Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy
Author(s): Adam D. Moore
Source: *Business Ethics Quarterly*, Vol. 10, No. 3 (Jul., 2000), pp. 697-709
Published by: Cambridge University Press
Stable URL: http://www.jstor.org/stable/3857899
Accessed: 06-01-2016 06:01 UTC

EMPLOYEE MONITORING AND COMPUTER TECHNOLOGY: EVALUATIVE SURVEILLANCE V. PRIVACY

Adam D. Moore

Abstract: In this article I address the tension between evaluative surveillance and privacy against the backdrop of the current explosion of information technology. More specifically, and after a brief analysis of privacy rights, I argue that knowledge of the different kinds of surveillance used at any given company should be made explicit to the employees. Moreover, there will be certain kinds of evaluative monitoring that violate privacy rights and should not be used in most cases.

Too many employers practice a credo of "In God we trust, others we monitor."
Marlene Piturro, "Electronic Monitoring"[1]

Introduction

Few would deny the profound impact, both positive and negative, that computers and digital technology are having in the modern workplace. Some of the benefits include safer working conditions, increased productivity, and better communication between employees, clients, and companies. The downside of this revolution can be tedious working conditions and the loss of privacy and autonomy. In the workplace there is a basic tension between surveillance technology and privacy. Companies want to monitor employees and reward effort, intelligence, productivity, and success while eliminating laziness, stupidity, theft, and failure. The market demands no less of most businesses. But against this pressure stands the individual within the walls of privacy—walls that protect against invasions into private domains.

Jeremy Bentham once envisioned a prison workhouse that placed overseers in a central tower with glass-walled cells and mirrors placed so that inmates could never know if they were being watched.[2] The idea was that "universal transparency" would keep the prisoners on their best behavior. Recent developments in surveillance technology are promising to turn the workplace into the modern equivalent of Bentham's workhouse. There are now computer programs that allow employers to monitor and record the number of keystrokes per minute an employee completes. Employee badges may allow the recording of movements and time spent at different locations while working. There is now the possibility of monitoring voice mail, e-mail, and phone logs—all without the

©2000. *Business Ethics Quarterly,* Volume 10, Issue 3. ISSN 1052-150X. pp. 697-709

knowledge or consent of those being watched. There are even global positioning systems that allow companies to track employee movements cross-country. While employers have always sought to monitor employees it is arguably the case that digital technology has changed the game, so to speak. We may wonder, in a networked world, when this kind of surveillance technology will be used to monitor all of us? And not by just governments, although this Orwellian nightmare will be possible, but by our employers.

In this article I will address the tension between evaluative surveillance and privacy against the backdrop of the current explosion of information technology. More specifically, and after a brief analysis and justification of privacy rights, I will argue that knowledge of the different kinds of surveillance used at any given company should be made explicit to the employees. Moreover, there will be certain kinds of evaluative monitoring that violate privacy rights and should not be used in most cases. As we shall see, certain jobs may warrant a smaller domain of privacy. We should not conclude, however, that the arguments used in these cases are easily generalized.

Privacy

Privacy may be understood as that state where others do not have access to you or to information about you.[3] I hasten to note that there are degrees of privacy. There are our own private thoughts that are never disclosed to anyone, as well as information we share with loved ones. Furthermore, there is information that we share with mere acquaintances and the general public. These privacy relations with others can be pictured "in terms of a series of 'zones' or 'regions' . . . leading to a 'core self.'"[4] Thus, secrets shared with a loved one can still be considered private, even though they have been disclosed.

In an important article dealing with privacy, morality, and the law, William Parent offers the following definition of privacy.

> *Privacy is the condition of not having undocumented personal knowledge about one possessed by others.* A person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him. Documented information is information that is found in the public record or is publicly available (e.g. information found in newspapers, court proceedings, and other official documents open to public inspection).[5]

The problem with this definition is that it leaves the notion of privacy dependent upon what a society or culture takes as documentation and what information is available via the public record. Parent acts as if undocumented information is private while documented information is not, and this is the end of the matter. But surely the secret shared between lovers is private in one sense and not in another. To take another case, consider someone walking in a public park. There is almost no limit to the kinds of information that can be acquired from this public display. One's image, height, weight, eye color, approximate age, and general physical abilities are all readily available. Moreover, biological matter

will also be left in the public domain—strands of hair and the like may be left behind. Since this matter, and the information contained within, is publicly available it would seem that all of one's genetic profile is not private information.

