Watchdog or Guardian? Unpacking the Issues Surrounding the Monitoring of InfoSec Employees

T. Whalen[1] and C. Gates[2]

[1] Perigraph Solutions, Ottawa, ON, Canada
[2]CA Labs, Islandia, NY, USA
e-mail: tjwhalen@gmail.com

Abstract

Much work has been conducted on the use of monitoring to improve quality of life (in such domains as the healthcare industry) versus the privacy trade-offs associated with such monitoring. However, little work has been done on the impact of monitoring on employees with information security responsibilities. We present here some initial results from interviews with such professionals, focusing on those who operated in classified environments. In particular, we draw attention to the benefits to being monitored that these employees identified: increased feeling of personal security, the presence of someone to help prevent you from making mistakes, simplifying collaboration in some instances, and the presence of an audit trail for employee protection. We also outline some of the complicating factors that may diminish these benefits. While government monitoring often has a negative connotation, we demonstrate that there are cases when *voluntary* monitoring *as a condition of employment* can be seen to have advantages to the employee.

Keywords

Employee monitoring, privacy, information security professionals.

1. Introduction

> At times, security practices and procedures cause personal inconvenience. They take time and effort and on occasion may make it necessary for you to voluntarily forego some of your usual personal prerogatives. But your compensation for the inconvenience is the knowledge that the work you are accomplishing at NSA, within a framework of sound security practices, contributes significantly to the defense and continued security of the United States of America.
>
> –excerpt from NSA employee handbook ("Security Guidelines," 1994)

This quote from the NSA handbook lays out a traditional dichotomy that arises in many information security (infosec) workplaces: the tradeoff between "personal prerogatives" (such as privacy) and national security. However, this description of polar opposites is a simplistic rendering of a complex dynamic: there are more factors for employees to consider than merely whether (or how) to sacrifice their liberties on the altar of security. In this paper, we explore one of the elements of infosec workplaces—monitoring—and demonstrate the ways in which this type of

monitoring does not simply result in negative effects for employees: there are a few positive aspects as well that can provide a degree of compensation for the inconvenience and intrusion that monitoring causes. In addition, we will describe some factors that can influence an infosec employee's decision as to whether or not the monitoring is tolerable.

This is primarily a position paper on the topic of infosec monitoring. However, to investigate infosec monitoring practices, we conducted a preliminary study, starting with four employees who held high-level clearances at American organizations involved with information security. In this paper, we will describe our early findings, combined with our exploratory thoughts on this emerging topic.

2. Monitoring: A Definition

Monitoring has many different definitions, depending on the context. For example, monitoring in terms of auditing and compliance in the healthcare industry has been defined as "an on-going process usually directed by management to ensure processes are working as intended." (Ruppert, 2006)

Many other publications discuss monitoring, and even specifically monitoring in the workplace, however they do not provide a definition. For example, Nord *et al.* (2006) discuss the legislative issues behind monitoring in the workplace, noting that often employer surveillance of employees is not protected by privacy legislation. Indeed, private corporations have very few regulations that govern their collection of employee information. However, their investigation focused on electronic surveillance of employees, specifically employee email and internet usage. Weckert discussed the issue of such monitoring in the workplace in the context of trust between employees and employers (Weckert, 2000), arguing that increased monitoring of employees erodes trust in the workplace, and that this has negative consequences for both employees and employers.

We define monitoring differently in this paper, extending the definition beyond those used by Nord *et al.* and Ruppert, to be: "processes and procedures for investigating employees and watching their on-going actions, designed to ensure that both the safety of employees and the needs of the employer are being met." Note that this definition can include the collection of personal information before offering an individual a position within a company (such as the standard background investigations performed by many private companies), as well as the ongoing collection of information about an employee, either self-reported or collected automatically through surveillance methods (such as those described by Nord *et al.*). In this respect, we extend the definition implied by both Nord *et al*. and Weckert. We extend Ruppert's definition to protect the employee as well as the organization.

