Summer 2014

Systematic ICT Surveillance by Employers: Are Your Personal Activities Private?

Arlene J. Nicholas
Salve Regina University, nicholaa@salve.edu

Systematic ICT surveillance by employers: Are your personal activities private?

Arlene J. Nicholas, PhD

Salve Regina University
Newport, Rhode Island, USA
arlene.nicholas@salve.edu

Abstract. This paper reviews the various methods of information and communications technology (ICT) that is used by employers to peer into the work lives and, in some cases, private lives of employees. Some of the most common methods – such as computer and Internet monitoring, video surveillance, and global positioning systems (GPS) – have resulted in employee disciplines that have been challenged in courts. This paper provides background information on United States (U.S.) laws and court cases which, in this age of easily accessible information, mostly support the employer. The paper does not provide a detailed analysis or present and defend the author's opinions nor does it undertake any form of comparative study of U.S. (and other nations') legislation. Assessments regarding regulations and policies, which will need to be continually updated to include new methods of employee monitoring, are considered. Whether employees are working from an office or home, using personal or company equipment, it is argued that they should be notified of any monitoring. The researcher also suggests that any such monitoring should only be used for business purposes. Future studies on employee satisfaction and productivity, that may identify employees' tolerance and acceptance of systematic ICT surveillance, are recommended.

Keywords: Keywords: court cases, Electronic Communications Privacy Act, employee monitoring, e-mail, GPS, ICT, privacy, social media, Stored Communications Act, U.S. laws

1 Introduction

In order to protect clients, workers, and their own reputations, organizations need to scrutinize the dissemination of company information to prevent loss of trade secrets, guard client data and thwart harassing e-mails. Information and Communications Technology (ICT) is utilized by companies to monitor many of these three activities as well as observing the productivity of employees. The rationale for the latter task is to increase efficiency of services and to prevent cyber loafing, "pad-

adfa, p. 1, 2011.

ded" timesheets, or speeding in company vehicles. However, does the employee have a reasonable expectation of privacy in relation to their employer whether at work or outside work?

This paper provides background on United States (U.S.) laws and court cases, which mostly support the position of the employer, regarding the various methods used for peering into the work lives and private lives of employees in an age of easily accessible information. It also includes a brief overview of the perceptions of intrusion or fairness by employees and their effects on employee motivation and retention. In the future, critical analysis may encourage management to clearly communicate policies to their employees about any monitoring practices which are conducted for the benefit of both the worker and employer.

2 Are Employees Protected from Intrusive Monitoring?

Constitutions, the common law, and statutes all offer some protection of the right to privacy. The U.S. Constitution has been held to provide privacy rights to state and federal government employees [1]. However, the Constitution does not protect the privacy rights of employees of private corporations. This lack of protection also extends to the employment-at-will doctrine, held by most states in the U.S., which allows an employer to terminate the employment of an employee at any time, without notice, although many cases have been challenged [2].

Title I of the 1986 Electronic Communications Privacy Act (ECPA) makes it a punishable offense for any intentional interception or attempted interception, use or attempted use of any device to intercept, disclose or attempt to disclose to any other persons, use or attempted use of contents of information from wire, oral, or electronic communications obtained in violation of the ECPA [1]. This act prohibited employers from reading workers' e-mails, but allowed the reading of e-mails if employees were notified in advance; some workers may even sign waivers to allow both internet and e-mail monitoring.

Title II of the 1986 ECPA is the Stored Communications Act (SCA) which prohibits access to stored communications by unauthorized persons [1], such as employees intentionally gaining access to private work files or records. This act also indicates that an employer should not view an employee's private e-mail account even if the account was accessed via a work computer or server. However, this is where the

interpretation of the law can become very muddled. Examples of cases exist where the employer has been determined to have the right of access.

3 Reasonable Expectation of Privacy

There is a reasonable expectation of privacy on the part of employees; however as long as any monitoring is deemed to serve a legitimate business purpose most employers' secret monitorings have been upheld [1].

In a U.S. Supreme Court case, the *City of Ontario, California v. Quon,* a public employee and union member, police officer Jeff Quon, did not have his Fourth Amendment claim to a reasonable expectation of privacy upheld when his excessive use of text messages was investigated. In 456 text messages sent during the month of August 2002, for example, only 57 were work-related and all the others were for personal use. It was found that the employer's search of the text messages was reasonable [3].

