Business and Society Review **106:1** 1–27

Technology and Ethics: Privacy in the Workplace*

LAURA P. HARTMAN

Privacy in the workplace is one of the more troubling personal and professional issues of our time. But privacy cannot be adequately addressed without considering a basic foundation of "ethics." We cannot reach a meaningful normative conclusion about workplace privacy rights and obligations without a fundamental and common understanding of the ethical basis of justice and a thorough understanding of the individual and organizational concerns and motivations.

In this article I discuss the status of privacy in the workplace from a technological as well as a legal perspective. What was once considered an inalienable right has now been reassessed as our society and the business world have grown ever more complex. Traditional ethical analysis offers some guidance on how to evaluate the balance between a worker's right to privacy and an employer's need for information with which to manage the workplace. But guidance is not the same as resolution: as concerns workplace privacy rights, there are many more questions than answers.

I then address the vexing issues of privacy, drawing on ethical theory to advance a means by which to identify the appropriate ethical balance for workplace privacy. My focus is on employee privacy in particular, because this is a critical area where

---

Laura P. Hartman is Assistant Vice President and an Associate Professor of Business Ethics at DePaul University in Chicago. Last year Professor Hartman was Bell Atlantic Visiting Professor in Business Ethics and Information Technology at Bentley College in Waltham, Massachusetts.

*I feel privileged to serve as the Second Annual Bell Atlantic Visiting Professor in Business Ethics and Information Technology. I am honored to serve in a role previously held by one of my most esteemed colleagues, Richard De George, and fortunate to have been invited by one of the colleagues whom I admire most in my field and who has truly served as a guide and mentor to many in our profession, Michael Hoffman. Finally, I am grateful to the Center for Business Ethics here at Bentley, not only for its invitation, but also for its leadership in this field and for the impact that it has had on ethics institutes and practices around the world.

© 2001 Center for Business Ethics at Bentley College. Published by Blackwell Publishers, 350 Main Street, Malden, MA 02148, USA, and 108 Cowley Road, Oxford OX4 1JF, UK.

technological advancement is spurred by our desire for information and the ease of its collection. We must ensure that our ethical analysis remains current with the possibilities created by innovations.

Ethics as "Perception"

Individual views of appropriate bases for assessing the ethical nature of acts and consequences vary widely. For me, the concept of perception is critical for ethical assessment, since perception plays such a paramount role in framing issues. Our ethical decisions are influenced by our own perception of ourselves, by others' perception of our actions, and by our perception of "universal laws." Our final choices are determined by the perception that has the greatest impact or weight at the time.

For example, perhaps you have a certain hat that you love to wear; and it is simply the ugliest hat in the world. But it keeps you warm, and you're just going to wear it. You do not care what anyone thinks. You do not care if people stare at you walking down the block. All you care about is that you are comfortable. *Your* perception is all that matters. This same circumstance might exist for you in connection with an ethical dilemma. Sometimes you believe so strongly in what *you* think that, even if the entire universe believes what you are doing is wrong, you will go ahead and do it because you believe it is right. You are following your own values. It is your particular perception that defines what is ethical.

Now contrast the influence of personal perception to the origin of the second potential influence on our actions: what concerns us may be whether *society* perceives what we are doing is right. Society can be defined as one's mother, colleagues, other family members, even the larger American or global society.

Ethicists often call this the *New York Times* or *CNN* test. Perhaps now we should call it the *Web* test. When reaching a resolution to an ethical dilemma, you might test how you will feel if you saw what you did today all over the Internet tomorrow. The question becomes, would you feel all right if everyone else (in your circle or society) knew about what you did? In fact, you might believe that what you did is absolutely right, but the world (or your mother) does not understand it, misunderstands it, or misperceives it. You can probably imagine scenarios where you know what you are doing is right, but everyone is going to get the wrong impression so

you simply choose not to do it. What matters to you in this decision is what other people think. There are certainly situations where all of us might be subject to that type of influence.

The third scenario is where one's determination of whether something is ethical is based on one's interpretation of some universal rule or rules (such as a religious guidance or the direction of universally held principles). For some people, the question they ask themselves is, What would Buddha or Jesus or some other universalist do in this circumstance? It is the "perception" of that religion, spiritual leader, or other "omniscient" being that is critical to your decision. In the end, you believe that the rule is the word of God, or another being or force, and that is what is going to influence your decision, whether or not society or you independently agree with it.

So your determination of that which is ethical in any one circumstance truly depends on whose opinion is important to you. I will give one example of the importance of perception in decision-making. When I first took my three and a half year old daughter on an airplane, about a year and a half ago, I was concerned about her comfort level since I am no fan of airline takeoffs or landings. I was trying to prepare Emma for the takeoff, so I said, "Emma, the plane is going to run, run, run and then jump in the air, and it's going to jump just like you do, but it's going to stay in the air, and it's going to be okay."

As we take off from the ground, of course, Emma looks out the window and starts getting upset. But she is all upset about something to do with the *ground*, and I couldn't figure out what she meant until I realized that she perceived that *the ground was falling away* rather than the plane flying in the air. She could not see that we were in an airplane that was lifting up into the air. She saw that the ground was falling away; and it never would have occurred to me that she would perceive it that way. Yet that is what upset her to such a great extent.

Now maybe if I had considered how she might perceive the takeoff, I might have addressed it differently. Do you ever go to sleep at night thinking that something you did was just fine, but wake up the next morning with everyone angry at you? Or you hand in a memo to some manager, thinking it is perfectly clear; but she or he hands it back to you later saying, "I don't know what the heck you're talking about here, you've got to be more clear"? You thought

you were so clear. In that regard it may be very helpful to engage in a bit of analysis to try to view things from the perspective of each of those individuals who might be impacted by your decision. I discuss the importance of this type of analysis further.