3. Types of Personal Information that are Monitored

As described above, we are including types of personal information disclosed during the employment screening process, including that which is collected for obtaining a

security clearance. To give an idea of the types of information used in screening, we provide examples here from the Standard Form 86, a questionnaire that is used by government and military agencies and security contractors (U.S. Office of Personnel Management, 2008). This form requests such information as addresses of residences, schools, and employment for the past 7-10 years; contact information for references and relatives; a list of any foreign nationals with whom you have close contact; foreign travel; any mental heath issues; police record; illegal drug use; financial history; computer misuse; and "associations" (e.g., membership in terrorist groups). During the background check, in-person visits of neighborhoods (and neighbors) may be conducted, and a person's references (i.e., individuals listed on the form) are interviewed for detailed information about the applicant.

Some organizations require additional information, such as medical screening, psychological testing, or a polygraph test. The polygraph test can take different forms, with varying scope. For example, a CounterIntelligence (CI) polygraph is restricted to topics such as espionage and terrorism ("Counterintelligence-Scope Polygraph"). A more comprehensive type of polygraph is the Lifestyle polygraph, which is not restricted in scope and often includes highly personal questions, such as those about one's sexual history (Bamford, 2001).

Once the screening is completed, most of the information is not routinely re-investigated, although some personal information is subject to being re-checked at any time during employment. Additionally, some items, such as finances, often require regular (annual) reports for certain personnel. In some cases, information is re-collected after an interval: for instance, NSA policy requires that a simplified-scope polygraph (not Lifestyle) be retaken once every five years.

Ongoing monitoring was the focus of our study: those pieces of information that employees are required to report regularly, as well as day-to-day procedures for information protection in the workplace. One category of items that employees might need to report is any major event that could pose a risk of blackmail (such as an unreported crime). A fairly comprehensive set of guidelines was published by the U.S. Department of Energy ("Counterintelligence Reporting Requirements"), which includes reporting on, and/or approval of, the following items: professional relationships, and visits with, foreign nationals; foreign travel ; personal relationships with foreign nationals; financial relationships with foreign nationals; unusual solicitations of information; "anomalies" [very broadly defined]; and any espionage indicators observed by employees, such as a co-worker who makes "excessive use of copiers" (p. 9).

In addition to information reporting, there are also procedures and processes in place at some agencies, designed to prevent information leaks, which employees are subjected to. One of these is the NSA "paper check" (humorously described in Stoll's *The Cuckoo's Egg* (1990)): bags were searched as part of a routine exit check, to ensure that no sensitive papers were removed from the building. Another procedure is regular "roll-calls": employees are expected to sign in for work each day (unless leave has been approved or a supervisor has been contacted about an

absence): if an employee has an unexplained absence from work, a search may be carried out to determine that person's whereabouts.

4. Overview of Preliminary Study

We conducted a series of qualitative interviews. Participants were recruited through personal contacts (of the authors) as well as through an infosec mailing list. To be eligible, participants needed to have experience in a high-security environment, and preferably held (or formerly held) a security clearance. The interviews were semi-structured and took approximately one hour to complete. Questions focused primarily on the participants' experience with security screening, ongoing requirements for reporting, and any critical incidents in the workplace that affected their attitudes toward monitoring. Because the respondents were located throughout the United States, interviews were conducted over the telephone. Data was collected through experimenter notes and voice recording.

Purposeful sampling was used to select a set of four typical-case participants, which provided a sample of information-rich cases for in-depth study. The four participants that we interviewed (3 male, 1 female) were all from American organizations: two were retired from government agencies, the third worked at a government agency, and the fourth had worked at a defence contracting corporation. All held clearances to at least the Top Secret level, and all had at least four years' experience in an infosec work environment that required such a clearance.