In June 2013, a U.S. District Court in Ohio rejected the dismissal of an employee. The court allowed Sandi Lazette to continue with claims that the supervisor of her former employer, Verizon, violated the Stored Communications Act (SCA) by accessing, without consent, her personal mails on a company-issued Blackberry phone[4, 5]. Only accessing unopened e-mails, not already opened ones, was considered a violation. This case, which was settled in August 2013, indicates the critical need for policies to be clearly understood by employees. The SCA, now 25 years old, can be considered to be outdated with regard to today's technology, and so it can be hard to interpret [4].

4 ICT Monitoring

The American Management Association (AMA) and the ePolicy Institute conducted a survey of 304 companies regarding the use of ICT monitoring. The employment population of the businesses, professional services, manufacturers, public administration and other companies surveyed was: 100 or fewer workers (27%), 101–500 employees (27%), 501–1,000 (12%), 1,001–2,500 (12%), 2,501–5,000 (10%) and 5,001 or

more (12%). Of these organizations, 54% of which were of small and medium size, 73% monitored e-mails, and 66% monitored Internet connections [6]. This monitoring, that can include phones, requires a two-party consent in only 12 states [7]. In 38 states, the second party of a conversation does not need to be aware of the interceptions of electronic communications being listened to and/or recorded [7].

Other forms of ICT monitoring, besides the use of phone monitoring, are also feasible. Examples include webcams and video surveillance, GPS and radio frequency identification (RFID), and the monitoring of social media use [6, 8, 9].

Webcams and Video Surveillance: Another aspect of ICT surveillance involves the use of video monitoring to watch employees and customers in order to counter theft and violence. In the AMA [6] survey, 48% of companies used this type of surveillance to monitor for theft and violence, and 7% used video surveillance of workers' job performance (of which 89% of workers were notified by employers). Therefore, 11% of employees are unaware that their place of employment practices ICT surveillance and may be recording their activities.

GPS and RFID: Another type of monitoring and location tracking of equipment or workers is accomplished with global positioning systems (GPS) and radio frequency identification (RFID). The equipment used can include vehicles, smartcards, laptops and cell phones [8]. To supervise mobile workers and encourage productivity, GPS is used to assist in reducing fuel costs and preventing accidents by monitoring vehicle speed. It can also be used to verify overtime claims, and check if a driver was texting while driving [9]. Only 8% of organizations from the AMA [6] survey, noted that they used GPS to track company vehicles; 3% used it for cell phones; and fewer than 1% for employee ID/Smartcards[1].

As with the other monitoring systems, there are little to no guidelines for businesses regarding any restriction in the use of GPS tracking. The Location Privacy Protection Act of 2001 that was intended to regulate the use of GPS was proposed in Congress but was not passed [9]. There are other pending forms of legislation such as the Location Privacy Act - S1233, that would require authorization from the tracked person to be tracked [10]. There are some state restrictions, such as in Texas and

[1] The majority (52%) of companies use smart card technology to control physical security and access to buildings and data centers (AMA, 2008).

California, where one must get owner consent for tracking but not consent for tracking company-owned vehicles [9].

GPS usage for tracking has been questioned and brought to the courts. For example, in the *State of Minnesota v. Bad* [11] a hidden GPS aided in the conviction of burglaries that Bad tried to have reversed but was denied. In *Elgin v. St. Louis Coca-Cola Bottling Company* [12], company trucks used by employees both on- and off-duty had tracking devices. Elgin sued, among other points, for intrusion of seclusion. The company won as the van was its own vehicle and the GPS revealed public information of its location.

Although it may seem to be an action of extreme apprehension, the states of California, North Dakota and Wisconsin have already passed laws that prohibit employers from requiring employees to have RFID implants. However, ingesting is not covered by these laws nor is voluntary implantation for financial gain. Only five states require disclosure/restriction of RFIDs [7].

Social Media: Linda Eagle, a former employee and co-founder of EdComm, in Pennsylvania, was misrepresented by the organization in social media. Eagle sued EdComm in *Eagle v. Morgan* (Morgan was the new CEO) under the 1986 Computer Fraud and Abuse Act (CFAA) the Lanham Act[2], and several Pennsylvania laws [13] for unlawfully taking over her LinkedIn account. Eagle's credentials were replaced with those of Sandi Morgan, although Eagle's honors and awards were listed [13]. The CFAA and Lanham claims were dismissed and EdComm was found guilty of unauthorized use of name, invasion of privacy by misappropriation of identity and misappropriation of publicity [13], however the company was not ordered to pay damages to it former employee.

