J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 3(2) 101-111, 1994-95

# COMMENT: ACTIVE IDENTIFICATION BADGES, PRIVACY IN THE WORKPLACE, AND A *CHIP* ON THE OLD BLOCK: OPENING PANDORA'S BOX

**BRUCE A. GRABOW**
*Widener University School of Law*
*Harrisburg, Pennsylvania*

**ABSTRACT**

Workplace privacy litigation has blossomed in recent years. The list of intrusive areas has grown so much that there is no shortage of work for the labor law attorney. New technology has developed an "active badge system" that has the potential to be the greatest threat to employee privacy to date. If active badges become commonplace, then new heights of litigation can be expected. This article explores the privacy implications that active badges may impose.

## PRIVACY IN THE WORKPLACE

"Historically, the employment relationship has limited an employee's ability to challenge an employer's unfair, adverse, or damaging practices" [1]. The impact of unions, regulation through the National Labor Relations Act and the Fair Labor Standards Act [2], and oversight by the National Labor Relations Board have helped to turn around this one-sided relationship. From this combination, the employer–employee relationship, and "employee privacy law" [3], in general, have developed dramatically in the past few decades [4].

Today, privacy in the workplace encompasses a wide range of topics including hiring practices [5], "health and safety" issues [6], "searches, . . . union meeting surveillance, . . . employee manipulation, . . . literature solicitation and distribution, jury or witness duty, voting time, whistle-blowing, dress codes and grooming, spousal policies, nepotism, third-party representation, performance evaluations, name changes, . . . religious accommodation, privacy misconduct, language requirements," [1, § 1.6] and privacy outside the workplace. As one can guess





doi: 10.2190/ARFJ-Q8QF-4VTU-NWCY
http://baywood.com

from this foreboding list, preserving employee privacy in the workplace is an everchanging challenge.

## PRIVACY AND INFORMATION GATHERING

Information gathering and information disclosure is another area of workplace privacy that has been well-litigated [1, § 1.12-1.14]. Employers consistently look for ways to "know more about the individuals they employ" [7]. As a result, this has "eroded the employee's sense that his or her life is a private matter" [7]. The recent onslaught of technological innovations has not helped. Polygraph testing, medical examinations, computer and phone call monitoring, and video surveillance are examples of technology serving the employer's need to pry into the affairs of employees.

Recent technology has developed yet another device that threatens employee privacy: active badge systems. This article explains what an active badge system is, why it was developed, and why it has the potential to impede upon the very heart of employee privacy movement into the workplace.

## WHAT IS AN ACTIVE BADGE SYSTEM AND WHAT ARE ITS BENEFITS?

### Initial Development

Researchers at the Olivetti Research Laboratory in Cambridge, England have developed an "active badge system" that may be used in the workplace. The system is an infrared tracking system "that allows a computer network to silently keep tabs on [an employee's] whereabouts" [8]. The employee wears the normal identification badge, but included is a chip that "every 15 seconds transmits [by infrared impulses] a 48-bit word, which is the wearer's unique ID" [9], to wall sensors located throughout the building. "Th[is] ID information is [, in turn] held on a central database . . ." [9]. In effect, an active badge enables an employer and certain fellow employees to locate another employee and to monitor the employee's activity.

To the average employee, an active badge system may send signals of fear. "My boss will now be able to completely monitor my every moment! How fearful. How degrading. How outrageous. Hey, is this legal? Is this really necessary? What about my privacy rights?" Such statements are reasonably expected. In newspaper and magazine articles written about "active badge systems," privacy concerns have been raised [8, 9, 10]. However, because these badges can serve a tremendous business function and are only being utilized by a select level of executives and researchers, such privacy dangers are not yet seen as an imposing threat. Yet, the potential for privacy invasion does exist.

## Benefits and Current Use of Active Badges

The name of the complete interactive communications system developed by Olivetti Research Laboratory in Cambridge, England, in conjunction with Digital, is called Pandora. Pandora works interactively with active badge systems. Consider the following description.

