Chapter III

New Millennium; New Technology; Same Old Right and Wrong

Joseph T. Gilbert
University of Nevada, Las Vegas

What does ethics have to do with computer security in the new millennium? What, for that matter, did it have to do with computer security in the old millennium? To answer these two questions, we will start with a more fundamental question: what is ethics? In the first part of this chapter, we will briefly review ethics as a part of philosophy. We will examine three approaches that have been taken for hundreds of years as humans have tried to decide what is the right way to behave. We will then examine business ethics, which is an applied subset of the more general topic. Finally, we will explore specific issues which currently present themselves as matters of ethical concern in the world of computer security, and provide a framework for analyzing issues which have not yet presented themselves, but will do so at some future date.

Is it ethical to lend a friend a set of discs which contain a $300 program that you have purchased, knowing that he intends to load the program onto his computer before returning the discs? Is it ethical to hack into computer systems, as long as you don't disrupt or corrupt the systems? Is it ethical to monitor the e-mail of your employees? In order to answer these and a host of other questions, it is useful to think about the common element in all these questions: is it ethical?

Ethics is a branch of philosophy. Philosophy is a field of study that has been actively pursued for at least 2,500 years[1]. It concerns itself with basic questions such as these:

— What does it mean to be human?
— What is truth, and how can we know it?
— What is beauty?
— What is the good life for humans?

The last of the above questions is the question which ethics attempts to answer. Philosophy as a method of inquiry does not either admit or deny the validity of sacred texts. Many people throughout history have found their answers to the questions above and to

others like them in religion. Some great philosophers have believed in many gods, some in one, and some in none. All agree that when they are doing philosophy, the appeal to the word of god or to sacred writings is not a valid way of proceeding. Extending this approach, philosophers do not generally accept any appeal to authority as conclusive. Many philosophers have been very much aware of earlier thinkers and writers, but philosophical arguments are not settled by citing authorities. Philosophers begin either with facts from the world around them or with general principles from which they deduce specifics. They generally concern themselves with logic as a basic operating tool, and while they may disagree on some of the rules of logic, they try to reach conclusions based on a coherent and consistent set of logical rules.

Ethics is the branch of philosophy that addresses issues of human action from the perspective of their moral goodness or wrongness. Human actions can also be judged in a number of other ways, including efficiency, effectiveness, technical correctness and others. When Aristotle (1953) asks what is the good for humans, or Jeremy Bentham (Mill and Bentham, 1987) asks whether an act produces the greatest happiness for the greatest number, or John Rawls (1971) asks whether a society distributes benefits and burdens in a just manner, they are asking, as philosophers, about ethics. In this chapter, we will consider the ethical views of some major philosophers in addressing questions about computer security in the new millennium. The problems we will examine are new; the principles we will apply are not. Since intelligent and perceptive people have thought deeply about ethics over a long period, and the writings of some of these thinkers have been read and discussed by many generations of humans seeking answers to ethical questions, we will not ignore this accumulated wisdom. However, in the spirit of philosophy, we will also not accept any of these views as true simply because someone said them.

Adults generally have a set of ethical principles with which they are comfortable. Some of the frequently cited sources of individual ethical codes include parents and teachers, religion, law, and societal customs [2]. James Q. Wilson (1993) has written a thoughtful book in which he argues that some moral sense is common to all humans. Psychologists generally agree that our sense of moral right and wrong is shaped significantly during our childhood years. For many people, religion provides the main source of moral judgments. Almost all religions prescribe that some actions be done (worship God, honor parents) and that some actions be avoided (murder, stealing, lying). People for whom religion plays a significant role often find religion to be not only a source for ideas about moral right and wrong, but a strong motivating force to follow these ideas in action.