Although the number of participants (n=4) is relatively small, it is appropriate for this type of ethnographic in-depth qualitative research. The approach we followed here was to provide insight into a specific situation: "to discover meaning and understanding, rather than to verify truth or predict outcomes." (Myers, 2000). This approach provided a methodological foundation for deep understanding of the specific phenomenon of infosec employee monitoring. To situate this work within the broader research literature, we note that a number of formal research studies have successfully used small, inclusive sample sizes of three to five participants. Examples of these studies abound within a range of research disciplines, such as education (Gibson and Peacock, 2006; Skrla et al., 2000), medicine (Luck and Rose, 2007; Zabinksi et al., 2001), and computer science (Nedstam et al., 2001; Hearst and Pedersen, 1996; Kelly *et al.*, 2007). To illustrate with a related example from infosec research, a study of virus writers was conducted with four participants (Gordon, 1996). To summarize, our sample size is validated by comparable empirical studies as well as by the qualitative research approach.

5. Employee Monitoring: Compensating Factors

5.1. Personal security

Perhaps the theme that most consistently arose in the interviews was the notion of there being a level of personal security inherent in the reporting and monitoring process. It was recognized that many of the requirements had been put in place in order to protect the employees should they be targeted by other organizations wishing to obtain particular information. Interestingly, everyone we spoke with had encountered at least one incident during their tenure where they had been comforted by their agency having measures in place to monitor and protect them.

One example of this was one interviewee, who was questioned intrusively by a seatmate during a plane trip. She noted that it was comforting to have someone that she could call upon landing to report the incident, knowing that her agency would be watching to ensure that she was safe.

Another interviewee had an experience where, when he checked into a hotel room in a foreign country, the front desk staff rather loudly stated his name and that he was from the "State Department". There were other people sitting in the lobby, reading newspapers, who would have easily overheard the lady. Once he had retired to his hotel room, there was a knock on the door from a young blonde lady. He turned her away, only to receive a knock on the door a few minutes later from a young brunette. He turned her away as well, only to receive a knock on the door a few minutes later from a young gentleman! After explaining that he was not interested in receiving "services" from anyone, he was left alone. However, to this day, he is unsure if the hotel provided such services on a routine basis, or if he had been targeted.

A third interviewee recounted an experience where he was at a conference and a Soviet representative, whom he knew only in passing, gave him a gift for his new grandchild. He reported the incident to his security staff, who responded with "Yes, we know him."

The fourth interviewee noted an experience where he had taken the day off, however his supervisor had forgotten to record this. When he did not arrive for work, his organization looked for him. While he felt that this was an over-reaction, at the same time it "made me realize...if I were ever kidnapped, because I was exposed to sensitive information there would be a sense of urgency there [to be rescued]."

In general, all of our interviewees recognized that they were vulnerable due to the nature of their work (such as what they knew, where they worked, and even at times their physical locations such as embassies or military bases). They noted that it was reassuring knowing that there was someone watching out for you (e.g., through roll-calls or with more general monitoring). One interviewee noted that she appreciated that she "had someone in my corner." Another interviewee, who is currently retired, commented "I had forgotten how nice that was," despite his having problems with the politics of his organization.

5.2. Catching Mistakes/Having a "Second Set of Eyes"

A second advantage to being monitored that the interviewees noted was the presence of a "second set of eyes" that can help catch innocent mistakes. One example of this is the publication review process, where the organization is required to review any material before it can be submitted for external publication. In every case, the interviewees appreciated this process, as it helped to ensure that they were not accidentally releasing classified information.

Another example provided was when security staff used to check all of papers being removed from the organization to ensure they were not classified. Interviewees who worked at that organization, interestingly, were not embarrassed at being caught with papers they should not have but were rather relieved that they did not accidentally remove the information. For example, one of our interviewees commented that if you found out that you had accidentally removed classified information, "[once you got home], God, you felt guilty!"

The advantage of having someone else confirm that you were not accidentally removing classified information was underscored by stories from another interviewee, who noted a couple of events where there were fires in the garbage cans at hotel or conference washrooms. While unconfirmed, it was suspected that these fires were started by someone who discovered they had classified information on their person, and thus they needed to destroy it quickly.

5.3. Simplifying Collaboration

Despite the reporting requirements, particularly when interacting with foreign nationals, there were aspects of the monitoring that were identified by the interviewees as simplifying collaboration. There were typically two scenarios that were identified here.