> The Pandora multimedia system consists of a group of networked, Unix-based workstations that provide real-time and recorded digital audiovisual information for users. Primary applications . . . include desktop videoconferencing and video mail.
>
> A pandora system . . . contains a video camera, a microphone, a loudspeaker and the Pandora processor box
> . . . .
>
> . . . .
>
> The simplest use of Pandora is just observation. The staff at Olivetti Research can view remote offices through video cameras mounted over each Pandora station. Although it's perfectly permissible to peek at the scene surveyed by another Pandora station, a user can't listen to that station until someone at that end lets him—i.e., accepts the call.
>
> In addition, if a staff member surveys another office, the user in that office will always get an image of the surveyor on the screen. In this way, no one can observe without being observed [9].

Initial testing of Pandora and in particular, active badges, has focused on convenience. Developers of the active badge are marketing it as "the office of tomorrow" [9], and rightfully so. The active badge will literally enable the office to follow an employee throughout the work building. For example:

- telephone calls will automatically be routed to the phone nearest to the last recorded location. No longer will a secretary have to say, "He's in, but I'm not sure where he is." Further, for the executive that does not want to be bothered, "a button can be pushed on the badge to tell the system the wearer is busy" [11].
- urgent communications through electronic, voice or video mail will "be sent to the nearest terminal and its arrival announced by a beep from [the] badge" [9].
- a computer terminal will automatically log-off when the employee leaves, and as the employee enters another room, another computer terminal will automatically log-on to a predetermined program—thus his work will follow him [8, 9, 11].

- "shared computer printers can be told to give priority to requests from those actually in the building" [11].
- when three or more "badges" are at the same location, a meeting will be presumed and no interruption will be allowed. Of course, there is a priority feature that allows certain calls to always be received [11].
- secured doors will open automatically when approached [8, 11].

The possibilities for efficiency and flexibility are tremendous.

Many service industries with health and safety concerns are also interested.

- Hospitals will be able to instantly locate emergency personnel [8, 11].
- Hospitals will be able to locate the whereabouts of roaming patients [12].
- Offshore worksites will better be able to monitor a worker's safekeeping [11].
- Badges may even be installed with a "send help" button [8, 11].
- Airports can track objects such as luggage or children [8].

In short, active badges do have very appealing qualities. Those currently using these badges wholeheartedly consent to their use, and quite understandably, "because [they] make[ ] life easier" [9].

## DISCUSSION: PUBLIC POLICY CONCERNS

So long as active badges remain among the limited fields listed above, privacy will not be a concern. But what if active badges become part of the standard uniform for the average employee? Will management have a legitimate business purpose to justify gathering active badge information? What duties might accrue to the employer if such information is gathered? May the employer include the chip on an employee's badge without the employee's knowledge and consent? If the active badge is mandatory, does the employee retain any privacy rights? Questions such as these merely reflect issues at the "tip of the iceberg." As this article demonstrates, engaging an active badge systems will launch a vessel that is destined to crash into an iceberg of serious privacy concerns.

Traditionally, so long as "health or safety considerations regarding personal harm are not present" [12], an employer may legitimately require employees to display identification badges. This is not to say that "[e]mployees have [not] asserted a privacy interest in [such] policies" [13]. But for the most part, wearing badges strictly for identification and security purposes is a settled topic. However, requiring the use of active badges may unsettle this area of employment law. Why? There are two reasons: productivity and information gathering.

## Productivity

What is an employee's right to not be tracked throughout the workplace and to be left alone? Obviously, an employer has a legitimate right to know, to a great degree, the whereabouts of an employee. Is the employee in an unauthorized area? Is the employee remaining in his work area so that the employer's expectations as to timely completion of assigned work can be realized? Such information is very useful to an employer. It helps to promote efficiency and productivity, which in turn may increase profit, and this is the ultimate legitimate business purpose.