Many adults equate law with morality, in the sense that they generally consider legal acts to be moral, and illegal acts to be immoral. This appears to be particularly true in the realm of business. While legal systems throughout the world concern themselves with the same kinds of things as moral systems, there are some major problems with establishing a simple identity between the legal and the moral. In the United States, laws at the federal level are made by senators and congressmen and women. Many people might have second thoughts about having their moral code determined for them by legislators. Laws can change, and for many people the idea that at least some actions are morally right or wrong permanently is important. Again, some actions are illegal in one state or country, but legal in another. The idea that ethics depends on geographical or political boundaries is troubling. Finally, there are particular examples which raise questions about a simple identity between the legal and the ethical. In the United States, there is no law against adultery. Yet, many people think that adultery involves unethical actions. It is technically illegal to drive 46

miles per hour in a 45 mile per hour speed zone, yet few drivers feel that they are doing anything unethical when they exceed the speed limit by one mile per hour.

THREE APPROACHES TO ETHICAL REASONING

How, then, are we to decide what is ethical? Over the long history of philosophy, several different approaches have been proposed and have gained at least some acceptance[3]. We now will examine three of these approaches, and see how they might serve to answer questions about business ethics[4], and more specifically, about computer ethics. The three approaches often provide the same answer regarding the moral or ethical action in a given situation, but they do not always do so. We will first consider rights and duties, since many philosophers feel that, in cases of different answers from different approaches, this one usually trumps the others.

This approach says that the moral act is the one which observes the rights of others, and follows the duties which these rights impose on the actor. If I have a right to my intellectual property, you have a duty not to take that property without compensating me. If workers have a right to privacy, employers have a duty not to violate that right. When using this approach, ethical analysis starts with a question about who has rights in the case under analysis. Such a question can be more complex than it first appears.

The stakeholder view maintains that a variety of individuals or groups have a stake in the outcome of business decisions (Freeman, 1984). Employees, customers, stockholders, regulators, lenders and others can be directly affected by what a business does. When we ask who has rights, the answer might involve many different stakeholders. Investors have a right to expect that a company will be run profitably. Workers have a right to reasonable compensation, and customers to reasonable prices. Profits would increase (delighting investors) if wages were reduced (troubling workers) and prices were raised (troubling customers). Wages could increase (delighting workers) and prices could decrease (delighting customers), but profits might disappear (troubling investors). What, then, can philosophy tell us about rights and their corresponding duties?

Some rights accrue to individuals by the very fact that they are human. The right to life, exhibited through a prohibition of random killing, is recognized in every known society. There are intense differences regarding the issue of what constitutes random killing, but no society grants to members the right to take any one's life any time they feel like it. Most societies recognize a right to property that we have as humans (not just as adults or voters or members of a certain class). Most societies also recognize, perhaps a bit more vaguely, a right to truth-telling which we have as humans. There are a wide variety of exceptions when falsehoods are sometimes justified by some people, but the phrase "pathological liar" describes in clearly negative terms a person who lies indiscriminately.

Individuals have some rights by virtue of their status of citizens. American citizens who are at least 18 years old and are not convicted felons have the right to vote for their representatives in government. Americans have a right to freedom of assembly and speech. Citizens of other countries have other rights. This class of rights is granted by law, and such rights are legally enforceable. As we noted above, there are problems with drawing a simple identity between the legal and the ethical, but legal systems and moral systems deal with many of the same issues, and so it is not surprising that they converge in many matters of concern.

Finally, individuals have some rights by virtue of their position. A policeman may interrogate a person, search them physically and take them into custody under certain circumstances. An accounts payable clerk may be authorized to disburse company funds up to $1,000, but the chief financial officer may be authorized to disburse up to 500,000. Each loses the right to disburse company funds on the day he or she gives up the position involved.

The moral act, using this approach, is not the one that I have a right to carry out, but the one that observes the duty imposed on me by the right(s) of another. We should also note here that, while we have been speaking of moral acts, there can also be a moral duty to refrain from action. If you have a right to your good name, I have a duty to refrain from publishing libelous comments about you. And, as we will see below, if you have a right to control distribution of your intellectual property, I have a duty to reimburse you for my use of it, or to refrain from further distributing it without your approval or recompense.