There have also been cases of employees fired by organizations for their social media activities that have included criticisms of either supervisors or the workplace. Two Domino's Pizza workers were fired after a YouTube video was posted showing the young men preparing sandwiches and one putting mucus on food and cheese in his nose [14]. A newspaper employee was legally fired due to sending inappropriate tweets posted to the employer-related Twitter account. The National

[2] Enacted by Congress in 1946 15 U.S.C. §§ 1051 *et seq., governs* trademarks, service marks and unfair competition.

Labor Relations Board (NLRB) noted the behavior was not protected or concerted[3]. However, some cases have been settled or reversed when the NLRB filed for unfair labor practices [15].

5 Dismissals and Exceptions

Some reasonable cause dismissals, based on the use of ICT methods, have been reported. According to the AMA [6] survey, 6% of employers have terminated workers for the misuse of office phones, and 28% have fired employees because of e-mail misuse which had included: violation of policies (64%), offensive/inappropriate language (62%), excessive personal use (26%), breach of confidentiality rules (22%), and other (12%). For Internet misuse, the major reason that 30% of supervisors terminated their workers' employment was for viewing, downloading or uploading inappropriate/offensive content (84%). Further violations included breaches of company policy (48%), excessive personal use (34%) and other causes (9%) [6].

Business Extension Exceptions: These exceptions are considered when activities that are monitored or recorded are not personal. In general, when monitoring a call, if it becomes clear it is a personal call, the monitoring should stop [16, 17].

Consent Exception: As noted earlier, these laws vary on a state-by-state basis regarding what constitutes consent. Some states require both parties to consent to monitoring while other states only require a one party consent [7]. It can be a tangled web of legalities. Salomon Smith Barney (SSB) a brokerage firm with offices in the states of Georgia and California surreptitiously recorded clients' calls from California to the Georgia office on a regular basis. When California clients became aware of the practice (California is a two consent state and Georgia is a one consent state), they filed a class action lawsuit. The court and an appeal to the intermediate appellate court found in favor of SSB. The California Supreme Court reversed the decision based on its consent statutes but did not award any monetary damages. However, the case put companies on notice that they must inform workers of telephone

[3] 'the right to act together to try to improve their pay and working conditions, with or without a union' (NLRB, http://www.nlrb.gov/rights-we-protect/protected-concerted-activity)

recording activities, so as to offer employees some level of protection [16, 17].

6 Benefits of ICT Monitoring to Organizations and the Outcomes for Employees

Monitoring technologies have long been seen as beneficial to improve services such as the tracking of packages and for allowing customers to follow the transit process. Business process optimization has also aided a company to reduce wrongful travel and entertainment expenses by 80% through continuous monitoring of employees' spending [18]. Another productivity example is how the plumbing and drain service company, Roto Rooter, had a 20% increase in customers served by tracking employees' completed site visits to assign them to the nearest scheduled customer [9]. It can be reasoned that organizations have the right to undertake technological monitoring, considering the benefits and profits to be gained from it [19].

Employer ICT surveillance may claim to be a cost-effective business option, but what about the privacy and the morale of the employee? This kind of intrusion, even if transparent, could have a negative effect on productivity. It could reduce productivity instead of raise it, lower morale and cause stress that can affect employee health [20, 21]. Some research supports employees' personal web use as a better way to balance work and family life and give employees methods to relax and meet social/psychological needs [22]. Restrictions on this use could be counterproductive. Even if it is known that an employer may monitor activities, the monitoring could reduce creativity with concerns for stifled and programmed output [23]. Additionally, "anxiety over how one is perceived by others diverts attention resources away from on-task processes to the detriment of learning and performance" [24:651].

7 Conclusion and Recommendations

Organizations depend on the productivity of their employees. Most organizations also depend on their web presence to do business. In fact, almost every U.S. government agency uses some form of social media, such as Facebook, Twitter and YouTube [25]. Employees with access

to social media sites could expect restrictions on their social media use. In businesses, there may also be monitoring of employee activities and tracking of property. But clear policies should exist so that employees understand their allowances and restrictions; this level of clarity could reduce any litigation against organizations. Courts usually decide these types of suits on a case-by-case basis. The general trend is in support of the organization for the tracking of its own property, with or without notification to employees. But it is for the mutual benefit of the organization and the employee to have enforceable policies that give guidelines on workplace expectations and any non-permissible activities [26]. This should include transparent understanding and distinctions of any real-time or archival monitoring [24].

Appropriate changes to U.S. law need to be formulated. A reasonable recommendation, from a study by law professor Ariana Levinson, is for a federal statute that would:

> cover more types of monitoring than the ECPA and would establish baseline protections for employees' basic right to privacy. It would also benefit employers because it would likely provide more consistent guidance across different jurisdictions and provide more selection of available safeguards for employees' basic right to privacy that employers could choose among in order to comply with the law [16:529].

