performance assessment, and then discuss arguments for and against acceptance this infringement, and lastly present and justify my personal opinion on the matter.

A. Is there a problem at all?

Kizza and Ssanyu [1] discusses ethics in technical workplace monitoring. The scene for a crisis management operation is a indeed a workplace, and there are many similarities between R&E monitoring and the methods and techniques that they mention; such as wiretapping, screen capturing, keyboard input logs, computer network surveillance, video recording, e-mail forwarding, etc. All of these technical monitoring solutions can be very useful in R&E, all depending on what aspects of work the OTs need to review. Hence, the arguments that [1] are using are worth considering for R&E.

The fundamental conflict of values concerning workplace monitoring is about the employees' right of privacy versus the employer's right to ensure that he/she gets value for his/her investments. That workplace monitoring does exist today is well known, and society seems to still be functioning, so maybe it is not a real problem after all? Kizza and Ssanyu [1] points at nine negative consequences of the workplace monitoring:

- Lack of trust between workers, supervisors and management,
- stress and anxiety,
- repetitive strain injuries because of refraining from taking breaks,
- lack of individual creativity,
- reduced or no peer social support,
- lack of self-esteem,
- worker alienation,
- lack of communication and
- psychological effects.

Some of these effects are the result of a lasting monitoring of an individual, and I do not believe that these are directly applicable to the domain of this study. However, it is reasonable to suspect that at least consequences 2, 4, 5, 6 and 8 exist also in the crisis management domain. The latter of them is something that can clearly be noticed during exercises as training audience sometimes turn off monitoring equipment to allow them to speak freely. This implies, not surprisingly, that monitoring does infringe on their privacy.

Palm [14] states, with reference to Alpert [15], that new technology has enabled employers to shift performance monitoring to target individuals as opposed to teams as was the case earlier. I second that opinion, and I see the same tendencies in the AAR domain, i.e. more and more technology-based solutions are implemented; making it easier to assess individuals rather than teams. As gadgets are easy to reproduce and relatively cheap, it does not always occur to the OTs that there may be a reason to minimize the amount of recording equipment instead of just adding more gadgets. The way to remedy this is to spend more time preparing the setup by thorough modeling and instrumentation planning in the initial phases of R&E, to carefully decide what recording is necessary and what is not. If this step is not properly managed, there is an apparent risk that the training audience gets a lower trust in the monitoring and develops a negative attitude towards it. However, with reference to Merz Smith [16], Palm argues that it is not just employers that benefit from this type of monitoring [14]. She continues to explain that employees can regard it as a positive experience that their hard work is being noted and that 'leeches' will have a harder time getting away with their laziness – especially since this type of monitoring is more objective than having a person watching over your shoulder and possibly favoring or discriminating among the employees. In the same manner, first responders and crisis management workers could benefit from monitoring, especially live operations, since they get an means to prove that they acted correct based on the information available to them at the time, and thus avoid criticism from the "all-seeing, never-knowing" public. This reasoning is something that Miller [2], among others, uses and I will return to it later in this paper.

Palm [14] especially mentions four risks of continuous and systematic collection of personal data:

- Unavoidability,

 ISBN: 978-1-61208-167-0

- continuity,
- dependency and
- identifiability.

By unavoidability she means that as an employee you have little or no say on what kind of data is collected about you, other than by changing jobs. By continuity she refers to the problems of continuous monitoring, which can have consequences for your privacy. The dependency issue she mentions is about the employee's dependency towards to employer and that there is therefore an asymmetric power relationship between them. The last bullet, identifiability, is negative according to Palm since it makes it easy to combine different data to find patterns and profiles that the monitoring system was not originally designed to do. She concludes that at the workplace you are more vulnerable to privacy violations than elsewhere. Whether her remarks are valid in the domain studied here is not easy to settle. For instance, it is obviously easy (and recommended) to give every member of the training audience a choice to accept monitoring and be part of the R&E evaluation, or to stay out, which should directly cross out the first bullet on her list. However, what is not clear is what will be the consequence of staying out. Is this person going to be replaced? Is the exercise going to continue as planned, with an altered instrumentation plan? Will the declining individual miss out on valuable training experience? If so, will that reduce his/her ability to operate in a crisis management operation? Ultimately, can the consequence become failure to save lives because of inadequate knowledge? In effect the unavoidability may still be a problem then.