But how far may an employer go in knowing an employee's whereabouts, especially to advance only productivity concerns? Are active badges really a necessary means to achieve this productivity information? I suggest not. To this day business has survived and flourished without infrared sensors monitoring employee movements. Productivity has always, and will always, be measured the old-fashioned way: reviewing the finished product. The work itself is the employer's monitoring system. So why the need for an active badge? The only legitimate reason would be to foster *employee* convenience—to facilitate productivity for certain executive and research employees. And, justly, this was the initial reason for their creation. However, if the employer's primary reason for an active badge is merely to gather information on employees, there may be illegitimate purposes involved.

## Information Gathering and Hypothetical Misuse

> Employers collect, maintain, use, and disclose considerable employment information. This information is used to hire, discipline, terminate, place, transfer, promote, demote, train, compensate, and provide full or partial fringe benefits. It may be collected or disclosed without employee notice, knowledge, or consent. Employment record privacy and integrity is important for both employees and employers [1, § 7.20].

The critical question becomes, how will an employer use active badge information? Such information may be dangerous and provide a means for serious abuse. As Roy Want, the inventor of active badges, stated, "It's great technology in the right hands . . . . [b]ut if you've got a bad manager, he's going to make your life hell" [14].

Such a statement accurately reflects the potential for abuse. Does management really need to know that an employee left his office for four minutes and thirty-nine seconds? Better yet, is it wise for management to accost its employees with such information? "Employees, after all, don't want to feel like house-arrest convicts whose bracelets trigger alarms when they stray from home . . ." [14]. This is a serious management consideration that must be addressed. Does management want to portray an atmosphere of distrust? Will society actively seek employment

in a business that monitors employee movement with such scrutiny? Usually not. Further, one can only imagine how unions would perceive such an intrusion.

## Promotions and Performance Reviews

Aside from having the potential to scare the employee into productivity, active badges raise other "informational" concerns. Will management now use this information in employee performance evaluations? Further, will promotions be affected? Consider, for example, the situation where two employees are being considered for one management position. Both are equally dedicated and hard working. Management then pulls such employee's active badge file. This file reveals that while both employees stray from their office now and then, one employee strays far more frequently and for longer durations. Moreover, this occurs every day. Yet, this employee's work is superior to that of the other employee. Management begins to speculate:

> His work is superior, yet every day he strays. The file does not record where he usually goes. Maybe this employee frequents the bathroom where there are no sensors to gather information [15]. Maybe this employee has a physical problem that we don't know about. This could cost the business a lot in future insurance coverage and sick leave. Maybe we should promote the other employee; his file doesn't seem to have any areas for such speculation.

Is this fair? Should an employer be able to gain this edge? If an employer is allowed to use this informational edge, then the workplace environment will drastically change. Employees will lose their autonomy and sense of freedom.

Consider another scenario. Suppose information leaks out that management reviews the active badge file weekly and utilizes it when considering promotions. Will not this provide an incentive for employees to defraud employers by simply leaving the active badge at the workstation. The sensors will record the employee securely at work. Yet, the employee is in the breakroom, bathroom, etc.

## Potential Employer Duties

Suppose after reviewing active badge information that management strongly believes an employee has some physical problem. What is management's duty at this point? Is there an affirmative duty to approach the employee and suggest that he see a doctor? What if the employee refuses, is this grounds for termination? Of course, there is the possibility that the employee may appreciate management's concern and hail management as a paternal hero.

Suppose management only makes a note in the employee's file, never affirmatively informs the employee, and subsequently the employee develops a physical ailment. May the employee bring a negligence suit against the employer? After all, the employer was in a good position to predict such an ailment. Suppose further that businesses that use an active badge system acquire an affirmative duty

to inform. One can image the increased costs that will result from such a duty. Employers will want malpractice insurance and, presumably, the insurance industry will be happy to provide it. In turn, employers may be forced to hire active badge "analysts" who can search the files and detect tendencies toward medical ailments. Of course, such waste of business assets could be avoided if management decides not to employ active badges.