Other clarifications should be made regarding the SCA although Levinson [16] does not think any of these will be enacted in the near future "even with calls from major companies, civil rights groups, and scholars for privacy legislation" (16:530). Employees should be given clear policies in plain language, notified of any monitoring before hire, and receive a warning on any system that is used [7].

In Europe, where current laws more strongly protect employees (for example, Data Protection Privacy Act, Data Protection Working Party and the European Convention on Human Rights), it is still advised that there should be clear and transparent policies for employees to understand what can be monitored [27]. European Union directives do not allow covert monitorings, or only with rare exceptions, so that employees are afforded much more consideration and ethical treatment [28]. This legislation is currently being revised, and so – in the future – its orientation may differ. Comparison of the legislation and regulations in the two continents of the U.S. and Europe could prove useful, particularly when the implications of international commerce and trade are

considered. Wider considerations of regulations introduced in emerging economies around the globe are also likely to be of importance in terms of the growing complexity of the international legal theatre.

Employers need to notify employees of ICT monitoring through comprehensible policies and practices that are consistently enforced [29]. Regulations and policies will need to be continually updated to include new methods of employee monitoring. With the increasing introduction and usage of bring your own device (BYOD) policies as a business necessity, organizations and workers will both need clear outlines regarding what devices can be used and what equipment can be tracked. If not, both parties may distrust each other in terms of ICT monitoring– the worker for any monitoring of personal files, and the organization for security of company data [30, 31].

Whether working from an office or home, using personal or company equipment, employees should be notified of any system of monitoring. Monitoring systems should only be used for business purposes. Even if there are no U.S. national or state policies available or yet passed, various ethical and moral concerns should be taken into consideration.

Future studies on satisfaction and productivity may identify employees' tolerance and acceptance of systematic ICT surveillance as it is proposed that more transparent ICT policies could aid in the retention and attraction of employees.

References

1. Determann, L, & Sprague, R. (2011). Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States; *Berkeley Technology Law Journal, 26*(979), 979-1036. Retrieved from http://btlj.org/data/articles/26_2/0979_1036_Determann_112111%20Web.pdf
2. Roehling, M. V. (2003). The employment at-will doctrine: Second level ethical issues and analysis. *Journal of Business Ethics*, *47*(2), 115-124.
3. Abril, P. S., Levin, A., & Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal, 49*(1), 63-124. doi: 10.1111/j.1744-1714.2011.01127
4. Coe, E. (October 10, 2013). Verizon case warns employers against vague device policies. Law360. Retrieved from http://www.mrllp.com/images/presscoverages/2013l10.10.13lLaw360lVerizonCaseWarnsEmployersAgainstVagueDevicePolicieslLaraShortz.pdf
5. DiPietro, B. (August 19, 2013). Lawsuit could sway use of employer-provided devices. *Wall Street Journal: Risk and Compliance Report.* Retrieved from

http://blogs.wsj.com/riskandcompliance/2013/08/19/lawsuit-could-sway-use-of-employer-provided-devices/