The aspect of continuity that Palm mentions is probably not as relevant in this study, since data collection is only being done during exercises, or possibly on some live operations. There is no reason to continue the collection during regular duty, at least not for the purpose handled in this paper. The issue of dependency however may face the exact same problems as in her study since there is often a well-defined hierarchy of command in these organizations where the same power-issues arise. Identifiability can also become a problem for R&E since typically much of the data streams are associated with individuals, making it very easy to deduct personal information that the system was not intended for. To avoid this there are techniques to de-identify persons, but that can potentially cause problems for the OTs as they need to know who was responsible for decisions and actions to interview them on their thoughts at that time.

A contractarian would be able to claim that Palm's dependency relationship between employer and employee is in fact a contract where the employee gives up some fundamental rights to privacy by accepting the job offer, especially so in the public sector since tax payers have a reasonable right to demand that their tax money is used for greater good. Since both parties have agreed to this contract, the employer should then be entitled to perform this monitoring according to the contractarian. To further strengthen the argument, some employers are adding monitoring clauses into the employment contract to clarify that his rights trump the individual's right of privacy. By signing the contract the employee can be considered as having given consent to the monitoring and therefore there is not an ethical issue at hand. To counter this, you could argue that the employee in reality has no good options, since by refusing to sign he or she would be unemployed and have no income. For instance, many philosophers compare this to voluntary slavery, which according to the contractarian would not be a problem, while someone with a broader perspective would argue that there may be problems with information or other issues that makes the contractee not understand the consequences of what is being agreed. In the field of medicine the notion of *informed consent* is often used. Malek [17] defines it as 'voluntary consent based on adequate understanding of relevant facts'. She mentions five important parts of informed consent:

- That the subject is given all information,
- that the subject understands all information,
- that the subject is able and allowed to make a choice,
- that the subject makes the choice without involvement of a third party and
- that the subject actually gives consent.

Within the area of medicine, this form of consent is necessary to conduct certain procedures. Clarke [18] states, and I concur, that the same requirements should be applicable to infringements of privacy such as through monitoring. He points at several actual problems within this area, such as installation of new surveillance equipment without explicit consent from employees. For the sake of R&E evaluation, this does not necessarily impose a problem as the equipment can be setup temporarily and that the training audience can easily be informed of all the data collection that will take place.

Of greater relevance to this study is the notion of *continuous informed consent* that [18] describes as extra complicated since the subjects may find it difficult to grasp in what way the surveillance equipment will be used in the future. E-mail forwarding on the workplace, for instance, can be used to counter industrial espionage. Although this can itself be very controversial and sensitive to some, it is not difficult to imagine that some employees accept this privacy infringement and agree to setting up the system. When employers use the system to create detailed analyses of their employees friends and relationships to find persons at risk of being targeted by spies, it all of sudden becomes a lot more violating to privacy and it is not likely that the subjects would agree anymore. Therefore a mechanism is needed that allows informed consent to be revoked. This applies also to evaluation of distributed tactical operations since combining several data sources can enable detailed profiling of individuals and teams that was not obvious at the start. It is clearly relevant to ask whether the subjects' consent can be regarded as informed according to the definition in [17] when the objective of data capture may be unclear even for the OTs at the time when participants give their consent.