Yet, assume that active badge systems do become frequently used, employers do recognize their affirmative duty to inform, and employees are on notice that management will provide this service for them. If an employer decides not to employ an active badge system, will this not send a message that management doesn't really care for its employees like the business down the street does? Guess who may lose employees! To take the scenario just one more hypothetical step further, if a business decides not to employ an active badge system while the rest of the industry does, will insurance companies raise that business's rates?

We must be mindful that such an affirmative duty may accrue in other situations as well: offshore worksites monitoring the whereabouts of workers [11]; or hospitals tracking roaming patients [12]. If certain business' in these service industries decide not to use active badges, may insurance companies raise rates or even cancel coverage? Finally, consider the tempting opportunity for government agencies to mandate the imposition of active badge systems for certain industries.

Moreover, consider referrals. After an employee either resigns or is terminated, what duty to inform does the employer carry when another business calls for a recommendation? If the employer fails to release the active badge information, may this amount to a cause of action? Suppose the employee is still in employ and the employer releases information to an outside source or even to other employees. Typically, the employer is under an affirmative duty to preserve confidentiality. "Wrongful disclosure of information or maintenance of inaccurate information may result in claims for invasion of privacy . . ." [17]. The employer may breach a duty if such information is released.

Finally, consider these remaining issues:

- Suppose the employer does not inform the employee that an identification badge is actually an active badge. Surely this will amount to an invasion of an employee's legitimate expectation of privacy. The employee has neither consented to nor been put on notice that he is being monitored.
- Will not active badge information provide an end run around the limits currently imposed on hiring inquiries? [1, § 1.1-6.22]
- Regarding the security of active badge information, consider the following comment: "By tapping into the data base from afar, any of the 5 million users of the worldwide Internet computer network—utter strangers, even—can find out [the whereabouts of an employee]" [17].

It should now be obvious to the reader that the imposition of an active badge system may easily upset employment relations as they exist today. However, at the risk of beating a dead horse, there still remain other problems that must be addressed.

## Social Concerns

To many employees, the workplace is an environment of bonding, a second family, where relationships are formed. An employer's use of active badge information could have a devastating effect on these social ties. Employees may stop visiting with each other for fear that the data being amassed may hinder job security. In addition, development of workplace social skills may be stunted. Moreover, what about the employee who has no family and relies on his/her fellow employees for stability and guidance? Is s/he to be left out in the cold (somewhere on the "tip of the iceberg")?

Admittedly, the workplace exists for work and productivity, but a by-product of attending work is social development. If this is stifled, especially in the case of the nonfamily employee, society may indirectly suffer. Society may lose future leaders. Society may bear the financial cost of supporting those who, because of such stifling activity, sink to depression and possibly even suicide. This, of course, is mere speculation, but these ideas are not too farfetched. Thus, management must recognize these potential social costs when it decides whether active badges are necessary.

## Where Will the Line Be Drawn?

Although each of these considerations is important, one must realistically ask, if society accepts active badges, where will the line be drawn? What is next?

- A microphone on the badge? What possible legitimate business concern could management advance? Surely, forcing all conversation to be work-related is not legitimate. Further, what if the employee is not informed that the microphone is attached, will it matter? Eavesdropping may also be thrown to the wayside [18]. Private and unmonitored conversation will no longer be treasured.
- What about tracking employee movement and relations outside the workplace? In the home? Will the employer now have the right to invade the most hallowed of personal and private locations? [19] Suppose such access to information enables the employer to determine that the employee is a lesbian, or has different religious habits. Such information might unduly influence the employer's future treatment of an employee [20]. Is society prepared to allow this?
- And for the kicker, why not let management insert a "chip" in the employee's arm. In this way, employee autonomy will be completely eradicated.