As we saw above in the discussion of stakeholders, more than one party may have a right in a given situation, and the corresponding duties may be mutually exclusive. Your right to pass by my house unmolested trumps my right to keep an aggressive pit bull dog unrestrained in my front yard. One of the most common conflicts in business is that between the right of the worker to a fair wage and the owner to a reasonable profit. There is not always a one-to-one correspondence, but it is not unusual to find that as wages go up, profits go down. However, the fact that more than one party may have rights in a given situation does not mean that we should simply throw up our hands in despair of reaching any decision about morality.

A second approach to sorting out ethical issues is called utilitarianism. The basic principle involved in this approach is that the moral act is the one that produces the greatest good for the greatest number. This first involves identifying those who will be affected by an act, and then calculating the balance of good and bad consequences of the act. It can sometimes be difficult to identify all those affected by an act. Even if we identify them, it can be difficult to calculate the good and bad effects of an act. Nonetheless, utilitarianism points out an important ethical consideration: whether we like it or intend it or not, our acts do have significant impacts on others. In deciding about the morality of those acts, the consequences on others which ripple out from our actions need to be taken into account.

A third approach to analyzing ethical issues involves *considerations of fairness and justice*. Many people would agree that it is unethical to treat others unfairly. Two kinds of fairness or justice are often identified: procedural and distributive. Procedural justice simply means that people in similar situations are treated similarly. If I apply for a job and I am qualified for that job, procedural justice requires that my application be considered. If an employment specialist simply threw away every other application, procedural justice would be lacking. If I am charged with a crime, certain procedures must be followed in my journey from indictment to trial. It is not procedurally fair to deny some accused individuals the same procedural protections that are allowed to others. Distributive justice or fairness involves outcomes. If you and I are each charged with stealing$500 worth of company property, and through fair procedures we are each found guilty, but you are given a warning and I am fired, then distributive justice did not prevail.

Considerations of fairness and justice often prompt us to think about how a social system works. If my company develops a new software product, it seems fair that I be able to sell this product and not be forced to give it away. If I choose to give it away for strategic reasons, that is a different story, but if I attempt to sell the product and users simply take it and refuse to pay, that is not fair.

The philosopher most identified with issues of fairness and justice is John Rawls. In his most famous work, *A Theory of Justice* (Rawls, 1971), he suggests a way of thinking about these issues which he calls the "veil of ignorance." Rawls suggests that if we want to get an objective view of whether a society is just or fair in its distribution of benefits and burdens, we imagine ourselves behind this veil of ignorance. We do not know whether we will be rich or poor, old or young, gifted or not. From this perspective, he suggests that we think about how fair a society or a social system is in the way it deals with its members. His premise is clever: we tend to favor systems that benefit us, and think unfair systems which leave us paying more and receiving less than others. By removing ourselves from our current position and imagining that we had to appraise a social system without knowing our place in it, we are apt to be more objective in our appraisal of that system.

Before applying these three ethical approaches to some specific issues involving information systems security, it will be useful to make some comparative comments about the three approaches. The rights and duties approach is the narrowest of the three. It maintains that the moral or ethical act is the one that observes any duties imposed on the actor by the rights of others involved in the situation under analysis. The utilitarian approach is a bit broader in its scope. It maintains that the moral or ethical act is the one that brings about the greatest good for the greatest number. This analysis involves identification not only of those involved in a given situation who have rights which impose duties on the actor, but also those who will be affected by the action under consideration, even if they do not have specific rights in this situation. Finally, the fairness and justice approach is widest in its scope, because it maintains that the moral or ethical act is the one which fits within a larger social system that is fair and just.

All three views of ethics provide guidance for helping to determine whether or not a given act is ethical or moral. All three are complex enough to require some time and consideration before any conclusion can be reached. They are not, then, tools for use on the everyday decisions which managers and professionals make constantly. They are useful when a significant decision produces concern about morality, and when it is not immediately clear what an individual who is trying to be ethical should do. They are not mathematical formulas (although utilitarianism may appear to be). They do provide ways to think about significant decisions that can help to clarify issues involved, and to sort out the moral consequences of these decisions, as opposed to their purely practical consequences.