I do not believe that our ethics are fundamentally different; but often we care about different perspectives. Certain perspectives seem more valid, depending on the circumstances. Addressed this way, it is clear that businesses, in particular, generally care about what their primary stakeholders consider to be ethical because they are perceived to have the greatest impact on the business.

The Impact of Ethics as Perception in Business Decision-Making

There are a number of factors that influence businesses to care about how they are perceived by society. The law persuades us to be ethical using deterrents or punishments. The Federal Sentencing Guidelines prescribe hundreds of millions of dollars in fines or jail time for violations. Businesses are also influenced by pragmatic reasons. The Ethics Resource Center in Washington, D.C., found that firms with written codes of conduct are a better investment than those that do not have written codes. When firms engage in strong decentralization efforts, perhaps ethics is the only thing that creates a consistent link within the firm.

Society is also persuasive in its forms of chastisement or praise (consider the *New York Times* test, mentioned earlier). Consider, as well, the Johnson & Johnson case in connection with the tainted Tylenol containers. That situation arose decades ago; yet I still discuss it in my classes as a laudable way to respond to a situation. Wouldn't you like to believe that decades from now people in your firm will say, "oh, you should always do that the way _____ [input your name] did it in 2000"? Or would you rather that people decades from now say, "do it any way, but never do it the way that _____ did it back in 2000," such as the individual at Ford who recommended that they *not* recall the Ford Pinto?

There are also additional incentives for firms to engage in ethical behavior. First, unethical behavior imposes terrible costs. Nestle continues to feel the backlash resulting from an insensitive marketing campaign for infant formula in developing economies that cost many children their lives. This happened over twenty years

ago; yet I still discuss that case, as well. Texaco has paid out almost $200 million for their failure to pay attention to diversity. Mercury Finance, Genentech, Bausch & Lomb, Microsoft: each of these firms has seen financial turmoil arise from ethical violations that were not originally anticipated.

Our Habitual Business Decision-Making Process

Business decision-making is not all that different from decision-making by reasonably rational individuals. (Of course neither businesses nor people are completely rational.) So now that we have a more clear understanding of ethics and the impact of perception, as well as an awareness of the incentives toward ethical behavior, how do you *do* it? Usually, we make decisions *considering limited alternatives*. I may say to you, what do you do, choice a or choice b? You consider the options, feeling the pressure. You think, "oh my gosh, a or b, a or b . . . I'll take choice a!" But another option exists, does it not? One might say, "wait a minute, I need to think about this. There are other choices that you did not offer me—choices c, d, e, f." But usually, we consider only the limited alternatives.

We use *simplified decision rules*. You must make the choice to terminate someone. You choose to follow a rule of thumb such as firing the last one hired. "I'm sorry, there's nothing I can do." Rules of thumb relieve the decision-maker of the accountability for that decision. It feels better to say, "there is nothing I can do" than to explain that you have all the discretion in the world, but are still firing the person.

Finally, we usually select alternatives that merely *satisfy minimum criteria*. I believe this normal habit is one of the most detrimental of our habitual decision-making practices. If all of us need to reach a compromise on something, we would naturally find a solution on which we all could agree, and then stop. It is often difficult to believe there is a better answer than the first possible solution over which there is no dispute. But, instead, it is seldom that one continues to seek alternative, *better* solutions at this point. Does anyone ever say, "Wait, that might not be the best; let's keep trying"? It does not happen very often. You can imagine that one might miss out on the *best possible* decision instead of the *earliest or easiest* possible decision. This process is how we *usually* make decisions.

The Ethical Process of Decision-Making

What follows is a discussion of the *ethical* process of decision-making. It may appear to be awfully complicated. But let me tell you this: it becomes habitual, so habitual that it becomes *uncomfortable* when you are in circumstances where you cannot conduct an ethical decision-making process.

If you have ever learned how to drive a stick shift car, you will understand the following metaphor. Consider the first time you sat in a stick shift car. You had eighty-five thousand, three hundred and thirteen things to remember. Stick shift driving is pretty complicated. You have to remember when to pop the clutch, when to put in the clutch, when to put the brake or the gas on, what to do with this hand over here, what gear you are in, and so on. You begin to drive and the car dies often, you stall, and you deal with it, and then you learn. However, once you become proficient at stick shift driving, you do not really think about when you have to put in the clutch anymore. I drive a stick shift car and I do not think about putting in the clutch. I do not think about which gear I should be in. I just drive. And, in fact, when I drive an automatic car, my left foot keeps going down to try to push the clutch in! I am uncomfortable driving an automatic car these days.

So, compare these circumstances to the ethical decision-making process. It will be difficult or challenging or burdensome in the beginning; but later it will evolve into a habitual process—a process that, if you do not have the ability to follow it in certain circumstances, you are still pushing that left foot in. You are trying to do it. It is uncomfortable that you cannot.

The ethical decision-making process is as follows:

1. **Issue(s):** Identify the dilemma.
2. **Facts:** Obtain all of the unbiased facts.
3. **Alternatives:** Identify the choices that you have (look not only to a and b, but also to y and z!).
4. **Stakeholders:** Identify those who have an interest. What are their motivations? How much power does each hold over you or your firm?
5. **Impact:** Identify the impact of each alternative on each stakeholder and the stakeholders' resulting impacts on you or your firm.

6. **Additional assistance/theoretical guidance:** Do theories uncover any hidden implications? Do they support one alternative over another?
7. **Action:** Decide how to respond and act.
8. **Monitor:** Monitor outcomes and make adjustments where necessary.

There are a few other questions that business practitioners usually ask themselves that might offer a bit of guidance or direction.