It would be very valuable to conduct empirical studies to decide how crisis management workers relate to workplace monitoring and give them a chance to give an informed consent. Such studies have unfortunately not been conducted for this particular paper, instead I will look at three empirical

 ISBN: 978-1-61208-167-0

studies [19] to continue my reasoning. They interviewed employees and students in Ireland and Great Britain to, somewhat surprisingly, conclude that employees do not regard workplace monitoring as problematic. Based on that finding, they question whether there is any point in discussing the ethics in it. A more detailed review of their studies shows that there seem to be quite a few interviewees that actually do consider monitoring as a problem, although the majority does not. This is a result that I find less surprising as the level of privacy infringement one can allow before feeling violated is highly personal. To state, as the authors do, that monitoring is then not problematic is to neglect that portion of the population that does, and I would say that their conclusion that employees do not consider monitoring a problem is therefore greatly exaggerated. They do, however, extend their reasoning and argue that surveillance reduces self-esteem and creativity among the subjects, just as Kizza and Ssanyu reported [1]. According to [19] this can happen without the subjects even realizing it, which makes the problem even more complicated, and again we have to revert to theories on informed consent. To count as an informed consent, the subjects need to understand what monitoring exists and how it affects to them, which according to [19] is not always the case.

First response and crisis management work differ from the kind of office work studied in [19] in the sense that workers are part of a process that fills an important role in society safety that we as tax payers and citizens rely upon and consider ourselves entitled to demand. Miller [2] makes a similar statement when he focuses on monitoring of police officers in their daily work. He notes that there are both differences and similarities compared to office workplace monitoring. He describes privacy as a morale right that all humans have, regarding control over information on themselves and how they are seen by others, sometimes referred to as the 'private sphere'. He argues that no matter who you are and in what situation you are in, the right of privacy always applies, and as such there is a problem in monitoring police officers since they in fact lose control over who sees them and how. From his reasoning we can deduct that workplace monitoring is an infringement on privacy regardless of workplace, and therefore also for the purpose of evaluating distributed tactical operations. My own conclusion is that there is a clear problem with workplace monitoring that does apply to exercises and operations of a distributed tactical character, such as the ones mentioned earlier. The problem lies in a violation of privacy of the training audience and it must be weighed against the positive effects that the R&E evaluation gives. How personnel reacts to this infringement on privacy can differ a lot, but I also note, with respect to [19], that problems can exist that the subjects are not aware of or has given consent to, since the effects can be subconscious, which according to [17] then negates the consent.

B. Can we demand that crisis management personnel accept an infringement on their privacy?

As argued above, there seems to be an infringement on crisis management personnel's privacy when being evaluated using AARs, and we must be able to motivate that this is an acceptable cost if we as a society are going to accept this infringement. In this section I will compare some of the pros and cons of monitoring, and try to relate that to the infringed privacy to establish a consistent view on R&E monitoring.

As [2] states, society as a whole benefits from a well functioning police, in the same manner it benefits from not only having well functioning crisis management organizations, but also just knowing that it works well can have a calming and positive influence on society. This means that a utilitarian could argue that privacy infringement on crisis management workers is accepted to create a better society. Ross' pluralism [20] tells us that there may more to the story and implies a paradox here, as we will have two duties facing each other: the duty of beneficence vs. the duty of non-maleficence. Which duty is our prima facie in this case is not obvious in the pluralistic deontology of Ross. An interesting recent such scenario, non-related to monitoring, is that of the triple disaster in Japan causing a nuclear crisis in Fukushima; any worker approaching the reactor faced an obvious risk of being exposed to lethal doses of radiation, not to mention risks of explosion and collapsing buildings. How can anyone be asked to go to work during such conditions? Meanwhile, society faced the risk of meltdown and an even larger calamity.

The utilitarian reasoning would be to put the duty of society's best first, which I can partly sympathize with. It is however, as so often in ethics, a trade-off and we have to be careful in our reasoning and not forget that sometimes creativity may suffer. In a crisis situation where routines and resources are not enough, individual creativity is often what drives the work. If we in our strive to evaluate our societal functions render them inefficient, it may mean that fewer lives can be saved at the next disaster, which will then be the price we pay to feel safer; a very disturbing and contradictive thought in itself. A consequentialist would of course argue that this is therefore the wrong path. Although the consequences here are stretched to the extreme, I argue that there are risks both in monitoring too much and too little.