ETHICAL ANALYSIS OF COMPUTER SECURITY ISSUES

In this section we will apply the three approaches to ethics discussed above to specific topics concerning information technology security issues of the present and future. As the title of this chapter indicates, specific decisions will involve new technologies in the new millennium, but the basic issues of ethics or morality remain the same. We will not attempt to be exhaustive in listing issues to be analyzed, but rather will take a sample of some of the issues likely to be of concern in the years ahead, and show how a moral philosopher might go about analyzing these issues. Topics that we will treat include software piracy, privacy rights of employees and computer hacking.

Software Piracy

The term piracy, named for people who "made their living" by stealing the goods and sometimes ships of others, refers to the appropriation, installation, and use of software without reimbursing its producer. If one pays a small price to a pirate for an expensive program, this still constitutes piracy because the original producer receives no reimbursement. A legal analysis of software piracy would center on the issue of intellectual property rights. How would a philosopher view the practice of software piracy?

Using the utilitarian approach, we might conclude that piracy results in the greatest good for the greatest number, because many users get the benefit of the software at little or no cost, while only those directly involved in producing it suffer any harm. We might also conclude that many of the users could not have afforded the software at its regular price, so their benefit is especially great, while the producers, having more access to resources, do not suffer a corresponding harm. An argument is also sometimes made that much software is overpriced (Microsoft, after all, is on a percentage basis, one of the most profitable companies in the world). The assumption underlying this argument is that zero may be too low a price, but the officially charged price is too high. Thus, if something like theft is involved, at least the theft is smaller than the list price.

There is another way of using utilitarianism to consider the issue of software piracy, and it leads to a quite different conclusion. If we extend our consideration of who benefits and who is harmed, the results are different. First, if we ask what good a person derives from using that which belongs to someone else without paying for it, we can identify the happiness or benefit that comes from obtaining something for nothing. However, if we were discussing a television set instead of a software program, would we judge it to be a good thing that someone got it without paying for it? If someone succeeded in obtaining another person's airplane ticket without their knowledge and consent, and thus enjoyed a free cross-country trip, would we judge this to be a good result? Second, what are we to think of those who purchased the software? Do they enjoy a benefit or suffer a harm when someone else gets and uses the same software without paying for it? Finally, if software piracy becomes widespread, what of those who produce software? Are they likely to continue this activity if they cannot obtain reasonable reimbursement for their efforts? In the longer run, if discouraged software producers decide to pursue other employment with better financial returns, who benefits and who suffers? Economic theory says that new companies start up in industries where the potential for profit is perceived. If those who might start software companies perceive that most "customers" do not pay for the product, are they not likely to pursue some other business opportunity with a greater likelihood of profits?

A utilitarian analysis of software piracy, then, suggests that this practice does not actually yield the greatest good for the greatest number of people. What about an analysis based on rights and duties? We saw earlier that this approach declares an act to be moral or ethical if it observes any duties imposed on the actor by the rights of others involved in the act or transaction. We also saw that there are three basic sources from which people obtain rights: as a human, as a citizen of a particular country, province, or state, and by position (Chief Financial Officer, police officer). One of the rights which individuals have as humans is the right to private property, reflected in the many cultural variations on "thou shalt not steal". Many countries, provinces, states etc. also confer legal property rights on their citizens, with corresponding penalties for failure to observe these rights. The question then arises whether intellectual property such as software generates the same rights and duties

as physical or real property does.

Patents and copyrights seem to provide ample precedent, in legal terms, for the notion that intellectual property can produce rights and duties in ways similar to physical property. If this is so, then the producer or owner of the intellectual property (the software company) has the right to demand compensation from those who use the property. If the compensation charged is excessive in the eyes of the potential users, they can obtain similar software from a different vendor, or forego the use of the software entirely. The underlying premise remains: the owner or producer of the software has a right to be compensated for its appropriation and use. This right imposes a duty on those who appropriate and use the software to compensate the owner or producer. Piracy ignores this right, and hence fails to observe a duty that arises from the owner's right to compensation. Even if the owner is very rich or very profitable, the right remains, and hence the duty does as well. There is no duty to use the software, only a duty to compensate the owner if one uses it. Again, it is well to remember that we are considering moral or ethical duties here; the legal rights and duties are a separate issue.