Furthermore, what is publicly available information is dependent upon technology. Telescopes, listening devices, heat imaging sensors, and the like open up what most would consider private domains for public consumption. What we are worried about is what should be considered a "private affair"—something that is no one else's business. Parent's conception of privacy is not sensitive to these concerns.

A right to privacy can be understood as a right to control access to oneself. It is a right to limit public access to the "core self"—and this includes personal information that one never discloses—and to information that one discloses only to family and friends. For example, suppose that I wear a glove because I am ashamed of a scar on my hand. If you were to snatch the glove away you would not only be violating my right to property—alas, the glove is mine to control—you would also violate my right to privacy; a right to restrict access to information about the scar on my hand. Similarly, if you were to focus your x-ray camera on my hand, take a picture of the scar through the glove, and then publish the photograph widely, you would violate a right to privacy.[6]

Having said something about what a right to privacy is we may ask how such rights are justified. A promising line of argument combines notions of autonomy and respect for persons. A central and guiding principle of Western liberal democracies is that individuals, within certain limits, may set and pursue their own life goals and projects. Rights to privacy erect a moral boundary that allows individuals the moral space to order their lives as they see fit.[7] Privacy protects us from the prying eyes and ears of governments, corporations, and neighbors. Within the walls of privacy we may experiment with new ways of living that may not be accepted by the majority. Privacy, autonomy, and sovereignty, it would seem, come bundled together.

A second but related line of argument rests on the claim that privacy rights stand as a bulwark against governmental oppression and totalitarian regimes. If individuals have rights to control personal information and to limit access to themselves, within certain constraints, then the kinds of oppression that we have witnessed in the twentieth century would be near impossible. Put another way, if oppressive regimes are to consolidate and maintain power, then privacy rights (broadly defined) must be eliminated or severely restricted. If correct, privacy rights would be a core value that limits the forces of oppression.[8]

Arguably any plausible account of human well-being or flourishing will have as a component a strong right to privacy. Controlling who has access to ourselves is an essential part of being a happy and free person. This may be why "peeping Toms" and rapists are held up as moral monsters—they cross a boundary that should never be crossed without consent.

Surely each of us has the right to control our own thoughts, hopes, feelings, and plans, as well as a right to restrict access to information about our lives,

family, and friends. I would argue that what grounds these sentiments is a right to privacy. While complete control of all our personal information is a pipe dream for many of us, simply because the information is already out there and most likely cannot or will not be destroyed, this does not detract from the view of personal information ownership. Through our daily activities we each create and leave digital footprints that others may follow and exploit—and that we do these things does not obviously sanction the gathering and subsequent disclosure of such information by others.

Whatever kind of information we are considering there is a gathering point that individuals have control over. For example, in purchasing a new car and filling out the car loan application, no one would deny we each have the right to demand that such information not be sold to other companies. I would argue that this is true for any disclosed personal information whether it be patient questionnaire information, video rental records, voting information, or employment applications. In agreeing with this view, one first has to agree that individuals have the right to control their own personal information—i.e., binding agreements about controlling information presuppose that one of the parties has the right to control this information.

If I am correct about all of this, then there is a fairly strong presumption in favor of individual privacy rights—even in the workplace. What justifies a photographer taking pictures of me about the house is my consent. Most would agree that absent such consent a serious violation of privacy would have occurred. Consent is also necessary, I will argue, for employee monitoring. But therein lies the problem. Under what conditions does consent or agreement yield the appropriate sort of permission. Alas, the initial bargaining situation must be fair if we are to be morally bound by the outcome.

Privacy in the Workplace

We are now in a position to consider an individual's right to privacy in the context of a working environment where evaluative surveillance is both necessary and desirable. If pay increases, promotion, profit-sharing awards, and incentive pay are to be based on effort, desert, and success, there must be acceptable methods of monitoring employees.

