IUSLabor 1/2007

BIG EMPLOYER: *"A study of the continuously decreasing expectation of privacy of employees in the US workplace"*

Manuel Martinez-Herrera
LL.M. Harvard Law School
Associate at Epstein, Becker & Green

"The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinized."[1]

I. Introduction

Ever since the first version of the "Big Brother" TV reality show[2] was aired in The Netherlands in 1999,[3] the show has originated multiple debates raising several privacy concerns in each of the countries where it has been broadcast. The absolute lack of intimacy and secrecy of the contestants, to which, of course, they had previously voluntarily submitted themselves, raises some fundamental questions among viewers and non-viewers alike, as it seems to attack some of the core values of Western civilizations.

In fact, privacy, in one form or another, is considered a fundamental right in most civilized societies. *"Yet it is clear that intuitive sensibilities about privacy differ from society to society even as between the closely kindred societies of the United States and continental Europe."*[4]That is to say, although privacy is viewed as an important value on both sides of the Atlantic, its construction and interpretation differs from one continent to the other, as *"privacy does not have a universal value that is the same across all contexts."*[5]

Indeed, it has been traditionally thought that the concept of privacy in the US derives from the idea of liberty,[6] and especially from the conception of an individual's home as his/her castle, *"where the individual enjoyed a freedom from government intrusion."*[7] [8] It is at home where US citizens feel that they can have an absolute *"reasonable expectation of privacy,"* which is the judicial test used to determine the existence of a possible violation of this fundamental value. However, as they cross their entrance door and abandon the *"sanctity of home"*,[9] their expectation of privacy is dramatically reduced. On the other hand, *"The core continental [European] privacy rights are rights to one's image, name and reputation."*[10], which are rights that citizens

[1] George Orwell, *1984*, 3 (1950).
[2] Surely this was not the result that George Orwell was aiming for when he first published his acclaimed novel "1984" in 1948 and introduced the "Big Brother" concept.
[3] See Endemol's, Big Brother's creator and producer, press release at http://www.endemol.com/Press%20center/default.aspx?fID=7153&rID=30&hl=1999
[4] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 403 (2004).
[5] Daniel J. Solove, *Conceptualizing Privacy*, 90:1087 Cal. L. Rev., 115, 120 (2005).
[6] Whitman, *supra* note 4, at 414.
[7] A great part of this core idea is rooted in the US Constitution, and more specifically in its Third Amendment which states: *"No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law."*
[8] Solove, *supra* note 5, at 164.
[9] See Boyd v. United States, 116 U.S. 616, 630 (1886).
[10] Whitman, *supra* note 4, at 414.

carry with them wherever they go, and whose protection is not only confined to the boundaries of their residence.

This different view of the same value has also affected the way and degree in which employers in the *"Old"* and *"New World"* intrude on the privacy of their employees in the workplace and, in some instances, even outside of it. The purpose of this paper is to show the current state of expectation of privacy for employees in the US workplace by showing the applicable regulation[11] and relevant caselaw regarding the most important issues (i.e., video surveillance, wiretapping, internet monitoring, background checking, drug testing and off-job conduct). This study is also aimed at analyzing the possible future consequences of these intrusive policies in the workplace[12] and to offer viable solutions to improve employees' expectation of privacy.

II. Background Checking

Employers, following some procedural safeguards[13] included in the Federal Credit Report Act ("FCRA"), can request specialized agencies to obtain investigative consumer reports on their applicants or current employees.

These reports may include very extensive information about the employee's or applicant's past and current activities.[14] Moreover, information may be obtained from personal interviews with neighbors, friends, or associates of the employee or applicant.

III. Drug-Testing

"In the 1980s, the federal government's focus on eradicating illegal drug use joined with technological advances making drug testing more affordable and accessible to produce an explosion in workplace drug testing programs (…)."[15] In fact, under federal law, any employer may implement a drug testing program that tests applicants and employees under any of the following circumstances: (i) mandatory testing of all applicants and employees; (ii) random testing of employees; and (iii) reasonable suspicion testing.