How would a philosophical analysis based on fairness and justice approach this topic? As we discussed earlier, fairness and justice involve social systems, and their distribution of benefits and burdens. In this analysis, emphasis is placed on assuring that those similarly situated receive similar treatment, or, failing this, that there are good reasons for deviation from similar treatment. If some individuals get the benefits of using a software package free, because they pirated it, and other individuals pay for the benefits of the same software package because they purchased it, fairness and justice do not prevail. If the producers of software are paid for their efforts by only some of those who gain the benefits, again fairness and justice are lacking. This is not to say that software producers cannot provide free copies of their software to beta customers for testing and feedback. It is also not to say that software writers who choose to do so cannot provide their software free to anyone who wants it. What we are saying is that software developers who choose to sell their product and then do not receive payment from some users (pirates) are suffering unjust and unfair treatment, and that this is true whether or not there are explicit laws against software piracy in a given country or province.

All three of the approaches to ethical or moral decision-making which we discussed in the first part of this chapter lead to the conclusion that software piracy is unethical. The prospect of something for nothing is attractive to humans. The arguments sometimes made to justify piracy, such as those outlined in the first part of our utilitarian analysis above, have a certain initial credibility. However, on further reflection, it is clear that from a philosophical viewpoint, software piracy is wrong.

Employee Monitoring

Existing information technology allows employers to monitor a variety of employee activities at very little cost. As technology continues to develop in the new millennium, such monitoring capabilities are likely to increase. There are some comparisons that can be made to employee use of non-computer equipment. Many companies have rules limiting employee use of company telephones for personal business. Employees who have access, on a regular or occasional basis, to company cars are usually subject to restrictions regarding their use. Policies regarding the use of office photocopiers and other equipment for personal use are common. Thus the issue of how employees can use company equipment, and how companies can monitor that use, is not new. However, the nature of computer technology

presents some questions and issues which are different from those involving other sorts of company equipment.

In addition to issues dealing with employee use of company equipment or technology, the nature of computer systems allows for easy employer monitoring of employee productivity and use of time. Many employees use computers as normal operating tools. Software to measure everything from keystrokes to transactions makes it easy for management to monitor productivity (and slack time) in ways that were only possible in the past by extended direct observation and measurement by supervisors. Even the server at a local restaurant now uses a computer to track orders and customer purchases, making it possible for supervisors to know at the end of a shift how many customers each server dealt with, the total amount of purchases at that server's tables, the frequency with which add-ons (desserts, side dishes) were purchased and the time each customer stayed in the restaurant.

There are two sets of related issues involved in the category of employee monitoring. The first of these is the use by employees of company equipment, and the second is the use of company time. The monitoring of both equipment and time which is made possible by information technology exceeds that possibility before its widespread use. Many employees are uneasy with constant, detailed monitoring of their performance. Disputes also arise around the issue of whether employer usage policies are appropriate. One example involves the use of company computers for business. Is it acceptable for an employee to type a personal letter or send a personal e-mail message on a company computer during break time or after working hours? What if the employee uses the company computer for on-line shopping? Viewing pornography? Sending anti-company messages?

A utilitarian approach would ask whether personal use of company computers is sometimes appropriate or acceptable, and would then ask the degree to which company monitoring of such personal use or of employee productivity measures is acceptable. In both cases, acceptable would mean producing the greatest good for the greatest number of people involved. We will address these two questions individually.