A very important difference that Miller [2] mentions is that the police are expected to serve society and that they therefore are prepared to accept a higher degree of monitoring and a reduced privacy, and that this is all well-known to them when they apply for the job. He also points at pros in monitoring where police officers can use audio and video recording to prove that they acted correctly when being questioned after severe incidents.

The type of monitoring that Miller [2] deals with, is more or less constant during daily work. When it comes to evaluating distributed tactical operations, it is always a matter of well planned exercises that are out of normal work. This has two major implications for the reasoning in this study. Firstly, the infringement on privacy is temporary and thereby easier to accept. Secondly, it is not at all safe to assume that the workers are used to this type of monitoring and some may react different than those who are used to it. This can result in the workers being so intimidated that their creativity and performance become dramatically reduced.

 ISBN: 978-1-61208-167-0

The arguments in [2] are partly applicable to the crisis management domain. It is clear that the workers have a greater acceptance to monitoring than would employees at an ordinary workplace, especially in the distributed tactical operation scenarios that this study deals with, as the monitoring is temporary. However, even though I lack evidence thereof, I can still imagine that the monitoring can affect the training audience to the extent that the evaluation becomes counter-effective. To minimize the risk of that, it is vital to inform every member of the audience of the benefits of evaluation and clarify that AARs are all about generating feedback to the team and that the assessment is primarily on team level, not personal.

VIII. CONCLUSION

Evaluation of distributed tactical operations is an important tool to verify and validate crisis management work and refine it. Technology advances quickly and generates more sophisticated tools to analyze the work. In my opinion, society benefits from going forward with this type of evaluations, but we should be careful and aware of the processes that are activated at the training audience. There are many similarities with workplace monitoring as [1] defines it, and crisis management workers are facing the same problems, albeit at a different scale and for other purposes. Based on [2] and [19] I have concluded that privacy infringements exist and a too aggressive and technology-oriented evaluation may reduce performance among the audience and thereby become counter-effective.

To motivate R&E it is important that every member of the training audience gets a chance to give their informed consent, according to the definition in [17], to minimize the negative effects. It is also desirable, although not always possible; to on beforehand define exactly which questions will be involved in the evaluation and reduce data collection so that not more is collected than needed to answer those questions. By doing that, the amount of persons that have their privacy infringed reduces, as does the extent. Collected data should also be restricted to only authorized analysts.

To not violate the right of control over information about yourself, all members of the training audience should also be notified of the data that has been collected on themselves, i.e. recorded radio communication, GPS track logs, collected e-mails, etc. and be given a veto right on what can be used in further studies and who it is shared with. I believe that the mere knowledge of this right would increase acceptance among the audience and reduce anxiety as well as risk of reduced creativity. Of course the propositions herein would benefit from an empirical study, and I welcome such a study. However I warn anyone undertaking such a study to be aware that it is not always clear to the subjects what problems they are exposed to.

REFERENCES

[1] J. M. Kizza and J. Ssanyu, “Workplace surveillance”, Electronic monitoring in the workplace: controversies and solutions, J. Weckert, Eds. Hershea, PA: Idea Group Inc. Publishers, 2005.

[2] S. Miller, “Guarding the guards: the right to privacy, and workplace surveillance and monitoring in policing”, Electronic monitoring in the workplace: controversies and solutions, J. Weckert, Eds. Hershea, PA: Idea Group Inc. Publishers, 2005.

[3] D. Andersson, S. Pilemalm, and N. Hallberg, “Evaluation of crisis management operations using reconstruction and exploration”, Proc. 5th International Information systems for crisis response and management conference (ISCRAM 2008), Washington, DC, USA, May 2008, pp. 118-125.