1. How'd I get here in this dilemma in the first place?
2. Is my action legal? Where's the legal line?
3. Am I being fair and honest (is it "just")?
4. Am I acting in line with my personal integrity? The firm's core values? The character traits I endeavor to exhibit?
5. Am I being only self-serving or am I considering others?
6. Will it stand the test of time?
7. Is this a model of "right" behavior?
8. How will I feel afterwards? (Am I proud?)
9. Will someone get the wrong idea?
10. Is my loyalty in the "right" place?
11. Is this something a *leader* should do?
12. *How do I never get here again? What should I have done a while ago to avoid getting to this horrible place?*

The important factor in ethical decision-making is not necessarily arriving at a correct or right decision, but is instead to be conscious of the impact of the decision on one's self and others. It is practically impossible not to be affected by this consciousness in one's decision-making if one follows the process set forth above. The end result is a world of more conscious, considerate decisions rather than those based on rapid-fire, gut-based instincts.

Ethical Decision-Making with Regard to Employee Privacy. Applying this ethical decision-making process to the complicated challenge of employee privacy, one must first identify the issue and understand the dilemma. Then one must obtain all of the facts, identify the variety of alternatives available to both employees and employers, and identify all of the stakeholders. The next step is to attempt

to understand the impact of the different alternatives in terms of workplace monitoring, surveillance, and so forth. Perhaps ethical theories will provide some insight. The issue of whether a fundamental "right" exists in personal autonomy or, conversely, managing the workplace may be illuminated by ethical theories. Finally, one needs to make a recommendation and monitor the outcomes. In the course of my research in this area, I am at the point of making a recommendation. I do not yet have evidence monitoring the outcomes.

ETHICS IN INFORMATION TECHNOLOGY AND WORKPLACE PRIVACY

Ethical Issues Unique to Information Technology

> It appears to me that in ethics the difficulties are mainly due to the attempt to answer questions without first discovering precisely what question it is which you desire to answer.
>
> —George Edward Moore

Information technology provides us with a host of ethical challenges. New technology imposes new implications for the balance of power in the workplace. We now have in-home offices, allowing for greater invasions. Moreover, the line between personal and professional lives has become blurred as workers conduct personal business in the office and professional business at home. The office usually provides faster, cheaper, and easier access to the Internet, while some work must be done at home in order to be completed according to our modern, technologically enhanced pace.

Faculty members, for instance, do not go home and become people other than faculty members. We often conduct work at home such as grading, class preparation, and so on. Similarly, our profession affords us a great deal of autonomy in terms of how we spend our days. We do not punch a clock nor hand in a time sheet. All of my students have my home number. My professional and personal lives are awfully blurred. (Sometimes, I wish they were not so blurred!)

Technology allows employers to ask more of each employee because we are now capable of greater production; we have greater abilities due to technology. We do not seem to know any longer when our work day is over. I used to be a lawyer and the understanding in that profession was, if you can work more hours, you do. This is because you will then be viewed as the preferred colleague. You will be the one who is going to get the plum assignments because you work so darned hard.

Other issues are raised by enhanced technology. For instance, should the technological ability to find something out make it relevant? With new employment testing technology, you can find out all sorts of personal information. Through genetic testing, hair follicle testing, drug testing, and so on, your employer can find out anything it wants to know about you. Should the employer find out the information simply because it can?

In addition, new technology allows for a more faceless communication.[1] If you have to fire someone, it is significantly easier to fire that person by e-mail than to walk into her or his office. In the latter case, you see the individual, desperate, perhaps disappointed, frustrated with the fact that you've worked them so hard and now you are terminating them. It is a lot easier to be nasty when you do not have to look your stakeholders in the face.

Finally, there is research that shows that the excessive exertion of power and authority may lead to what the researchers call a "semi-schizoid response," including insecurity, "disruption of biographical continuity," feelings of being overwhelmed and powerless, and doubts about worthiness. The implication is that if someone questions you too much or takes away too much of your power, the ultimate cost may be your emotional security. Somewhat prophetically, Lawrence Lessig wrote in his bestseller *Code*, "We have been as welcoming and joyous about the net (and other technologies) as the earthlings were of the aliens in 'Independence Day.' But at some point, we too will come to see a potential threat . . . and its extraordinary power for control."

Ethical Issues in the Privacy Arena

Specifically in connection with privacy, ethical issues arise with gathering information, assessing its accuracy, correcting it, and disclosure, as well as the substance of the information itself.

Simply knowing that someone knows personal information about you can feel invasive or violating. For that amorphous reason, privacy is a slightly difficult concept to define. Ethan Catch says it is "the ability to control what others can come to know about you." Why do we care that someone knows our personal information? We can imagine items of personal data that we simply do not want others knowing, whether or not they would actually do something with that information. We do not like people knowing things about us; it comes down to one's ability to be autonomous in controlling one's personal information.

Do you, personally, care about the information others know about you? Would you care if your boss knew of all of your off-work activities? Consider Milton Hershey. Milton Hershey would tour Hershey, Pennsylvania, making note of workers' lawns that were not kept up, or homes that were not maintained. He would even hire private detectives to find out who was throwing trash in Hershey Park. Another business owner, Henry Ford, used to condition wages on workers' good behavior outside the factory. He had a hundred and fifty inspectors in his "sociological department" to keep tabs on workers' hygiene habits and housekeeping. Imagine!

Only recently did OSHA retract a statement that the occupational safety and health standards apply equally to workplaces and personal homes, when you work as a telecommuter. Can you imagine if you had to maintain the same standards of safety in your home that your employer must maintain at the traditional workplace?

Status of New Technology with Regard to Workplace Privacy

A multitude of basic and inexpensive computer monitoring products allow managers to track Web use, to observe downloaded files, to filter sites, to restrict employee access to certain sites, and to know how much time employees spend on various sites. Products include WebSense, Net Access Manager, WebTrack, and Internet Watchdog.