Sound ridiculous? Sound frightening? It should. Yet, as I hope this list of hypothetical considerations demonstrates, mandating the use of active badges in the work environment is a ridiculous and frightening idea. If management is allowed to embark on such a course, choppy waters are in the forecast.

### Recommendations

In sum, from this pervasive viewpoint, active badges have the potential to invade every phase of employment privacy interest: "(1) speech; (2) beliefs; (3) information; (4) association; and (5) lifestyle" [1, § 1.5]. The solution is simple: keep active badges where they belong—with the high tech executives and researchers. Leave the rest of the workforce alone. Because employees are already watched with management's eagle eye, any hopeful enhancement in productivity will be minuscule at best. So why open "Pandora's box"? [21]

One note for the record. If society does accept active badges as a legitimate "productivity" interest, only "current" information should be stored. As one commentator suggested, only the "last five 'sittings' of each individual" should be temporarily retained [8]. After they are reviewed and gleaned for their productivity value, management should erase and discard the information. After all, if the whole idea is to know of an employee's current whereabouts, once the information is old, who needs it? Having access to historical information is only asking for trouble.

## CONCLUSION

Business' primary goal is profit achieved through efficient productivity. Thus, management has a legitimate right to monitor productivity. Now management has a tool to track an employee's whereabouts through the use of an active badge system. As a tool to enhance productivity, certainly knowing employee whereabouts has appeal. To date, however, management has monitored productivity quite successfully without the use of active badges. Other than use among high tech executives and researchers, and members of certain service industries, active badges gain little for management. Yet, active badges offer tremendous opportunities for privacy exploitation, not only from an undue invasion into employee movement, but through information gathering. If society still values privacy in the workplace, an active badge system should remain simply a high-tech toy for the executive. If business is allowed to shackle employees with an active badge, a myriad of employment battles awaits management, and without a doubt, employees will make a "federal case" out of it.

* * *

Bruce Grabow received his J. D. from Widener University School Law in 1994, Magna Cum Laude. He served as Editor-in-Chief of *Widener Journal of Public Law* (1993-94) and also as Editor of *Harvard Journal of Law & Public Policy* (1993).

## END NOTES

1. K. H. Decker, Employee Privacy Law and Practice § 1.2 (1987) (citing H. Perritt, Jr., Employee Dismissal Law and Practice ch. 1 (2d ed. John Wiley & Sons, New York, 1987) ).
2. 29 U.S.C. § 1 *et seq.*
3. Taken from the title of an extremely comprehensive employment law treatise by Kurt H. Decker [1]. "[P]rivacy is the most rapidly evolving employment law area." [1, § 1.4].
4. The very notion of a privacy right, in general, is credited to the "*Harvard Law Review*'s 1890 article by Samuel D. Warren and Louis D. Brandeis." [1, § 1.3 (citing 4 Harv. L. Rev. 193 (1890))]. "Warren and Brandeis preferred the phrase 'right to privacy'; however, 'right *of* privacy' has become the generally accepted expression used by the legislatures and courts in privacy matters." [1, n. 45].
5. "Hiring privacy alone can affect an employee through advertisements, applications, interviews, credit checks, arrest records, criminal convictions, fingerprints, photographs, immigration requirements, reference checks, medical screening, genetic screening, blood testing, skill testing, polygraph examinations, honesty testing, handwriting analysis, negligent hiring and so forth." [1, § 1.6 (footnotes omitted)].
6. Health and safety issues range from "smoking, employee assistance programs, alcohol and drug abuse, acquired immune deficiency syndrome (AIDS), [and] sterilization. . . ." [1, § 1.6 (footnotes omitted)]
7. [1, § 1.4] (citing Cook, *Invasion of Privacy: 1984 Syndrome*, 28 *Indus. Mgmt.* 18, No. 5 Sept./Oct. 1986).
8. M. Johnson, Wherever You Go, They Will Follow, *Computerworld*, p. 19, July 15, 1991.
9. A. Hopper, The Walk-and-Wear Office, *Computerworld*, p. 99, Apr. 20, 1992. "[Mr.] Hopper is the director of the Olivetti Research Laboratory in Cambridge England." [9].
10. M. May, Playing Tag in the Office, *The Times, p. 26,* Mar. 6, 1992; P. Coy, Big Brother, Pinned to Your Chest, *Business Week*, p. 38, Aug. 17, 1992; B. Metcalfe, More on Active Badges and Fears about Loss of Privacy, *InfoWorld*, p. 51, July 6, 1992.
11. May [10]; *See Coy* [10].
12. Decker [1, § 7.32 (citing Briggs & Stratton Corp., 77 Lab Arb. (BNA) 233 (1981) (Mueller, Arb.)]; M. Hill, Jr. & A. Sinicropi, Management Rights, Bureau of National Affairs, Inc., pp. 157-159, Washington, D.C., 1986.
13. [1, (citing Michigan Consolidated Gas Co., 53 Lat. Arb. (BNA) 525 (1969) (Keefe, Arb.) for the proposition that badges may cause "adverse reactions on the peace-of-mind, personal security and family privacy of at least certain individuals, thereby