A few states, including, among others, California, Connecticut or Montana, have restricted employers' rights to drug test employees. Some states may limit the circumstances in which the tests can be performed, while others may only add requirements with regard to the certification of the laboratories conducting the tests.[16]

IV. Wiretapping

Title II of the Omnibus Crime Control and Safe Streets Act of 1968 proscribes the willful interception of any wire or oral communication. However, there are two widely used basic exceptions that allow employers to wiretap their employees' telephones under certain circumstances:

---

[11] The author wishes to remark that due to the short nature of the project, the study is mostly focused on federal regulations and cannot include all state-based peculiarities and differences.

[12] According to the recent 2005 Electronic Monitoring & Surveillance Survey conducted by the American Management Association, 76% of the surveyed employers were monitoring employees' internet connections, 25% have terminated workers for misusing internet, another 25% have dismissed employees for inappropriate e-mail use, and 6% have fired employees for misusing office telephones.

[13] These safeguards basically consist of a written authorization by the employee or applicant to carry out the report and a written notice including certain information prior to taking any adverse employment action against the applicant or employee. A few states, such as California or Massachusetts, have enacted statutes providing some further safeguards.

[14] The report may include information regarding such intrusive and comprehensive topics as character, general reputation, personal characteristics, mode of living, criminal records, driving records, credit history, reference check, military records, previous employment, educational background, professional licensing, etc.

[15] Crain, Kim & Nolan, *Worklaw: Cases and Materials*, 415 (2005).

[16] Albert L. Vreeland et al., *50 Employment Laws in 50 States*, 4-1, 4-20 (2006).

(i) The consent exception: it is legal to intercept wire or oral communication when one of the parties[17] to the communication has given prior consent to the interception. Consent may be express or implied.[18]

(ii) *"In the ordinary course"* of the interceptor's business exception: In order for this exception to apply two requirements must be fulfilled: *"(1) the intercepting equipment must be obtained from the provider of communication service or furnished by the user for connection to the facility and use in the ordinary course of the user's business, and (2) the interception itself must be in the normal course of the user's business."*[19]

As a result of these two exceptions, most employers are able to wiretap their employees' conversations in the workplace.

V. Video Surveillance

Video surveillance may be a very effective tool for monitoring employee safety, observing employee productivity and training employees by avoiding previous mistakes *"caught on tape."* However, it is also a very intrusive practice that *"can destroy a person's peace of mind, increase her self-consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities."*[20] [21]

US courts generally uphold the use of video surveillance in the workplace, provided it is limited to video images without sound recording. The analysis is, of course, based on the *"reasonable expectation of privacy"* test. As a result, it is not considered offensive to monitor an area *"which is in plain view within an open work area."*[22] Nevertheless, employers are forbidden from monitoring areas where employees have an expectation of privacy, such as restrooms or changing rooms.

Even hidden cameras of which employees had no prior knowledge or notice have been considered legal as long as employees had no *"reasonable expectation of privacy"* in the areas where they were installed.[23]

VI. Internet Monitoring

At the federal level,[24] the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510-2522, technically protects most electronic communications from interception, disclosure, use and unauthorized access. However, the *"Use of computers to monitor employee performance is a natural extension of earlier methods of tracking employees' work"*[25] and the actual limitations for employers on controlling the electronic communications of their employers are scarce. Employers providing their employees with electronic services may not only be free to review and disclose already stored employee electronic communications,[26] but also to monitor such communications after obtaining the consent of the originator or intended recipient of the