Consider the following case. In January 1990, Alana Shoars, an administrator for the electronic mail system at Epson America Inc., discovered that the company was monitoring the e-mail messages of its employees. She was shown a batch of printouts of employee e-mail messages—messages that she thought were protected through the use of passwords. "I glanced over at some of the printouts, and a lot of warning bells went off in my head. As far as I'd known, as e-mail coordinator, it wasn't possible to do such a thing."[9] Upon criticizing this breach of employee privacy, Ms. Shoars was dismissed from the company for insubordination.[10]

This case represents only the tip of the iceberg with respect to employee monitoring. A survey of companies in *Macworld* concerning electronic monitoring

"reported that 21.6 percent of the 301 participating companies admitted searching employee files, including electronic work files (73.8 percent), e-mail (41.5 percent), network messages (27.7 percent) and voice mail (15.4 percent)."[11] And even more alarming, only 30.8 percent of the companies surveyed gave advance warning of the monitoring activities.[12]

In the most general terms, the case of Alana Shoars and e-mail monitoring highlights the tension between rights to control information and individual privacy in the workplace. What was objectionable with Epson America's monitoring was not their wish to control the information that was found on the company's computer network. The objection is that their employees were not notified of the monitoring or the strict company policy forbidding personal use of the network.

Epson argued that the system was company-owned and therefore any information found in e-mail accounts, private or otherwise, was justifiably available for inspection. Moreover, it could be argued that notification of surveillance was both unnecessary and unwise from a corporate perspective. If each instance of monitoring was known to an employee, then the data collected would be almost worthless. It would be like telling the fakes to start faking.

Thin Consent

Justifying employee monitoring in light of privacy rights begins with what I call thin consent. A first step in justifying a kind of monitoring is employee notification. The consent takes the following form: if your employment is to continue then you must agree to such-and-so kinds of surveillance. This is appropriately called "thin consent" because it is assumed that jobs are hard to find, the employee in question needs the job, etc. Nevertheless, quitting is a viable option. The force of such agreements or contracts is echoed by Ronald Dworkin.

> If a group contracted in advance that disputes amongst them would be settled in a particular way, the fact of that contract would be a powerful argument that such disputes should be settled in that way when they do arise. The contract would be an argument in itself, independent of the force of the reasons that might have led different people to enter the contract. Ordinarily, for example, each of the parties supposes that a contract he signs is in his own interest; but if someone has made a mistake in calculating his self-interest, the fact that he did contract is a strong reason for the fairness of holding him nevertheless to the bargain.[13]

An employee cannot consent, even thinly, to a type of monitoring if it is unknown to her. Given a fairly strong presumption in favor of privacy, thin consent would seem obligatory. Here the employee would be notified of each different type of monitoring. Individual acts of surveillance, however, would not require notification—thus slackers would not be notified to stop slacking.

Moreover, a thin consent policy for each different type of surveillance allows companies and businesses to seize the moral high ground in one important respect. There is no sneaking around riffling through office files, midnight program installations, or hidden backdoor keys into e-mail accounts. All of this up front

and in the open. Part of what makes this kind of employee monitoring distasteful is the deceit involved. Locked voice-mail accounts, e-mail files, and desk drawers present the air of privacy when these domains are anything but private.

In any case it should be clear that thin consent is not enough to justify the array of monitoring systems that are now possible or will soon be possible—not in every case. When jobs are scarce, unemployment high, and government assistance programs swamped, thin consent becomes thin indeed. In these conditions employees will be virtually forced to relinquish privacy because of the severe consequences if they don't. But notice what happens when we slide to the other extreme. Assume a condition of negative unemployment where there are many more jobs than employees and where changing jobs is relatively easy. In circumstances such as these, thin consent has become quite thick. And if employees were to agree to a certain type of monitoring in these favorable conditions most would think it justified.

As we slide from one extreme to the other—from a pro-business environment (lots of workers and few jobs yields low wage overhead) to a pro-employee environment (lots of jobs and few workers yields high employee compensation)—this method of justification becomes more plausible. What begins looking like a necessary condition ends up looking like a sufficient condition. To determine the exact point where thin consent becomes thick enough to bear the justificatory burden required is a difficult matter. The promise of actual consent depends on the circumstances. Minimally, if the conditions favor the employee then it is plausible to maintain that actual consent would be enough to override a presumption in favor of privacy.

Hypothetical Thick Consent

As noted above, thick consent is possible when employment conditions minimize the costs of finding a comparable job for an employee. Put another way, an employee who doesn't have to work, but agrees to anyway, has given the right kind of consent—assuming of course they have been notified of the different types of monitoring that will occur. What justifies a certain type of surveillance is that it would be agreeable to a worker in a pro-employee environment. If thin consent is obtained and the test of hypothetical thick consent is met, then we have reason to think that a strong presumption in favor of privacy has been justifiably surpassed.