One particular firm, SpyShop.com, claims to service one-third of the *Fortune* 500 firms. This firm sells items such as a truth-telling device that links to a telephone. One can interview a job candidate on the phone and the device identifies those who lie. Another firm,

Omnitracks, sells a satellite that fastens to the top or inside of a truck. The product allows trucking firms to locate trucks at all times. If a driver veers off the highway to get flowers for her or his partner on Valentine's Day, the firm will know what happened.

SpyZone.com sells an executive investigator kit that includes the truth phone and a pocket recording pen. Other outlets sell pinhole lens camera pens and microphones that fit in your pocket. The motto of one firm is "In God we trust. All others we monitor." That firm offers a beeper buster, a computer program that monitors calls placed to beepers within a certain vicinity. A computer screen shows the manager all of the numbers so that he or she can determine whether the employee is being distracted during working hours.

Competing Interests

The predominant question I have sought to answer by my recent research is whether a balance is possible between the employer's interest in managing the workplace and the employees' privacy interest. Do employees even have a right to privacy? If one believes the answer is "no," then the entire issue becomes moot. If the employee does have some, even limited, right to privacy, one must seek to find a balance of interest. I will return to the consideration of "rights" as we apply ethical theories. First, it is helpful to identify the proposed rights in dispute.

The employer has a right to manage the workplace. In more specificity, employers want to manage the workplace so they can place workers in the appropriate positions. They want to ensure compliance with affirmative action and administer workplace benefits. They want to ensure effective or productive performance. They need to know what their workers are doing in their workplace. The employer's perspective is as follows: "I am paying them to be there working. If they are not working, I should know that and either pay them less, or hire different workers." It seems like a relatively understandable concern.

Employees, on the other hand, want to be treated as free, equal, capable, and rational individuals who have the ability to make their own decisions about the way their lives will unfold. They are interested in their own personal development and valued performance (the lack of privacy may prevent "flow"); conducting *some* personal

business at the office; being free from monitoring for performance reasons (wary of increased stress/pressure from monitoring); being free from monitoring for privacy reasons; and in being able to review and to correct misinformation in data collected.

Consider the issue of personal work conducted at the office. I get to work some days at 7:00 A.M. and I do not leave until 7:00 P.M. on some days. Last I heard, many doctors' offices are not open before or after 7:00 in the morning or night. So when is one supposed to call and make an appointment, much less ever go to an appointment, if one is punching the clock with those hours? The employer has to understand that workers must be able to call the doctor and make an appointment. Workers need to be able to conduct *involuntary* personal matters at the office. Now, they might not need to e-mail their mother or chat on the phone with friends. Should workers still have the right to conduct that *voluntary* personal business, as well? Perhaps the resolution lies in the precise definition of voluntary or involuntary business.

THE LAW, NEW TECHNOLOGY, AND WORKPLACE PRIVACY

As dictated by the ethical decision-making process, one must obtain all the unbiased facts before responding to an ethical dilemma. Where new technology impacts the dilemma, the "facts" may be all the more difficult to ascertain since we are not yet completely equipped to obtain the necessary information. For example, some scholars contend that nearly everyone who has a computer (estimated to be about 80% of the people in the workforce in the United States) is subject to some form of information collection, no matter how much we protect ourselves.[2] Another source reports that more than 30 million workers were subject to workplace monitoring last year, up from only 8 million in 1991.[3] We are not yet at a point where we can even determine whether this information is realistic.

We are relatively certain about the ways in which information is collected. As of 1999, two-thirds of mid- to large-sized firms conduct some form of monitoring, whether computer-based monitoring, video monitoring, monitoring of personal investments, or maybe simply monitoring key card access to the building or

parking garage (up from 30% in 1993).[4] Our style of working, even of communicating, has created greater possibilities for monitoring. In connection with e-mail, for instance, over 90 million American workers now send over 2.8 billion e-mail messages per day, an average of 190 e-mails per day per worker.[5] We might not be too concerned about some forms of monitoring, while others might feel it to be particularly invasive.

Federal Legislation

Over 100 bills on privacy protection have been introduced in Congress, but as of this writing only one on the collection of personal information from kids on the Internet has been approved. Also, the White House is only supporting privacy protections related to medical information privacy because they believe that this type of uncertainty will dissolve as firms and employees become more comfortable with the medium.

Constitutional Protections

The Fourth Amendment to the U.S. Constitution protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This protection implies a reasonable expectation of privacy against intrusions *by the State, only*. As this provision of the Constitution does not apply to actions by private sector employers, their employees must rely instead on state-by-state laws and the common law made and accepted in the courts. Similar limitation exists in connection with the First Amendment's protection of personal autonomy and the Fifth Amendment's protection against self-incrimination—each of these only protects the individual from invasions by the State. Currently there is proposed employment-related privacy legislation in several states that would apply to private sector employers, but those states fall in the distinct minority.

What the courts will generally consider in cases involving both the Fourth Amendment and common law privacy protections is (a) whether the employer has a legitimate business interest in obtaining the information and (b) whether the employee has a reasonable expectation of privacy. Several examples of common law

actions by the courts are illustrative of the courts' attempts at creating this balance, but perhaps more significant are the settlements reached by firms concerned about the *prospect* of a judge's decision.

Case Law

In one case, two McDonalds restaurant employees used voicemail to transmit love messages during an affair. They believed that these messages were private since the firm told them that only *they* had the access codes. The franchise owner monitored the voicemail messages and later played messages for the wife of one of the workers. The lovers sued for invasion of privacy. They settled for several million dollars, so we do not yet have any judge's decision in a situation like this.

In another case that never made it to the courts, the Minnesota Attorney General sued several banks for revealing personal information about clients to marketers in exchange for more than $4 million in fees. One bank eventually agreed to pay attorney fees plus $2.5 million to Habitat for Humanity.