[17] Please note that a dozen or so states require the consent of both of the parties involved in the communication.
[18] In George v. Carusone, 849 F. Supp. 159 (D.Conn. 1994), implied consent was found when memoranda had been circulated including the wiretapping policy, certain phones included warnings in this regard and the topic was regularly discussed among the employees.
[19] Matthew W. Fink, *Privacy in the Employment Law*, 263 (2nd ed. 2003).
[20] Solove, *supra* note 5, at 157.
[21] Legal counsel for the defendants in Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997), graphically described this sensation by stating: *"while at work under the cameras' unrelenting eyes they cannot scratch, yawn, or perform any other movement in privacy."*
[22] See Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997).
[23] In Acosta v. Scott Labor LLC, 377 F.Supp. 2d 647, 652 (N.D. Ill. 2005), the court found the video surveillance of an office by a hidden camera to be legal. In Branen v. Kings Local Sch. Bd. Of Educ., 144 Ohio App. 3d 620 (Ohio App. 2001) the use of hidden cameras in a staff break room was also upheld.
[24] A few states (e.g., Connecticut, Illinois) have enacted statutes further restricting employer's ability to monitor electronic communications.
[25] Dennis R. Nolan, *Privacy and Profitability in the Technological Workplace*, 24 J. LAB. RES. 207, 209 (2003).
[26] See 18 U.S.C. § 2702(b).

communication.[27] Such consent does not even have to be express, as many courts will accept implicit consent based on the employee having prior notice of the company's policy.[28]

Moreover, under employment discrimination regulations an employer may be liable under the *"respondeat superior"* doctrine for the creation by one of its employees of a hostile work environment. This hostile work environment may very well be created by one employee sending harassing or racist e-mails to other employees or by displaying inappropriate images or comments on his/her computer screen. Therefore, not only are US employers not discouraged from monitoring the electronic communications of their employees, it even makes good business sense for them to do so to avoid any kind of liability in this type of situations.[29]

VII. Off-job conduct

An Employee's privacy does not recover its full protection once the employee finishes his/her work shift. Even though they are outside of their workplace, employees will not be fully shielded from attacks on their intimacy until they are surrounded by the walls of their *"castle-home."* In fact, many employers have terminated or disciplined employees for actions committed outside of the workplace in the employee's free time. For instance, the University of Alabama terminated its college football coach after it became public that the coach had a party with strippers, and the San Francisco Chronicle fired one of its reporters after he was arrested for participating in protests against the war in Iraq.[30] [31]

Employers take these decisions under the rationale that *"the consequences of the off-duty behavior in some way spill over to the workplace, affecting the employer's legitimate interests."*[32] More than anything employers are trying to protect their reputation and image vis-à-vis their clients, customers and/or investors.

An employee's legal protection in this regard is minimal. The common law privacy tort does not offer an effective defense against employers' decisions based on off-duty conduct. One possible protection is afforded by *"for cause"*[33] provisions.[34] However, these provisions are usually only applicable to unionized or highly qualified employees.

Only a couple of states (i.e., Colorado, North Dakota and New York) have enacted statutes specifically providing protection against employment decisions based on off-duty behavior.[35]

---

[27] See 18 U.S.C. § 2511(3)(b)(ii).

[28] See Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002).

[29] In Blakey v. Cont'l Airlines, Inc., 164 N.J. 38, 751 A.2d 538 (2000), the New Jersey Supreme Court held that derogatory and potentially offensive e-mails posted on an electronic bulleting board provided by the employer could support a hostile environment claim. The court stated that the bulletin board was an extension of the workplace and that employer's duty to prevent harassment also included the e-mail system.

[30] Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24:2 Berkeley J. Emp. & Lab. L., 183, 184 (2003).

[31] Other cases included terminating employees for having extra-marital affairs or dating fellow employees or employees of competitors.

[32] Sugarman, *supra* note 20, at 185.

[33] The traditional rule in the US is that employees are hired under an *"at-will"* employment relationship. Thus, unless there is an agreement to the contrary or a statute limiting an employer's right, either party may terminate the employment relationship at any time with or without cause or notice. However, unionized employees frequently count on the protection of *"for cause"* clauses under their Collective Bargaining Agreements. For cause clauses change the at-will status by defining the specific circumstances under which the employment relationship can be terminated by the employer without liability. Therefore, if the employer decides to terminate the unionized employee for his/her off-duty conduct, such circumstance will more than likely not be included in the for cause definition and the employer will either have to retain the employee or pay the compensation established under the applicable Collective Bargaining Agreement.