The first scenario involved interactions with foreign nationals. As a general rule, any significant interactions are required to be reported, which would seem to discourage collaboration. However, one story related to us involved a foreign national from one of the particularly sensitive countries. In this case, the interviewee asked their organization if there would be any issues in working with the foreign national, and was told that it would be all right. This provided a sense of comfort to the interviewee – as the foreign national had now essentially been vetted – and the result was a productive relationship that otherwise might not have been possible.

The second scenario involves working on a team, particularly either within your own organization or with people from other government organizations. In this case, the presence of reciprocal clearances made collaboration both easier and smoother. For example, everyone on such a team would be aware of the monitoring and reporting requirements, and would understand how information should be treated. This allowed the team to relax to some degree, as they knew that everyone else in the room had their "tickets" and so had already been vetted as trustworthy.

5.4. Audit Trails

One final advantage that was identified by interview participants was the advantage of there being an audit trail. The advantages here fell into two categories: audit trails as evidence, and the ability to "keep honest people honest."

In the first case, it was often noted by our interviewees that audit trails are there to help protect employees. For example, if an employee reported on an incident, then this started an audit trail, so that no one could later claim that the employee had not followed proper procedure or that he was not following reporting requirements.

In the second case, some interviewees noted that knowing there was an audit trail helped keep them honest. There was never any temptation to not report something or to shortcut the system because of the audit trail. As one interviewee stated: "monitoring is a bit of a help because it helps me keep my word." On a related note, a discussion point that was reported informally to the authors during the early stages of this project (not through formal interviews), is that stress or emotional upset could lead to corners being cut in his infosec job: "[on a bad] day, I don't even want to *think* about anything but doing the right thing. That requires accountability." Thus the audit trail guides this person towards appropriate behavior, particularly at those times when he is most susceptible to ignoring proper procedure.

6. Complicating Factors: Aspects of the Work and Workplace

When employees are determining whether the nature and degree of monitoring is tolerable for them, there are other factors that are brought to bear on the equation. These elements, if handled incorrectly, can tip the balance and make the monitoring demands far less acceptable. The factors that we have identified below emerged from analysis of the employee interviews that we conducted; these were not specifically elicited, but arose from the overall comments that our participants provided.

6.1. Professionalism

One element mentioned by several interviewees was the importance of professionalism, particularly in how the security officers handled information that the employees reported to them. Interviewees described their need to know that the people to whom they reported would handle information with discretion, in a trustworthy fashion, and with measured response. In particular, some of the employees we spoke to expressed strong dislike for incidents when the security team overreacted to what they believed to be a routine report; this response made them less comfortable with making security reports. Similarly, one interviewee described frustration when dealing with the security team to whom he reported, as they were unable to provide suitable advice for how to proceed with a security matter, because his work was highly specialized: they would not give informed guidance but would later tell him that he had acted incorrectly. The relationship between employees—those who report and those who deal with reports—can be damaged in cases such as these, leading to a lack of trust and confidence.

6.2. Openness

A factor that is related to professionalism is that of *openness.* Some interviewees expressed a desire to know more about the reporting process, such as basic policy information (e.g., who handles info, how long it is kept, the security screening process). One example provided by an interviewee was that he expected to be told that that his neighbors would be contacted during his background check. As it happened, he expected this, but this knowledge arose from sources other than his potential employer. He posited that someone who did not know as much as he did about screening might find this activity upsetting if they were not warned.

Maintaining openness (within limits appropriate to high security environments) can be helpful for establishing a trust relationship between an employee and the organization. Indeed, one long-term infosec employee that we spoke with stated that "I trust my agency far more than the government at large."

A final point raised by one interviewee is that openness of the process is helpful for non-employees as well—specifically, for the general public, whom infosec employees interact with professionally or socially (or both). She stated that when people don't know how the process works (for example, how information is collected and handled), then the only impressions they get "are from the movies," which are usually wildly inaccurate. To counteract this misinformation, some degree of openness to the public is required.