Does some personal use of company computers (we include company software here) produce the greatest good for the greatest number of people, or would a policy reserving company computers strictly and exclusively for business use be more in accord with utilitarian principles? If work time were strictly and exclusively for work, it would be easier to justify a work-related usage only policy for company computers. As more people work irregular hours, have flexible scheduling, work from home or from the road by means of some form of telecommunication, and take work home in the form of computer work, the line between work and personal time becomes increasingly blurred. If employers want their employees to perform some work outside of the normal work place or hours, it becomes more difficult to justify a policy limiting company computers strictly and exclusively to work-related matters. Most employers would allow an employee working late to make a telephone call using company equipment to inform their spouse or baby-sitter of their delayed arrival. Is this really any different than allowing the same employee to send an e-mail message instead of making a phone call? Such use of company computers seems to produce a benefit or good for the employee, the spouse or sitter, and the child or children without causing harm to anyone. The cost of sending such an e-mail (like the cost of making the phone call) is so small that transaction costs for collecting it would exceed the amount collected.

At the other extreme, suppose an employee is using the company computer to spend several hours a day shopping at on-line auctions, or trading stocks in his or her personal

account, or viewing pornography on-line. It is difficult or impossible to argue that such practices produce the greatest good for the greatest number. The time spent in such pursuits obviously is not spent on the work for which the employee is being paid. The cost of using company computers and networks becomes significant. Other employees, observing such behavior while they are engaged in the employer's work do not benefit. If such practices become widespread, prices will rise and profits fall as the company hires more and more workers to do the tasks left undone by those dedicating large parts of their working day to personal pursuits. Clearly, the total of harm done in such a situation outweighs the good that the employee may perceive as a result of his or her personal pursuits on company time. The issue here is not so much technology as it is productivity.

A utilitarian approach, then, finds that occasional limited use of company computers for personal business might well be for the best, while frequent and extended use clearly is not. The problem for managers comes in deciding what constitutes occasional limited use and what goes beyond that norm. Wherever the line between acceptable and unacceptable usage is drawn, the only way for employers to know which, if any, employees are exceeding acceptable limits is to monitor employee usage of company computer resources. Without such monitoring the employer has no objective basis for confronting even the most brazen abuser of company regulations in this area. Lack of such monitoring means that whatever standard is set, it is basically unenforceable.

Given that monitoring of usage is reasonable, what about monitoring of content? It is one thing for a supervisor to know that an employee spent ten minutes last week surfing the Net on a company computer. It is quite another thing to know that the employee visited 12 pornographic sites, or downloaded instructions for making bombs at home. Here computer technology presents different issues from previous technologies. An employer might review telephone records and see that an employee made three calls last week, but further effort is required to determine the recipient of the calls, and there is no way to determine what was said. With current technology, an employer can easily know to whom an e-mail was sent, and what it said. Although an employer can carry out such monitoring, is it ethical? Is a review of the sites visited by an employee on the World Wide Web using company technology ethical, or must the employer stop at the point of monitoring number of sites without proceeding into their content?

A utilitarian would argue that the invasion of privacy for the many employees whose usage is innocent is a greater harm than the good that might come from the occasional apprehension of an individual whose usage is not. While some might argue that e-mail is more like a postcard than a sealed letter, many employees and managers would feel that their privacy had been violated if their personal e-mail was read without their knowledge or permission. The case would be different if an employee had already been identified as a bomber or embezzler, and evidence was being sought to confirm information already known through other means. Here the invasion of privacy would be specific and grounded in apparent good cause, whereas routine random review of the contents of employee Web browsing or e-mail involves a general invasion of privacy without any particular grounding.

Analysis of the same issues using a rights and duties approach would proceed as follows. The key question is whether someone (in this case either the employee or the employer) has rights which impose duties on another party. Let us first address the question of employee use of company computers or networks for personal matters. The company clearly owns the computers, software, networks etc. As the owner, the company has a right

to determine their use, and this right imposes a duty on employees. Can the company absolutely restrict all use to company-related business? Obviously it could attempt to do so. However, as we saw in the utilitarian analysis above, at least occasional minimal use by employees for personal matters such as notifying a spouse or sitter of late arrival seems to be reasonable, and its prohibition unreasonable. Thus some uses of company technology for personal use appear to be in order. It is not clear that the employee has a right to such use that imposes a duty on the employer. Rather, it seems that an employer who exercised an absolute ban on any personal use by employees would be acting unreasonably, and it is difficult to argue that an employer has a right to act unreasonably which imposes a duty on employees to accept such action.