[34] Crain, Kim & Nolan, *supra* note 15, at 407.

[35] See COLO.REV.STAT. § 24-34-402.5; N.D. CENT. CODE §§ 14-02.4-03; and N.Y. LAB. LAW § 201-d.

VIII. Conclusion: Searching for the Perfect Employee. Limits and Boundaries.

Let's imagine an average job applicant in the US, whom we will call John Doe. John is an American citizen in search of a job, like many others,. To that end, Mr. Doe applies for a position with a fictitious company named XYZ Corporation. As part of the application process, and even though XYZ Corporation does not have the slightest suspicion or evidence that John may be a drug addict, a criminal or an individual of moral turpitude, John is requested to produce urine and hair samples for drug-testing purposes; XYZ Corporation obtains through an investigative agency a credit report outlining John's financial health, as well as a criminal report; and John's father and mother along with some of John's neighbors, close friends or even high school teachers are interrogated with regard to his reputation and trustworthiness. Luckily or not, John obtains a position with XYZ. However, his privacy expectations are still equally ominous. As an employee, John may have all his calls and electronic communications monitored; his stored e-mails may be reviewed by XYZ and he may constantly be recorded by a visible, or even worse, hidden video camera. If all of the above does not seem enough to destroy any sense of privacy in our imaginary employee, XYZ's tentacles may be able to reach and in some way control and limit John's activities once he abandons the workplace under the pretext that such activities may negatively affect its business interests, and even discipline or terminate him for, let's say, wanting to have some fun in a strippers bar or rallying against the war in Iraq.

Therefore, have not US employers become in a sense that omnipresent "Big Brother" non-blinking eye that symbolizes our most intrinsic fears derived from a book and a TV show based on a complete lack of privacy?

The matter is actually even worse, because at least the contestants of all these new generation reality shows voluntarily agreed to be fully monitored and controlled, receiving important amounts of money and the possibility of becoming new media icons (with all the economic advantages that such status carries along with it) in exchange for a flagrant violation of their privacy, and the characters in 1984 were only a product of Orwell's marvelous imagination. On the other hand, employees have to accept these practices from their employers, in some cases without even giving their express consent,[36] in order to perform their jobs and earn a living for their families.

We could also argue that employees also voluntarily accept to work for employers that carry out these practices and that they could choose to work for other types of employers with a higher sense of respect for their privacy. The argument has already been made that the market might be able to find a solution to this dilemma.[37] As more and more employees leave what we can call privacy-invader[38] companies, the argument goes, to join privacy-respecter ones, privacy-invaders will be forced to change their policies in order to retain their more talented employees and avoid going out of business.[39]

In my opinion, this argument, although somewhat appealing at a first glance, suffers from an irreparable flaw. Companies are much stronger than individuals, even more so in countries like the US where Unions' bargaining power is continuously decreasing.[40] What would happen if all companies, or at least a majority of them, decide to be privacy-invader type companies? Following the proposed market rationale, this decision would not be illogical as it would seem like it makes more business sense to have complete control over your

[36] See Sections IV, V and VI for practices that do not require the express consent of the employee.
[37] Sugarman, *supra* note 30 , at 234-235.
[38] The term is not technically correct as these companies are not doing anything illegal under the law as it currently stands. However, it does reflect the perception that such companies do not attach great value to the privacy rights of their employees.
[39] Sugarman, *supra* note 30, at 234-235.
[40] In the 1950's 35.7% of private employees were unionized. Fifty years afterwards less than 10% of private employees are union members. See Robert P. Hunter, *Michigan Labor Law: What Every Citizen Should Know*, 53 (1999).

employees as you might be able to reduce some economic liabilities.[41] As a natural consequence, there would not be enough job positions in the few privacy-respecter companies for all employees who value their intimacy. Therefore, employees would be left without a real market choice, as they would have to choose between their privacy and their survival.