6.3. Scope

A number of participants mentioned that they could handle the monitoring because it was limited in scope: if the reporting requirements became too onerous, for example, they could find another job. (This is in contrast, say, to covert government wiretapping, which is not voluntary and is not restricted to work-related activities.) Much of the friction mentioned in interviews came when the reporting requirements spilled over into private life. One example mentioned by an interview participant was avoiding social contact with a friend whose visa status was questionable: the participant did not want to "rat out" that friend, but knew that the contact needed to be reported. Another interview participant avoided going to a social event with a spouse's colleague, to avoid having that person investigated. These types of social incidents seemed to cause strain. To the extent that the reporting remains within the work domain, and with the assurance that reporting requirements will be lifted when the high-security job is over, employees seem more tolerant of monitoring.

7. Related Work

The privacy, convenience, and security tradeoffs involved in monitoring have been explored in contexts outside of information security, such as telecare. Telecare is a technological form of assisted care that requires health information to be collected (and sometimes transmitted). Telecare "involves the use of sensors within people's homes or worn on their bodies, connected to a monitoring centre and then to a

response service. This both provides an 'electronic security blanket' for those at risk of medical or other physical risk and more continuous monitoring to allow the early detection of changes in an individual's condition." (Barlow and Curry, 2006, p. 399). The privacy implications of telecare are readily apparent: information of a deeply personal nature—health—is being monitored by other parties. However, despite concerns over confidentiality, some patients find that telecare is worth the tradeoff. A telecare researcher stated that he has been contacted by patients who are more than willing to provide health information (within reason) to maintain personal freedom: "A lot think they've already lost their privacy by being institutionalized. They say, give me a break, I'm perfectly willing to share information with my daughter or whoever in order to continue to live in my own home." (Ross, 2004).

Within the broader domain of workplaces in general, employee monitoring is also performed (e.g., Watkins Allen et al. (2007)), but usually for reasons other than the protection of information or personnel security (such as efficiency); this monitoring is also usually performed automatically by the company, rather than being initiated from the employee. Thus, this type of monitoring is outside the scope of our discussion of infosec workplaces, as it is not specifically applicable to our topic; we will mention, however, that there has been a great deal written about the privacy implications of such monitoring, such as Miller and Weckert (1999).

8. Conclusions and Future Work

Our study to date has been preliminary in nature, although we have begun to identify some of the factors that come into play when infosec employees consider whether or not they find voluntary monitoring acceptable. The negative factors of monitoring, such as privacy intrusions and additional effort required, have been readily recognized. However, we have added two elements to the discussion of infosec monitoring. First, we have identified some positive elements of monitoring that *may* (for some employees) serve to compensate for the negative aspects. Second, we have proposed a number of complicating factors than can shift the balance, such that monitoring can become more or less acceptable, such as the degree of professionalism and openness that an employee experiences in an organization. Because monitoring is thought of as a "necessary evil," it can be endured so long as the limits remain tolerable; despite any mitigating factors, an employee may simply decide that the job is no longer worth the hassle.

Given that our work has identified positive aspects to employee monitoring, at least in high security situations, our future work will focus on determining the extent of this view. For example, it might be the case that there are demographic influences that result in a positive view of some monitoring, or it may be the case that certain responsibilities or experiences alert an employee to the positive benefits. It may also be the case that further investigation will reveal more benefits other than the four we identified. We intend to examine this issue further so that we may provide guidance to organizations in how they can implement a monitoring system that provides benefits to employees as well as the employer.

9. References

Bamford, J. (2001) *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency,* Doubleday: New York, ISBN 978-0385499071.

Barlow. J. Bayer, S. and Curry, R. (2006) "Implementing complex innovations in fluid multi-stakeholder environments: Experiences of 'telecare'", *Technovation*, Vol. 26, No.3, pp. 396-406.

"Counterintelligence Reporting Requirements in the Department of Energy" (year unknown), Office of Counterintelligence, http://www.hanford.gov/oci/maindocs/ci_r_docs/cirepreq.pdf (Accessed 25 February 2009).

"Counterintelligence-Scope Polygraph Examination" (year unknown), Office of Counterintelligence, http://www.hanford.gov/oci/maindocs/ci_r_docs/cipoly.pdf, (Accessed 25 February 2009).