We will also have to assume that the hypothetical worker making the choice is modestly interested in maintaining control over private information. If this constructed individual has nothing to hide and a general attitude of openness, then any type of surveillance will pass the test. And if I am correct about the importance of privacy with respect to sovereignty and autonomy, anyone would be interested in retaining such control. Rawls's notion of placing individuals behind a veil of ignorance may be of some service here.[14] If the individual agreeing did not know whether she was a worker, manager, or owner and if we assume

that anyone would be interested in retaining control over private domains, then the correct vantage point for determining binding agreements will have been attained.

The force of hypothetical contracts has been called into question by Dworkin and others—"A hypothetical contract is not simply a pale form of an actual contract; it is no contract at all."[15] Here I agree with Dworkin. The moral bindingness of hypothetical contracts has to do with the reasons for why we would choose to do this or that. Viewing it this way, hypothetical contracts are simply devices that enable us to more clearly understand the reasons, moral or otherwise, for adopting a particular institution or process. Dworkin notes,

> There must be reasons, of course, why I would have agreed if asked in advance, and these may also be reasons why it is fair to enforce these rules against me even if I have not agreed. But my hypothetical consent does not count as a reason, independent of these other reasons, for enforcing the rules against me, as my actual agreement would have.[16]

Thus the test of hypothetical thick consent can be understood as a way of clarifying, and allowing us to arrive at, a position that is fair and sensible. Hereafter, when I talk of hypothetical consent and the moral force of such agreements, be aware that this is simply a tool or device that is notifying us when privacy rights may be justifiably relaxed.

Taking up the Epson case again, we may ask if a policy of e-mail monitoring would satisfy the test of hypothetical thick consent. Here we are to imagine a world where there were numerous jobs like the ones found at Epson and that moving to these other jobs would be relatively easy. Moreover, given that there is no industry-wide interest in monitoring e-mail activity many of these other positions would not include e-mail monitoring. If an employee would not agree under these conditions, then this type of surveillance would fail the test. Had Epson notified its employees of a company e-mail monitoring policy, then those employees who stayed on at Epson would have given thin consent. But we should not rush to judge that such a policy would be automatically justified unless the test of hypothetical thick consent is also met. Meeting this latter test in the Epson case seems unlikely.

I take a virtue of hypothetical thick consent to be that satisfaction is determined by imagining a pro-employee situation and then asking what an employee would do in the face of some kind of surveillance. Some may charge that I am stacking the deck, however. Why not imagine a pro-business situation and then ask what an employee would do. We wouldn't have to do much imagining though, and employee consent in such conditions wouldn't justify anything. Moreover, if I am correct in positing privacy rights for each of us, then the deck is already stacked. There is a presumption in favor of individuals having control over personal information—we have privacy rights. Since employee surveillance may cross into private domains, we must consider under what conditions a privacy right may be given up or relaxed. In relatively few cases is thin consent thick

enough to handle the justificatory burden. Hence, the use of hypothetical thick consent. We are imagining a case where the bargaining situation favors the employee—and if agreement is offered in these conditions, then we have reason to think that the type of surveillance in question is warranted.

I hasten to note that even in a pro-employee environment there would be certain kinds of employee monitoring that would be necessary for any business. Punching a time clock or measuring time spent working, for example, would occur in almost any business or company. Even in a pro-employee market theft would have to be minimized. It is not as if McDonald's would become so desperate for workers that they would leave the register drawers open, allow employees to come and go as they please, and continue to pay wages. The market demands that businesses make a profit or at least break even. Given this, there will be certain kinds of employee monitoring that every business will use.

Moreover, there will be employment-specific monitoring as well. For example, trucking companies will have to monitor driving records and ensure that drivers maintain the appropriate skills needed to operate the big rigs. This kind of surveillance may be required by the market or by legislation of one kind or another. There may be laws that require certain licenses that make businesses liable for noncompliance. Absent laws or other government regulation, market efficiency may require certain kinds of monitoring. An example of the latter may be employee time monitoring. The hypothetical or constructed truck driver, no matter where he goes, will be subject to certain kinds of monitoring. So, even in a pro-employee environment certain kinds of surveillance will be justified—those kinds that are necessary for doing business.