[4] S. Pilemalm, D. Andersson, and N. Hallberg, “Reconstruction and exploration of large-scale distributed operations – multimedia tools for evaluation of emergency management responses”, Journal of Emergency Management, vol. 6, iss. 4, 2008, pp. 31-47, Weston Medical Publishing, LLC.

[5] Headquarters Department of the Army, A Leader’s Guide to After-Action Reviews (TC 25-20), Washington, DC, Sep. 1993.

[6] W. J. Rankin, F. C. Gentner, and M. J. Crissey, “After action review and debriefing methods: technique and technology”, Proc. 17th Interservice/Industry Training Systems and Education Conference (I/ITSEC 1995), Albuquerque, NM, USA, pp. 252-261.

[7] J. E. Morrison and L. L. Meliza, Foundations of the after action review process, Special Report 42. Alexandria (VA): United States Army Research Institute for the Behavioral and Social Science, 1999.

[8] Guy Carpenter & Company Ltd., “Windstorm Erwin/Gudrun – January 2005”, Specialty Practice Briefing, iss. 2, pp. 1-14, http://www.guycarp.com/portal/extranet/pdf/Speciality_Briefing_170105.pdf, retrieved 2011-05-11.

[9] T. Lay, H. Kanamori, C. J. Ammon, M. Nettles, S. N. Ward, R. C. Aster, S. L. Beck, S. L. Bilek, M. R. Brudzinski, R. Butler, H. R. DeShon, G. Ekstrom, K. Satake, and S. Sipkin, “The great Sumatra-Andaman earthquake of 26 December 2004”, Science, vol. 308, 2005, pp. 1127–1133.

[10] J. Cassuto and P. Tarnow, “The discotheque fire in Gothenburg 1998 – A tragedy among teenagers”, Burns, vol.29, iss. 5, Elsevier Science Ltd., Aug. 2003, pp. 405-416, doi:10.1016/S0305-4179(03)00074-3.

[11] Estonia Commision (Joint accident commission of Estonia, Finland and Sweden), Final report of the M/S Estonia disaster of 28 September 1994, Helsinki, Finland: Edita Ltd., 1997.

[12] S. D. Warren and L. D. Brandeis, The Right to Privacy, vol. 4, no. 5, Harvard Law Review, 1890.

[13] J. R. Aiello and K. J. Klob, “Electronic performance monitoring: A risk factor for workplace monitoring”, Organizational Risk Factors and Job Stress, S. L. Slater and L. R. Murphy, Eds. American Psychological Association, 1996, pp. 163-179.

[14] E. Palm, The ethics of workplace surveillance, Doctoral thesis in philosophy from the Royal Institute of Technology, Stockholm, Sweden, ISBN 978-91-7178-818-4, 2007.

[15] S. A. Alpert, ”Protecting medical privacy: Challenges in the age of genetic information”, Social Issues, vol. 59, no. 2, 2003, pp. 301-322.

[16] E. Merz Smith, Everything is monitored, everything is watched – Employee resistance to surveillance in Ontario call centers, MA thesis, Dept. of Sociology, Queen’s University, Canada, 2004.

[17] J. Malek, “Informed consent”, Encyclopedia of Science, Technology and Ethics, vol. 2, C. Mitcham, Eds. Detroit: Macmillan Reference USA, 2005, pp. 1016-1019.

[18] S. Clarke, “Informed consent and electronic monitoring in the workplace”, Electronic monitoring in the workplace: controversies and solutions, J. Weckert, Eds. Hershea, PA: Idea Group Inc. Publishers, 2005.

[19] B. C. Stahl, M. Prior, S. Wilford, and D. Collins, “Electronic monitoring in the workplace: If people don’t care, then what is the relevance?”, Electronic monitoring in the workplace: controversies and solutions, J. Weckert, Eds. Hershea, PA: Idea Group Inc. Publishers, 2005.

[20] W. D. Ross, The right and the good, Oxford: Clarendon Press, 1930.

 ISBN: 978-1-61208-167-0