Gibson, S. and Peacock, K. (2006), "What Makes an Effective Virtual Learning Experience for Promoting Faculty Use of Technology?", *Journal of Distance Education*, Vol. 21, No. 1, pp. 62–174.

Gordon, S. (1996), "The Generic Virus Writer II", *Proceedings of the 6th International Virus Bulletin Conference*, http://www.research.ibm.com/antivirus/SciPapers/Gordon/GVWII.html, (Accessed 10 April 2009).

Hearst, M. A. and Pedersen, J. O. (1996), "Reexamining the Cluster Hypothesis: Scatter/Gather on Retrieval Results", *Proceedings of the 19th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, pp. 76–84.

Kelly, D., Wacholder, N., Rittman, R., Sun, Y., Kantor, P., Small, S., and Strzalkowski, T. (2007), "Using Interview Data to Identify Evaluation Criteria for Interactive, Analytical Question-Answering Systems." *Journal of the American Society for Information Science and Technology*, Vol. 58, No. 7, pp.1032–1043.

Luck, A.M. and Rose, M.L. (2007), "Interviewing people with aphasia: Insights into method adjustments from a pilot study", *Aphasiology*, Vol. 21, No. 2, pp.208–224.

Miller, S. & Weckert, J. (1999). "Privacy, the Workplace and the Internet." Journal of Business Ethics, Vol. 28. No, 3, pp. 255–265.

Myers, M. (2000), "Qualitative Research and the Generalizability Question: Standing Firm with Proteus", *The Qualitative Report* [On-line serial], Vol. 4, No. 3/4, Available at http://www.nova.edu/ssss/QR/QR4-1/myers.html, (Accessed 10 April 2009).

Nedstam, J., Höst, M., Regnell, B., and Nilsson, J. (2001), "A Case Study on Scenario-Based Process Flexibility Assessment for Risk Reduction", *Proceedings of the Third International Conference on Product Focused Software Process Improvement (PROFES)*, pp. 42–56.

Nord, G. D., McCubbins, T. F. & Nord, J. H. (2006), "E-Monitoring in the Workplace: Privacy, Legislation, and Surveillance Software." *Communications of the ACM*, Vol. 49, No 8, pp. 73–77.

Ruppert, M. P. (2006), "'Auditing and Monitoring' – Defined", http://www.compliance-institute.org/ pastCIs/2006/106/106%20-%20Handout%201%20Ruppert%20AM-WhitePaper-Definitions_FINAL-Article12022005_.pdf, (Accessed 27 February 2009).

Ross, P.E. (2004), "Managing Care Through the Air", *IEEE Spectrum*, December 2004, pp. 26–31.

Phrack. (1994) "Security Guidelines", *Phrack*, Vol. 5, No. 45. http://www.phrack.com/issues.html? issue=45 (Accessed 10 February 2009)

Skrla, L., Reyes, P., and Scheurich, J.J. (2000), "Sexism, Silence, and Solutions: Women Superintendents Speak Up and Speak Out", *Educational Administration Quarterly, Vol. 36, No. 1, pp.44–75.*

Stoll, C. (1990), *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books: New York, ISBN: 0-7434-1146-3.

U.S. Office of Personnel Management (2008), "Questionnaire for National Security Positions", http://www.opm.gov/Forms/pdf_fill/sf86.pdf, (Accessed 26 January 2009).

Watkins Allen, M., Coopman, S.J., Hart. J.L., and Walker, K.L. (2007), "Workplace Surveillance and Managing Privacy Boundaries", *Management Communication Quarterly*, Vol. 21, No. 2, pp. 172–200.

Weckert, J. (2000), "Trust and Monitoring in the Workplace", *IEEE International Symposium on Technology and Society*, Rome, Italy, Sept 6-8, 2000, pp. 245–250.

Zabinski, M.F, Wilfle, D.E, Pung, M. A., Winzelberg, A.J., Eldredge, K.E., and Taylor, C.B. (2001), "An Interactive Internet-Based Intervention for Women at Risk of Eating Disorders: A Pilot Study", *International Journal of Eating Disorders*, Vol. 30, No. 2, pp. 129–137.