So far I have been pursuing a kind of top-down strategy in presenting certain principles and considering arguments that may be marshaled to support these principles. If I am correct, thin consent will justify certain kinds of monitoring when employment conditions favor the employee. Absent such conditions actually occurring, we can imagine what an employee would choose if she were in a pro-employee environment. If she would agree to a type of monitoring from this vantage point—either because every business in her field will monitor in the way she is considering or she agrees for some other reason (maybe because the new monitoring policy will benefit her in some way)—then the monitoring is permitted. In the next section I will pursue a bottom-up strategy by presenting certain cases and then examining how the proposed model fits with these cases and our intuitions about them.

Test Cases and Illustrations

Let us begin with an easy one first. Suppose that one day an employee is approached by his boss and is informed that the company will be moving to a new building. Excited about the new digs, the employee tours the recently constructed office and is quite dismayed. It seems that management has been reading Bentham's *Panopticon* and the site has been built so that employee cubicles can

be monitored by an overseer who can't himself be seen. The video cameras found in the new office have been placed so that computer screens can be watched as well as facial expressions, body motions, and the like. The employee complains and asks what conceivable purpose such a system could have at an insurance company. Management replies that only someone with something to hide would object and this system of monitoring will allow hard workers to be recognized and fairly compensated.

We may now ask if such a monitoring system is justified in relation to hypothetical thick consent. I think it is clear that an individual who is modestly interested in protecting privacy and in a pro-employee environment would leave, other things being equal, and find similar employment elsewhere. The "other things being equal" exception is important because if management were to double employee salaries then maybe a deal could be made—no privacy at work for lots of cash.[17] Outside of such offers the presumption in favor of privacy rights would not have been surpassed for this type of surveillance.

Before moving on, I would like to briefly address the kinds of replies that were offered for why employees shouldn't oppose this kind of monitoring. First, that an employee should have nothing to hide is irrelevant. It is her private life that is being monitored and so it is up to her to deny access. Whether or not she has something to hide is nobody's business. We all may have perfectly normal bedroom lives and have nothing to hide in this area. Nevertheless, mounting a company video camera and wake-up siren on the bedroom wall cannot in the least bit be supported by such reasons. Employee benefit is equally, and for the same reasons, dubious.

Consider a different case. Suppose in an effort to eliminate "time theft" a company begins using "active badges" that monitor employee movements while at work. These badges are sophisticated enough to monitor time spent in a specific area. So, employees who linger in the break room, arrive late, leave early, and stroll the halls, will be discovered and treated accordingly.

Few would deny that time monitoring is a necessary part of any business. Nevertheless, there will be more and less invasive ways to monitor time. Bentham's *Panopticon* with a time overseer is one of the more invasive methods. Given that there are various less invasive ways to obtain this information about employees, it would seem that a constructed individual interested in maintaining private domains would not agree to this type of surveillance. Thus for most companies such a policy would be unjustified. There may be exceptions however. For example the U.S. Pentagon, Arms R&D departments, and the like, may have to maintain this level of monitoring to ensure secrecy.[18] Monitoring college professors in this way is clearly unjustifiable.

A final case that I would like to discuss deals with remote computer monitoring. The case is provided by John Whalen.

> A recent ad for Norton-Lambert's Close-Up/LAN software package tempted managers to "look in on Sue's computer screen. . . . Sue doesn't even know

> you're there!" . . . these "remote monitoring" capabilities . . . allow network administrators to peek at an employee's screen in real time, scan data files and e-mail at will, tabulate keystroke speed and accuracy, overwrite passwords, and even seize control of a remote workstation. Products like Dynamics Corp.'s Peak and Spy; Microcom Inc.'s LANlord; Novell Inc.'s Net Ware; and Neon Software's NetMinder not only improve communications and productivity, they turn employees' cubicles into covert listening stations.[19]

While this kind of employee monitoring may yield some benefits, the preponderance of the evidence would suggest otherwise. Some studies have shown that these monitoring systems produce fear, resentment, and elevate stress levels.[20] Another study concluded that "the introduction of computerized performance monitoring may result in a workplace that is less satisfying to many employees . . . [and] creates a more competitive environment which may decrease the quality of social relationships."[21]

Putting aside the unsavory consequences we may ask if such monitoring passes either test under consideration. First the test of thin consent would not be passed if the employees being monitored were not notified of such practices. Given the absence of a clear pro-employee environment in most industries that would use such surveillance, even if employees were notified the consent would seem too thin. Moreover, remote computer monitoring would fail the test of hypothetical thick consent for most companies. Individuals who did not know if they were the owner, manager, or employee would not agree to such privacy invasions. The presumption in favor of privacy would thus remain intact.