6. AMA-American Management Association/ePolicy Institute (2008). 2007 electronic monitoring & surveillance survey, AMA/ePolicy institute research. Retrieved from http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf
7. Ciocchetti, C. A. (2011). The eavesdropping employer: A twenty-first century framework for employee monitoring. *American Business Law Journal, 48*(2), 285-369. doi: 10.1111/j.1744-1714.2011.01116
8. Herbert, W. A. & Tuminaro, A. K. (2008). Symposium, Emerging technology and employee privacy: The impact of emerging technologies in the workplace: Who's watching the man (who's watching me)? *Hofstra Labor & Employment Law Journal, 25,* 355-370. Retrieved from http://law.hofstra.edu/pdf/Academics/Journals/LaborAndEmploymentLawJournal/labor_vol25no2_Herbert.pdf
9. Towns, D. & Cobb, L. (2012). Notes on: Gps technology; employee monitoring enters a new era. *Labor Law Journal, 63*(3):203-208. Available from: Business Abstracts with Full Text (H.W. Wilson), Ipswich, MA.
10. Geolocation Privacy Legislation (April, 2013). Official U.S. Government Information on GPS and Related Topics. Retrieved from http://www.gps.gov/policy/legislation/gps-act/
11. *State of Minnesota v. Bad* (2012) retrieved from Legal.com http://www.leagle.com/decision/In%20MNCO%2020120117177.
12. *Elgin v. St. Louis Coca-Cola Bottling Company* (2005). Retrieved from http://www.morganbrown.com/legal/legal_update.php?id=210.
13. Francis, V., Johnson II, T., & Ericsson, K. (2013). Social Media and Employee Monitoring: New Lessons for Employers. *Employee Relations Law Journal*, *39*(2), 59-70.
14. Clifford, S. (April 16, 2009). Video prank at Domino's taints brand. *N.Y. Times, B1*.
15. Alaniz, R. (March 13, 2012). When employees rant online - the NLRB weighs in on workers' rights. *Accounting Web.* Retrieved from http://www.accountingweb.com/topic/social-networking/when-employees-rant-online-nlrb-weighs-workers-rights.
16. Levinson, A. R., (2012). Toward a cohesive interpretation of the electronic communications privacy act for the electronic monitoring of employees. *West Virginia Law Review, 114,* 461-530: University of Louisville School of Law Legal Studies Research Paper Series No. 2011-06. Available at SSRN: http://ssrn.com/abstract=1798822 or http://dx.doi.org/10.2139/ssrn.1798822.
17. Sanders, D. E., Ross, J. K., & Pattison, P. (2013). Electronic snoops, spies, and supervisory surveillance in the workplace. *Southern Law Journal*, *23*(1), 1-27.
18. Cangemi, M. P. (2012). The real benefits of continuous monitoring: as a new foundation technology, CM can go beyond current approaches to improve operations and profits and increase cash flows. *Financial Executive - financiaexecutives.org*. Retrieved from September 2013. http://www.thefreelibrary.com/The real benefits of continuous monitoring: as a new foundation...-a0290522153.
19. Connolly, R., & McParland, C. (2012). Dataveillance: Employee Monitoring & Information Privacy Concerns in the Workplace. *Journal of Information Technology Research (JITR), 5*(2), 31-45. doi:10.4018/jitr.2012040103.
20. Ambrose, M. L., Adler, G.S. & Noel, T. W. (1998). Electronic performance monitoring: A consideration of rights. 61-80. In *Managerial Ethics: Moral Management of People and Processes*. Schminke, M. ed. Psychology Press, N.Y.

21. Lane III, F. S. (2003). *The naked employee: How technology is compromising workplace privacy*. AMACOM, division of American Management Association. NY, NY.
22. Anandarajan, M., Simmer, C. A., & D'Ovidio, R. (2011). Exploring the underlying structure of personal web usage in the workplace. *Cyberpsychology, Behavior, and Social Networking, 14*(10), 577-583.
23. Martin, K., & Freeman, R. (2003). Some Problems with Employee Monitoring. *Journal of Business Ethics*, *43*(4), 353-361.
24. Watson, A. M., Thompson, L. F., Rudolph, J. V., Whelan, T. J., Behrend, T. S., & Gissel, A. L. (2013). When big brother is watching: Goal orientation shapes reactions to electronic monitoring during online training. *Journal of Applied Psychology, 98*(4), 642-657. doi: 10.1037/a0032002.
25. Government Accountability Office (2011). Federal agencies need policies and procedures for managing and protecting information they access and disseminate. Retrieved from http://www.gao.gov/products/GAO-11-605.
26. Mika, K. (2012). The benefit of adopting comprehensive standards of monitoring employee technology use in the workplace. *Cornell HR Review, 38*, 1-6. Retrieved from Cornell University, ILR School site: http://digitalcommons.ilr.cornell.edu/chrr/38.
27. Lugaresi, N. (2010). Electronic privacy in the workplace: Transparency and responsibility. *International Review of Law, Companies & Technology, 24I(2), 163-173.*
28. Lasprogata, G., King, N. J. & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, *4*. http://stlr.stanford.edu/STLR/Article/04_STLR_4.
29. Huth, C. L. (2013). The insider threat and employee privacy: An overview of recent case law *Computer Law & Security Review, 29*(4), 368-381. http://dx.doi.org/10.1016/j.clsr.2013.05.014.
30. Crossler, R. E., Long, J. H., Loraas, T. M. & Trinkle, B. S. (2014) Understanding Compliance with BYOD (Bring Your Own Device) Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems* In Press. doi: http://dx.doi.org/10.2308/isys-50704.
31. Seigneur, J., Kölndorfer, P., Busch, M. & Hochleitner, C. (2013). A survey of trust and risk metrics for a byod mobile worker world. The Third International Conference on Social Eco-Informatics. Lisbon, Portugal. www.thinkmind.org/.