subjecting them to unjustifiable and avoidance hardship and inconvenience—if not personal hazard." [1, § n. 828].

14. Coy [10].
15. One commentator noted that to the happy sigh of employees, there are no plans to put infrared sensors in the toilet. Thus, bathroom habits may remain secured information. *See* B. Metcalfe, More on Active Badges and Fears about Loss of Privacy, *InfoWorld,* p. 51, July 6, 1992.
16. [1, § 7.30]. Moreover, the employer may be liable under a variety of tort theories. "Invasion of privacy"—when a "broad public disclosure of private facts occurs." *See also* [1, § 4.3] citing Restatement (Second) of Torts § 652D comment a (1977); *Bratt v. International Business Machines,* 467 N.E.2d 126 (Mass. 1984) (disclosure of employee medical records); *contra Eddy v. Brown,* 715 P.2d (Okla. Sup. Ct. 1986) (no privacy invasion for disclosure of employee psychiatrist problems). "Defamation"—*see* [1, § 7.30] citing *Wendler v. DePaul,* 499 A.2d 1101 (Pa. Super. 1985) (negative employee performance evaluation); [1, § 4.4]. "Intentional infliction of emotional distress"—[1, § 7.30] citing [1, § 4.6]. "Negligent maintenance or disclosure of employment records"—*see* [1, § 7.30] citing [1, § 4.7]; *Quinones v. United States,* 492 F.2d 1269 (3d Cir. 1974) (release of inaccurate personnel file); *Bulkin v. Western Kraft East, Inc.,* 422 F. Supp. 437 (E.D. Pa. 1976) (negligent maintenance of employment records).
17. Coy [10]. However, as one commentator has stated, "[At least] all users have access to information on who is monitoring their whereabouts because inquiry information is logged and recorded." Hopper [9].
18. *See* The Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520.
19. Employers already have the capability of knowing location outside the workplace through cellular phone systems "since they must pin down the approximate location of every customer to deliver incoming calls via the closest antenna." Coy [10].
20. Comment made by Professor Kurt H. Decker, Labor Law: Employee's Rights, class discussion on April 26, 1993. [1, § 1.16].
21. This reference to Pandora's box is rather apropos. *See* discussion above about the Olivetti/Digital Pandora System. Perhaps, now we can speculate why it is called Pandora's box. Consider the possibilities. Although there are safeguards against unsolicited and unannounced surveillances, this does not mean that management will not obviate this. The technology is in place. Pandora is invading the workplace. Employees of the business world, be on your toes.

Direct reprint requests to:

Bruce A. Grabow
Widener University School of Law
Harrisburg, PA 17111