As of this writing the law has not yet settled in connection with monitoring or the privacy of obtained information, hence the settlements. However, monitoring does seem justified by several cases where e-mail was later used as evidence to encourage a settlement. Within the past several years several large firms, including R. R. Donnelly, Morgan Stanley, and Citicorp, have found that cases often hinged on e-mail transmissions that people originally thought were deleted. In one case this included an e-mail containing 165 racial, ethnic, and sexual jokes sent to the entire firm. In another, the e-mail included sexual jokes about why beer is better than women. Had the firms enforced stringent policies about the use of e-mail and monitored to enforce these policies, perhaps these e-mails would never have been sent.

The *New York Times* also had some problems. They fired 24 employees at a Virginia payroll processing center for sending "inappropriate and offensive e-mail in violation of corporate policy." The public sector is not immune from similar challenges: The U.S. Navy reported that it had disciplined over 500 employees at a supply depot for sending sexually explicit e-mail. It happens all the time,

and it's continuing to happen. You would think that people would actually learn.

In cases where the courts have been able to address the issue, it seemed at first that notice of monitoring might emerge as the critical factor. Perhaps persuaded by early case law, of the 67% of mid- to large-sized firms that monitor, 84% notify their employees of this activity. Notice might range from a one-line comment in the middle of an employee manual that someone receives on the first day of work to a dialogue box reminding you that e-mail may be monitored that pops up each time you hit the "send" button to transmit an e-mail.

In an early case addressing this topic, the court in *K-mart v. Trotti* held that the search of an employee's company-owned locker was not appropriate where the workers were told to use their own personal lock. The basis for the decision was that the employees were left with the legitimate, reasonable expectation of privacy because they used their own locks. On the other hand, an employer's search of employee lunch buckets was held reasonable by another court only two years earlier.[6]

In a later 1990 case, *Shoars v. Epson*, Epson won a suit filed by an employee who complained about e-mail monitoring.[7] In that case, the court distinguished the practice of *intercepting* an e-mail transmission from *storing and reading* e-mail transmissions once they had been sent, holding that the latter was acceptable. In a 1992 action, Northern Telecom settled a claim brought by employees who were allegedly secretly monitored over a 13-year period. In this case, Telecom agreed to pay $50,000 to individual plaintiffs and $125,000 for attorneys' fees.[8]

Similarly, an employee-plaintiff in a 1995 federal action won a case against his employer where the employer had monitored the worker's telephone for a period of 24 hours in order to determine whether the worker was planning a robbery. The court held that the company had gone too far and had insufficient evidence to support its claims.[9]

One might therefore conclude that, if an employer adequately notifies workers that it will conduct monitoring, it has effectively destroyed any reasonable expectation of privacy on the part of the workers. It would now be *unreasonable* to expect privacy since one is told not to expect it. However, in a case where the alternative extreme was true, where a firm notified workers that it would *not*

monitor, the court did not follow congruent logic. It did not find a reasonable expectation of privacy based on a firm's pledge not to read e-mail.

In this case, *Smyth vs. Pillsbury*, Smyth sued the firm after a manager read his e-mail. At the time, Pillsbury had a policy saying that it would not read e-mail. One might presume that this policy should have created this reasonable expectation of privacy. But, instead, this was the first federal decision to hold that a private sector, at-will employee has no right of privacy in the contents of e-mail sent over the employer's e-mail system. The court held, "We do not find a reasonable expectation of privacy in the contents of e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system, notwithstanding any assurances that such communications would not be intercepted by management."

THE LIMITATIONS OF THE LEGAL SYSTEM: A CALL FOR ETHICS

The law offers little, if any, guidance in this area in connection with workplace monitoring, and technology as a whole. In fact, "the development of our moral systems has not been able to keep pace with technological and medical developments, leaving us prey individually and societally to a host of dangers."[10] And does this not represent our current situation in terms of technological advances? It never occurred to most workers that some of this information was available or that they could be monitored in various ways. When it does not occur to them, they do not adequately protect themselves against it. Failure to completely understand the new technology may prevent people from completely understanding their exposure or potential vulnerability.

In his State of the Union address in January 2000, Clinton said, "Technology has to be carefully directed to assure that its reach does not compromise societal values. We have to safeguard our citizens' privacy."[11] The primary ethical issue for analysis is therefore whether the employee's fundamental right to privacy outweighs the employer's right to administer the workplace according to its desires. If not, is there a way to satisfy both parties? As law does not yet provide the answers, we turn to ethics for guidance.

The strongest, most persuasive, and most consistent guidance in this area is based in a theory called Integrative Social Contracts Theory (ISCT), promulgated by Tom Donaldson and Tom Dunfee, both faculty in Wharton's ethics program. ISCT seeks to differentiate between those values that are fundamental across culture and theory ("hypernorms"[12]) and those values that are culturally specific, determined within moral "free space," and that are not hypernorms. In identifying values as hypernorms, Donaldson and Dunfee propose that one look to the convergence of religious, cultural, and philosophical beliefs around certain core principles.[13] Included as examples of hypernorms are the freedom of speech, the right to personal freedom, the right to physical movement, and informed consent.[14] In fact, individual privacy is at the core of many of these basic, minimal rights and is, arguably, a necessary prerequisite to many of them.[15]

Specifically, ISCT seeks evidence of the widespread recognition of ethical principles that support a hypernorm conclusion, such as:

1. Widespread consensus that the principle is universal;
2. Component of well-known industry standards;
3. Supported by prominent nongovernmental organizations such as the International Labour Organization or Transparency International;
4. Supported by regional government organizations such as the European Union, the OECD, or the Organization of American States;
5. Consistently referred to as a global ethical standard by international media;
6. Known to be consistent with precepts of major religions;
7. Supported by global business organizations such as the International Chamber of Commerce or the Caux Roundtable;
8. Known to be consistent with precepts of major philosophies;
9. Generally supported by a relevant international community of professionals, e.g., accountants or environmental engineers;
10. Known to be consistent with findings concerning universal human values;
11. Supported by the laws of many different countries.[16]

With regard to privacy, a key finding of a recent survey of the status of privacy in fifty countries around the world included the following conclusion:

> Privacy is a fundamental human right recognized in all major international treaties and agreements on human rights. Nearly every country in the world recognizes privacy as a fundamental human right in their constitution, either explicitly or implicitly. Most recently drafted constitutions include specific rights to access and control one's personal information.[17]

Accordingly, it would appear that the value of privacy to civilized society is as great as the value of the various hypernorms to civilized existence. Ultimately, the failure to protect privacy may lead to an inability to protect personal freedom and autonomy.[18]

The application of ISCT, however, has limitations. ISCT does not quantify critical *boundaries* for rights. If employees have a right to privacy based on a hypernorm, how far does it extend and what should happen in a conflict? Does not the employer have certain hypernorm-based rights that might be infringed by the protection of the employees' privacy right? To quantify the boundaries of the universal rights, one must therefore look beyond ISCT to a more fairness-based methodology.

Ethicist John Rawls' theory of distributive economic justice provides fairness-based guidance for quantifying the boundary levels of fundamental rights. Distributive justice is a teleological approach to ethical decision-making that defines *ethical* acts as those that lead to an *equitable* distribution of goods and services. To determine a fair method for distributing goods and services, Rawls suggests that one consider how we would distribute goods and services if we were under a "veil of ignorance" that prevented us from knowing our status in society (i.e., our intelligence, wealth, or appearance). He asks that we consider what rules we would impose on this society if we had no idea whether we would be princes or paupers. Without knowing what role we might play in our society, would we devise a system of constant employee monitoring or complete privacy in all professional and personal endeavors? Rawls contends that those engaged in the exercise would build a cooperative system that was sensitive to the interests of all stakeholders. The reason Rawls believes that such a standard would emerge is that the members of the exercise do not know whether they would be among the employer population or employee population. Actions

consistent with a system devised under a veil of ignorance are deemed ethical because of the inherent fairness of the system.

Rawls' theory of distributive justice does not provide guidance for identifying the categories of fundamental rights. What Rawls does provide is a method for establishing distribution rules that avoid market transgressions of the boundaries of ethical actions.

Conjoining ISCT and Rawlsian methods enables one to identify basic human rights and boundaries, and provides for a reasonable balance between economic and ethical consequences of privacy protection for both employees and employers. ISCT establishes the underlying, or foundational hypernorms within a society, whereas distributive justice offers guidance on the extent of those hypernorms and the means by which to implement them.

Scholars are not in complete agreement as to whether a right to privacy is a hypernorm, though most would agree that some form of personal autonomy must be protected. As mentioned above, evidence of a hypernorm such as freedom from slavery unequivocally supports this conclusion—personal autonomy serves as a cornerstone of this protection. On the other hand, the *quantification* of one's right to privacy, in particular workplace privacy, is better identified using a Rawlsian analysis. A proposal for such a fairness-based balance follows.

The implementation of an Ethical Resolution. Assuming for the purposes of this argument that privacy is a hypernorm, but one that may be limited by the employer's congruent right to managerial autonomy, how should the matter be resolved? I suggest a fairness-based decision based on two values: integrity and accountability.

Integrity, meaning consistency in values, would require that the decision-maker define her or his values, as well as create a prioritization of those values. This effort is often accomplished by a firm's mission statement or statement of values. Then, when faced with a dilemma or conflict between two or more of these values, the decision-maker will have internal as well as external guidance regarding the direction her or his decision should take. Second, no matter which direction is taken, the decision-maker must be accountable to anyone who is impacted by this decision. That would require a consideration of the impact of alternatives on each stakeholder, a balancing of that impact with the personal values

addressed in the first step, and actions that represent the accountability to the stakeholders impacted by the decision.

Applying this process to a firm's response to monitoring and its impact on employee privacy, the firm may obtain guidance from its mission statement or alternative statement of values. Does monitoring satisfy or further the mission or values of the firm? Assuming monitoring satisfies or furthers the values of the firm (since a negative relationship here would end the discussion and resolve the dilemma), the employer must impose monitoring in a manner that is accountable to those affected by the decision to monitor.

To be accountable to the impacted employees, the employer must respect their privacy rights and their right to make informed decisions about their actions. Accordingly, this model would require that the employer should give adequate notice of the intent to monitor, including the form of monitoring, its frequency, and the purpose of the monitoring. In addition, in order to balance the employer's interests with those of the workforce, the employer should offer a means by which the employee can control the monitoring in order to create personal boundaries. In other words, if the employer is randomly monitoring telephone calls, there should be a notification device such as a beep whenever monitoring is taking place *or* the employee should have the ability to block any monitoring during personal calls. This latter option would address an oft-cited challenge to notification: if employees have notice of monitoring, there is no possibility of random performance checks. However, if employees can merely block personal calls, they remain unaware of which *business-related* calls are being monitored.

If it feels wrong, it probably is. Ethicist Gary Marks suggests that we look to a number of questions about monitoring, and he proposes that if you answer "yes" to these questions, your monitoring is more likely to be unethical.

- Does the *collection* of the data involve physical or psychological harm?
- Does the technique cross a personal boundary without permission?
- Could the collection produce invalid results?
- Are you being more intrusive than necessary?

- Is the data subject prohibited from appealing or changing the information recorded?
- Are there negative effects on those beyond the data subject?
- Is the link between the information collected and the goal sought unclear?
- Is the data being used in such a way as to cause a disadvantage to the subject?