If some employee use of company technology for personal matters is permissible, there are clearly limits to such use. As we discussed above in the utilitarian analysis, an employee who spends half the workday pursuing personal interests by using company technology is not acting properly, and the company has a right to limit or halt such actions. But, the company cannot halt actions of which it is unaware, so a right to monitor employee usage seems reasonable.

On the question of monitoring content in addition to usage, a moral analysis using rights and duties would examine employee rights to privacy, and employer rights to control the uses of its technology. Most societies agree that individuals have some right to privacy, although there can be disagreement on the extent of this right. All except totalitarian societies accept a right of individuals to private conversation. E-mail can be seen as conversation conducted by way of an electronic medium, and hence a general right to privacy in such conversation can be argued. If there is a right to read what one wants without obligation to make this public knowledge, then by extension viewing sites on the World Wide Web might be seen as a form of reading which entails some right to privacy. To the extent that such rights exist, employers have a corresponding duty not to interfere with these rights.

Clearly, exceptions can and should be made for compelling reasons. If an employee whose monitor is in public view of other employees chooses to view sexually explicit material on that monitor, the employer has both a right and a duty to stop such viewing. In the United States, failure to do so would quite probably result in a lawsuit against the employer for allowing a hostile work environment which is offensive to other employees. However, in the absence of compelling reasons, an ethical analysis based on rights and duties would put considerable weight on the employee's right to privacy with regard to content.

A third way of analyzing these issues involves consideration of fairness and justice. This is a more systematic view, and asks whether the system of distributing benefits and burdens is fair or just. Is it fair not to let employees use company technology for personal use ever under any circumstances? As we saw in the two previous analyses, there are some cases, such as the use of e-mail to alert a spouse or baby-sitter about late arrival, where it seems that employers should allow personal use by employees of company technology. There are also cases where such use is clearly abusive, and employers should not allow it.

To be fair and just, employer policies on such issues need to be uniform as they apply to employees, not favoring some and punishing others in similar situations. Employees who routinely work long hours might be allowed more personal use of technology because of the corresponding lack of opportunity to take care of personal business outside of work hours. Fairness would require that all employees who routinely work long hours benefit from

similar policies. If an employer routinely reads the e-mail messages of all employees, is this fair, since they are all being treated alike? While procedural justice might be invoked here, the many who do not abuse e-mail and the few who do are being equally monitored, and this result does not reflect distributive justice.

We can conclude, then, from this analysis of employee privacy issues that the moral approach involves a balance between the interests of employers and those of employees. While computer technology presents some new issues, and will undoubtedly present more, there are analogies or comparisons to other technologies that provide a starting point for thinking through the issues. Policies and procedures that take into account both the employer's rights and responsibilities and those of employees can be both practical and ethical. This is not to say that all employers or all employees will agree with this analysis, or that clear answers to every possible situation can be found. It is to say that some principles of moral or ethical behavior can be identified and applied regarding computer technology and employee privacy.

Hacking

The last issue that we will examine to illustrate the philosophical approach to issues of computer security is that of hacking. For purposes of this discussion, we will define hacking as deliberate attempts, whether successful or not, to gain unauthorized access to one or more computer systems. Various motives drive hackers: some merely want to see if they can gain unauthorized access, while others want to gain such access in order to appropriate information within the system or to interfere in some way with the system's normal functioning. While the first category of motives (merely to see if the hacker can gain access) may appear harmless, and thus not really a matter for ethical analysis, comparison to other types of "harmless" intrusion puts a different light on the matter. If someone breaks into your home just to show that they can, but does not damage or steal anything, chances are you would not consider this a harmless intrusion. Under U.S. law, breaking and entering is a crime by itself, even if nothing is taken and no damage is done. Again, if someone tapped your phone and listened to your private conversations just to show that they could, you probably would not shrug this off as a harmless intrusion. We need, then, to consider both kinds of hacking as subjects for ethical analysis.