Conclusion

As noted in the opening, high-tech surveillance is promising to turn the modern workplace into an Orwellian nightmare achieving Bentham's ideal workhouse for prisoners—"universal transparency." And even if such monitoring somehow produced an overall net increase in utility, it would still be unjustifiable. Sometimes the consequences be damned. Not that I think generally good consequences could be had from such surveillance. Arguably, human beings are the most productive and creative in conditions completely opposite from those found in Bentham's *Panopticon*.

In this article I have argued that individuals have rights to privacy that shield us from the prying eyes and ears of neighbors, governments, and corporations—electronic eyes and ears are no more welcome. If we begin with a fairly strong presumption in favor of privacy and test different types of employee monitoring with thin and hypothetical thick consent, many currently used kinds of surveillance will be unjustified. Arguably this consent is necessary and sufficient for overriding or relaxing privacy rights with respect to employee monitoring.[22] We will each spend at least a quarter of our lives and a large part of our most productive years at work. This environment should be constructed to promote creative

and productive activity while maintaining the zones of privacy that we all cherish. Although privacy rights are not absolute, it would seem that in a networked world filled with devices that may be used to capture information about each of us, we should take privacy invasions—whether at home, on a public street, or in the workplace—much more seriously.

Notes

This paper was presented at the APA Pacific Division Meetings (April 5–8, 2000). I would like to thank Nancy Snow, Mark VanHook, Bill Kline, and the other session participants for their comments and suggestions. I would also like to thank Kimberly Moore, Scott Rothwell, and an anonymous reviewer at *Business Ethics Quarterly* for reading and commenting on an earlier draft.

[1]Marlene Piturro, "Electronic Monitoring," *Information Center,* July 1990, p. 31; quoted in Richard Spinello's *Ethical Aspects of Information Technology* (Englewood Cliffs, N.J.: Prentice Hall, 1995), p. 141.

[2]J. Bentham, *Panopticon* (The Inspection House), originally published in 1791.

[3]A longer version of this section appears in my article "Intangible Property: Privacy, Power, and Information Control," *American Philosophical Quarterly* 35 (1998): 365–378. I would thank the editors of APQ for allowing me to present this material here.

[4]Alan Westin, "Privacy in the Modern Democratic State," in *Ethical Issues in the Use of Computers,* ed. D. Johnson and J. Snapper (Belmont, Calif.: Wadsworth, 1985), p. 187.

[5]W. A. Parent, "Privacy, Morality, and the Law," *Philosophy and Public Affairs,* Fall 1983, pp. 269–288; reprinted in *Ethical Issues in the Use of Computers,* ed. D. Johnson and J. Snapper (Belmont, Calif.: Wadsworth, 1985), p. 203 (all page citations refer to the reprint).

[6]Legal scholar William Prosser separated privacy cases into four distinct but related torts.

> *Intrusion*: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. For example, a woman sick in the hospital with a rare disease refuses a reporter's request for a photograph and interview. The reporter photographs her anyway, over her objection.
>
> *Private facts*: Publicizing highly offensive private information about someone that is not of legitimate concern to the public. For example, photographs of an undistinguished and wholly private hardware merchant carrying on an adulterous affair in a hotel room are published in a magazine.
>
> *False light*: Publicizing a highly offensive and false impression of another. For example, a taxi driver's photograph is used to illustrate a newspaper article on cabdrivers who cheat the public when the driver in the photo is not, in fact, a cheat.
>
> *Appropriation*: Using another's name or likeness for some advantage without the other's consent. For example, a photograph of a famous actress is used without her consent to advertise a product.

Dean William Prosser, "Privacy," *California Law Review* 48 (1960): 383, 389, quoted in E. Alderman and C. Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995), pp. 155–56. What binds these seemingly disparate cases under the heading "privacy invasions" is that they each concern personal information control. And while there may be other morally

objectionable facets to these cases—for example the taxi driver case may also be objectionable on grounds of defamation—there is arguably privacy interests at stake as well.