As a manager, you are not without additional guidance on these issues. Kevin Conlon, District Counsel for the Communication Workers of America, suggests additional guidelines that may be considered in formulating an accountable process for employee monitoring:

- There should be no monitoring in highly private areas, such as restrooms.
- Monitoring should be limited to the workplace.
- Employees should have full access to any information gathered through monitoring.
- Continuous monitoring should be banned.
- All forms of *secret* monitoring should be banned.
- Advance notice should be given.
- Only information relevant to the job should be collected.
- Monitoring should result in the attainment of some business interest.[19]

Moreover, in its bargaining demands for last year, the Union of the United Auto Workers demanded concessions with regard to monitoring, including:

- Monitoring only under mutual prior agreement.
- No secret monitoring—advance notice required of how, when, and for what purpose employees will be monitored.
- Employees should have access to information gathered through monitoring.
- Strict limitations regarding disclosure of information gained through monitoring.
- Prohibition of discrimination by employers based on off-work activities.

RESOLUTION?

I am emphatic in much of what I have presented here because I passionately believe that there is a balance possible between workers and employers—not simply in the privacy/monitoring debate, but in many of the ethical challenges presented by new technological advances. Ultimately, employees and employers share a common vision with regard to the purpose of work and of the market in general. When the personal interests of both sides are considered, viable alternatives emerge.

Extreme opinions exist. An employer may believe that employees should simply quit if they don't want to be monitored, while certain employees may believe that they should have the ultimate control over their personal communications and other information. Two extremes. Yet, there is an absolute middle. One can absolutely respect the interest of the employee while also protecting the interest of the employer. A monitoring program that is developed according to and guided by the mission of the firm, then implemented in a manner that is accountable to the employees, follows the integrity/accountability approach I explored earlier.

From the employees' perspective, this type of resolution would respect their personal autonomy by providing for personal space, by giving notice of where that space ends, by giving them access to and the right to change or correct the information gathered, and by providing for monitoring that is directed toward the personal development of the employee and not merely to catch wrongdoers.

From the employer's perspective, this balance offers a way to effectively but ethically supervise the work done by their employees. It protects the misuse of resources, while also allowing them to better evaluate their workers and to encourage their workers to be more effective. I contend that any program that fails to satisfy these basic elements has the potential not only for ethical lapses, but also for serious economic problems.

Former vice president and presidential candidate Al Gore, who of course is an appropriate person to quote since he "invented" the Internet, claims that "new technology must not reopen the oldest threats to our basic rights: liberty and privacy. But government should not simply block or regulate all that electronic progress. If we are to move at full speed ahead into the information age, government must do more to protect your rights—in a way that empowers

you more, not less. We need an electronic bill of rights for this electronic age."

CONCLUDING THOUGHTS

Before I conclude, I ask that you consider the following questions not only with regard to information technology and the impact that that technology has on your particular workplace, but also with regard to the ethical issues that arise in other areas of your work. Consider what you might be willing to quit over. What would be so damaging, so intrusive, so much of a violation of your personal space that you would simply quit right then and there? What could be so bad?

Second, and perhaps it seems extreme in this particular circumstance, what would you be willing to give your life for? You may not believe right now that information technology is going to present life-and-death ethical dilemmas, and yet when we consider the ultimate usage of some of that technology, it really does have a life-and-death impact. If you knew that it would have a fatal, negative impact, would you quit if your firm or client failed to ameliorate it? Monitoring probably does not fall within this range, but you can imagine situations where technology does allow such an extreme unethical and certainly illegal act.

The reason why I want to conclude with this query is because this is really the purpose of this article. The world is a better place because you have thought about these questions now, rather than when you are first faced with these challenges in the workplace.

Have you ever had a situation where you act impulsively in the face of some dilemma, and you realize hours later that, if you'd only thought about it, there were other alternatives or there were other ways to look at it? It did not occur to you at the time. The best solution is to consider these situations now, in advance, so that your gut tells you more information when you need to know it. In speaking of inventor Charles Lindbergh, it is said that, "of all the man's accomplishments, and they were very impressive, the most significant is that he spent most of his life considering and weighing the values by which you should live."

If I ask you what your personal mission statement was so that you could actually implement the integrity and then accountability

steps, would you know what it would be right now? Could you recite to me what you think are your critical values? Maybe not, but now is the time to think about them and not when those values are ultimately challenged.

Stanley Milgram conducted an experiment in the 1960s. In that experiment he called in two people. We'll take Megan and Jim. Megan and Jim come into my laboratory at Yale University, and I am wearing a white lab coat. I give to Jim fifty cards that have printed on them fifty pairs of symbols, i.e., a square and a heart, a diamond and a star, etc. Jim has a few minutes to memorize these. "Okay, Megan," the laboratory technician explains, "you are going to come into another room and test Jim. You're going to read off one of these symbols and, if he gets it correct, you'll continue. If he doesn't, you'll shock him with this electric shock machine, and then continue higher and higher voltages each time. It's just a little uncomfortable." Megan says that she understands.

Minutes later, the experiment begins. Jim remembers a few pairs in the beginning, but on the fourth card, he makes a mistake. He gets shocked and Jim says, "ah, that really hurt!" Megan says, "well, sorry." They keep going. They continue through a few more and Jim's saying, "wait a minute. This really hurts. Let me out of here! Let me out of here!" Later we hear, "I have a heart condition! Please let me out of here. This is horrible! I can't bear this any longer!" Megan's asking the experimenter, "what should I do?" The technician responds, "the experiment requires that you continue. You're being paid to participate in the experiment. There is no permanent tissue damage."