As a result, it seems like employers have initiated a race in search of the perfect corporate employee by forcing and expanding to never before imagined maximums the degree of intrusion and control over their employees' privacy. The perfect corporate employee will not loose time on personal calls or making appointments with doctors or talking with his wife, husband or the teacher of his/her sons, will not surf the web to read the sports magazine or look for adult material, will not send jokes either through the corporate e-mail or through his/her personal e-mail accounts (access to which will be prohibited during work hours), will always have the business's interests in mind when taking any decision or carrying out any activity outside of his/her working schedule, and the list goes on and on. More than human beings, it seems like what corporations are nowadays looking for are robots.

But where are the limits on this perfect employee search? As explained, the current trend shows how companies want to obtain as much information about applicants as possible before making a hiring decision in order to reduce any exposure to economic liabilities to the maximum degree possible. Employers may even want to know if in the future their employees will be predisposed to developing certain illnesses such as Alzheimer's, cystic fibrosis, anemia or Huntington's disease[42] [43], to name a few. With such information employers would be able to only employ workers with a bright health future to assure that they will be able to remain for a long time in the company and consequently reduce their health insurance burdens, training and hiring costs. This is not a chimera, as genetic testing makes it possible to obtain this and much more in-depth information.

However, numerous states have already enacted state laws prohibiting employers from requiring prospective employees to take genetic tests as an employment pre-requisite and from discriminating against employees based upon their genetic predisposition.[44] These regulations have stopped the pretensions of many companies that were already planning to implement such drastic measures and have shown the path that, in my opinion, needs to be followed in order to return privacy to the American employee.

Taking into consideration the above explained damaging effects for employees and perverse incentives for employers of a non-privacy-regulated market, and the current trend among companies focused on obtaining increasing amounts of information about their applicants and employees, it seems like a unified body of legislation enacted at federal level establishing the foundations, basic protections and employers' limitations with regard to employees' privacy rights is the easiest, most effective and less burdensome solution to stop, or at least reduce, the continuously decreasing expectation of privacy in the US workplace.

It is a fact that nowadays human beings spend most of their time at the workplace. Many citizens leave their home early in the morning only to return late at night after a long day of work. Therefore, many of our daily interpersonal relationships take place in our jobs where people make new acquaintances, friends and even find

---

[41] Employers can make their employees be more productive and effective as they will not lose time on internet or private calls; employers would not be exposed to negative consequences from their employees' off-duty behavior; employers would not hire potentially dangerous or untrustworthy applicants, etc.

[42] *"Huntington's disease (HD) results from genetically programmed degeneration of brain cells, called neurons, in certain areas of the brain. This degeneration causes uncontrolled movements, loss of intellectual faculties, and emotional disturbance. HD is a familial disease, passed from parent to child through a mutation in the normal gene."* See the National Institute of Neurological Disorders and Stroke Huntington's Disease Information Page at http://www.ninds.nih.gov/disorders/huntington/huntington.htm

[43] Rowe, Russell-Einhorn & Weinstein, *New Issues in Testing the Work Force: Genetic Diseases*, 38 Labor Law Journal 518 (1987).

[44] See N.Y. Exec Law § 296 ("New York Human Rights Law") for New York; see also N.J.S.A. 10:5-12 for New Jersey; see also M.G.L.A. 111 § 70G for Massachusetts; and see also M.S.A. § 181.974 for Minnesota.

new romantic companions. All these relationships, basic pillars of our society, become much harder without a decent sense of privacy.

As the worldwide reputed Harvard Law School Constitutional Law professor Charles Fried long ago masterfully explained it: *"To respect, love, trust, feel affection for others and regard ourselves as the objects of love, trust and affections is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion."*[45] Therefore, if we do not want to "*suffocate*" our employees, that is to say most of our population, something, in the form of new legislation, needs to be done. This new legislation will not only benefit employees, as companies will also be better off with employees that can interact, work and evolve as true human beings.

ISSN: 1699-2938

[45] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477-478 (1968).