[7]Clinton Rossiter puts the point succinctly:

> Privacy is a special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of the modern society. . . . It seeks to erect an unbreachable wall of dignity and reserve against the entire world. The free man is the private man, the man who still keeps some of his thoughts and judgments entirely to himself, who feels no over-riding compulsion to share everything of value with others, not even those he loves and trusts.

C. Rossiter, *Aspects of Liberty* (Ithaca, N.Y.: Cornell University Press, 1958) quoted in Westin, "Privacy in the Modern Democratic State," p. 188.

[8]For more about privacy rights see E. Hendricks, T. Hayden, and J. Novik, *Your Right to Privacy* (Carbondale: Southern Illinois University Press, 1990); F. Cate, *Privacy in the Information Age* (New York: The Brookings Institution, 1997); B. Givens, *The Privacy Rights Handbook* (New York: Avon Books, 1997); Charles Fried, "Privacy," *Yale Law Journal* 77 (1968): 477; A. Westin and M. Baker, *Databanks in a Free Society* (New York: Quadrangle Press, 1972); J. Rachels, "Why Privacy is Important," *Philosophy and Public Affairs* 4 (Summer 1975): 323–33; and Paul Weiss, *Privacy* (Carbondale: Southern Illinois University Press, 1983).

[9]IDG Communications, Inc., *Infoworld,* October 22, 1990; quoted by Anne Wells Branscomb in *Who Owns Information?* (New York: Basic Books, 1994), p. 92.

[10]Alana Shoars filed a wrongful termination suit. "The lower court agreed with Epson's lawyer that neither state privacy statutes nor federal statutes address confidentiality of E-mail in the workplace and dismissed the case." Branscomb, *Who Owns Information?* p. 93. See *Alana Shoars v. Epson America*, Inc., No. SWC112749 (L.A. Super. Ct. 1990).

[11]Branscomb, *Who Owns Information?* p. 93.

[12]While the courts have ruled that employers cannot monitor their workers' personal calls, the Electronic Communications Privacy Act of 1986 grants bosses a "business-use exception," which allows supervisory and quality-control monitoring. J. Whalen, "You're Not Paranoid: They Really Are Watching You," *Wired Magazine,* March 1995. See also *Briggs v. American Filter Co.*, 704 F.2d 577 (11th. Cir. 1983), *Watkins v. L. M. Berry*, 704 F.2d 579 (11th. Cir. 1983), and Hendricks et al., *Your Right to Privacy*, Part 2.

[13]Ronald Dworkin, *Taking Rights Seriously* (Cambridge: Harvard University Press, 1977); reprinted in *Justice: Alternative Political Perspectives*, 3rd ed., ed. James Sterba (Belmont, Calif.: Wadsworth, 1999), p. 126 (all page references refer to the reprint).

[14]J. Rawls, *A Theory of Justice* (Cambridge: Harvard University Press, 1971), pp. 136–142. The hope is that Rawls's veil of ignorance will serve as a device that ensures impartiality.

[15]Dworkin, *Taking Rights Seriously,* pp. 126–27.

[16]Ibid., p. 127.

[17]Employment agreements grant rights, powers, liberties, and duties to both parties. Thus an employee may trade privacy for some kind of compensation like time off or the opportunity to learn. When tradeoffs such as these have occurred we may take the obligations, generated by the agreement, as prima facie—alas, the agreement may have been brokered in unfair conditions. If I am correct, fairness of conditions and binding agreements that justifiably relax rights are guaranteed when the tests of thin and hypothetical thick consent are passed.

[18]Even in these cases the different types of surveillance used should be made explicit to every employee.

[19]J. Whalen, "You're Not Paranoid: They Really Are Watching You," *Wired Magazine,* March 1995.

[20]Richard Spinello, *Ethical Aspects of Information Technology* (Englewood Cliffs, N.J.: Prentice Hall, 1995), p. 128.

[21]R. H. Irving, C. A. Higgins, and F. R. Safayeni, "Computerized Performance Monitoring Systems: Use and Abuse," *Communications of the ACM,* August 1986, p. 800.

[22]I take consequentialist concerns to be factored into laws or market demands. That is, hypothetical thick consent includes utility maximization arguments for requiring licenses, safety regulations, and the like.