Continuing, Megan gets to number forty-eight, and she hears no sound from Jim's chamber. She looks to the technician who informs her that "no response is the same as a negative response." So she swallows, takes a deep breath and she zaps him. Forty-nine, no response. Fifty, no response. She stands up, gets out of the chair and says, "go, go, see if he's okay!"

And, of course, Jim is okay. He's reading from a script. He's not hooked up to a machine. He's part of the experiment. What is being tested is whether Megan will do what she has been told to do by an authority figure in a business or medical environment, against what she believes to be this person's best interest. One can now understand how this might be relevant to ethics and business ethics in particular.

Would you do something you knew was wrong because your boss tells you to do it? Oftentimes people say, "well if I didn't, I'd be fired." Well, so is it worth being fired? Should you do it or not do it? You still have a choice. You have a choice in everything.

In my lecture (the basis for this article) I asked my listeners the following question: "How many of you sitting here this afternoon believe that you might actually continue the whole experiment and go through number fifty?" Probably very few, and certainly significantly fewer than the more than 60% that completed the experiment for Milgram.

Now, the essential question: What is the difference between my listeners and those tested? Are my listeners unique? Well actually yes, because they have read a discussion about ethics and have had the opportunity to consider the issues for a moment. It creates a bit of skepticism. Moreover, they have had the opportunity to observe the ethical dilemma and to have a slightly more objective opinion as to what they might do.

I believe that if you went into a psychological experiment tomorrow in real life, you would still challenge that experiment early in its process. Why? Because you have actually thought about what you might do in that circumstance. You have thought about the power or lack of power that this lab person would have over you. I am hoping that, as we consider ethics more and more on a regular basis, when ethical dilemmas come up, perhaps you will already have considered your response or at least your values with regard to the dilemma.

Simply by virtue of considering a dilemma beforehand, considering how you would act or what is important to you, you are going to make a different decision. The process cannot help but modify how you act. And so that's why I appreciate you caring about and reading about this subject.

NOTES

1. For additional insight in this area (and perhaps foresight, given the original date of publication), see William S. Brown, "Ontological Security, Existential Anxiety and Workplace Privacy," *Journal of Business Ethics* 23: 1 (2000), 61; citing in addition R.D. Laing, *The Divided Self* (New York: Penguin Books, 1965).

2. "More US firms checking email, says AMA," http://www.amanet.org/research/specials/monit.htm.

3. Julie Cook, "Big Brother Goes to Work," *Office Systems* (Aug. 1999), 43–45; John MacIntyre, "Figuratively Speaking," *Across the Board* (Jan. 1999), 17.

4. Ibid.

5. Ibid.

6. *Simpson v. Commonwealth of Pa., Unemployment Compensation Bd. of Review*, 450 A.2d 305 (Pa. Comm. St. 1982), *cert. den'd*, 464 U.S. 822.

7. No. SCW112749 Cal. Sup. Ct., L.A. Cty., 1989, *appeal den'd*, Sup. Ct. Ca., 994 Cal. LEXIS 3670 (6/29/94); James McNair, "When You Use Email at Work, Your Boss May Be Looking In," *Telecom Digest*, http://icg.stwing.upenn.edu/cis500/reading.062.htm, reprinted from *The Miami Herald*.

8. Bureau of National Affairs, "Northern Telecom Settles with CWA on Monitoring," *Individual Employment Rights* (Mar. 10, 1992), 1.

9. Winn Schwartau, "Who Controls Network Usage Anyway?" *Network World* (May 22, 1995), 71.

10. John Haas, "Thinking Ethically About Technology," http://www.nd.edu/~rbarger/haas.ethic.

11. http//www.whitehouse.gov/WH/SOTU00/sotu-text.html (Jan. 27, 2000).

12. Thomas Donaldson and Thomas Dunfee, "Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory," *Academy of Management Review* 19 (1994), 252, 264 (hereinafter "Donaldson and Dunfee") (defining hypernorms as those principles that would limit moral free space, analogizing hypernorms to "hypergoods," "goods sufficiently fundamental as to serve as a source of evaluation and criticism of community-generated norms [within moral free space]." Ibid.).

13. Donaldson and Dunfee, 252, 265.

14. Ibid.

15. Donaldson and Dunfee suggest that one look to international rights documents and statements of human rights for evidence of or support for certain hypernorms (Donaldson and Dunfee, 265–267). Evidence of privacy and data protection as a hypernorm may be found in the Organization for Economic Co-operation and Development's "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" [O.E.C.D. Doc. C(80) 58 final (Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981)], the Council of Europe's "Council of Europe, Convention for the Protection of Individuals with Regard to

Automatic Processing of Personal Data" [Jan. 28, 1981, EUR. T.S. No. 108, *reprinted in* 20 I.L.M. 317 (1981)], or the Commission of the European Community's Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [COM(92)422 final 1992], European Commission Press Release IP/95/822 (7/25/95), "Council Definitively Adopts Directive on Protection of Personal Data." In support of the claim that privacy is either a hypernorm or a prerequisite to fundamental human rights, Charles Fried (*An Anatomy of Values* [n.p., 1970], 142) contends that privacy is necessary to other values such as love and trust.

16. Thomas Donaldson and Thomas Dunfee, *Ties That Bind* (Boston: Harvard University Press, 1999), 60.

17. Global Internet Liberty Campaign, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice," http://www.gilc.org/privacy/survey/exec-summary.html (1998).

18. For a discussion on identifying Donaldson's and Dunfee's Integrative Social Contracts Theory-relevant ethical attitudes and the establishment of hypernorms, see Donaldson and Dunfee, 274–275, 276–277.

19. Kevin Conlon, "Privacy in the Workplace," *Labor Law Journal* (Aug. 1997), 444, 447. See also Organization for Economic Cooperation and Development (OECD), "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," available from the OECD at 202/785-6323.