Some systems do not require any authorization for users to access them. Many Web portals are of this nature. Similarly, many Web content sites and retailers provide open access to anyone, with no authorization required. By the way we have defined hacking (deliberate attempts...to gain unauthorized access) these sites cannot be hacked. The systems underlying these sites, however, are not open to general access. Other systems require authorizations for a variety of reasons: commercial, content privacy, military security, etc. When a hacker attempts to gain unauthorized access to a system, the attempt itself presents questions of morality, aside from whatever is or is not accomplished as a result of the attempt.

A utilitarian analysis would measure the happiness or the good gained by the hacker and compare it to the harm suffered by others. It does not appear that others besides the hacker gain from unauthorized entry. Whoever has established authorization requirements obviously thought there was some grounds for such requirements. They suffer some harm when one or more individuals violates these grounds and attempts to gain unauthorized access. While some see this as an innocent technical contest between those establishing

access routines and those attempting to circumvent these routines, a utilitarian sees more at stake. Since authorization is required for some reason, and not merely to set up a game or contest, unauthorized access is not harmless. If the access becomes known, the system administrator suffers the harm of realizing that authorization procedures have been breached, but typically does not know what additional harm, if any, has been done. Thus he or she must not only revise the authorization procedures at some expense of time and money, but might well also have to perform additional diagnosis on the system to determine whether and to what extent the hacker has changed it. The harm suffered will vary with the content of the system. A system containing names and addresses of past customers is exposed to much less harm than one containing information on the targeting of nuclear missiles. Nonetheless, a known breach of authorization procedures quite probably causes more harm than can be offset by whatever good the hacker enjoys by the simple fact of unauthorized system entry.

If unauthorized entry leads to further action, such as appropriating private information from the breached system, or crashing the system, then the harm suffered is greater. The gain to the hacker might also be greater, since he or she may obtain monetary benefit from appropriated information or additional personal satisfaction from crashing the system. Whatever the benefit obtained by the hacker subsequent to gaining unauthorized entry, it is very difficult to make a case that his or her gain outweighs the total loss of others affected. Thus, a utilitarian analysis will conclude that the greatest good for the greatest number is not obtained by hacking, whatever the motive and regardless of whether harm beyond the fact of entry is done.

A rights and duties approach to the issue of hacking asks whether anyone has a right that imposes a moral duty on the hacker. By definition the hacker is attempting to gain unauthorized access to a system. Does anyone have a right to impose such authorization requirements, which in turn would impose a duty to obtain authorization on the hacker? As we saw earlier in our analysis of software piracy, systems do have value. Their creation, testing and maintenance have real costs in terms of time and money. Those who own or administer the systems have a right to control their intellectual property, just as those who own or administer real property have a right to control access to it.

What happens in the case where the owner or administrator believes that he or she has a right to limit access, but the hacker does not? Some hackers justify their actions either on the basis that information contained in a system should be accessible to all, or that either the system or its owner or administrator is immoral, and therefore the hacker has a right or even a duty to interfere with the system. If the morality of hacking were determined by every individual's personal views, then those who oppose the policy of a government would have a right and perhaps a duty to access and interfere with its computer systems. The idea that rights and duties come from each individual's personal view of things is fundamentally opposed to the whole moral approach of rights and duties that we discussed earlier in the chapter. At least some rights exist independently of whether every individual agrees with them or not. Individuals who believe they have a right and a duty to take the lives of others who disagree with them are not called principled; they are called killers.

We can also analyze the morality of causing damage (appropriating information, crashing a system) after gaining unauthorized access using a rights and duties approach. As we saw in our earlier discussion of employee monitoring, the issue to be analyzed is not really the use of a particular technology, but rather the action which is conducted using the technology as a tool. If proprietary information is appropriated by means of hacking into a

system, the issue is really one of stealing the intellectual property of another. Computer technology was used, but if one had stolen paper documents containing the same information, the issue of theft of intellectual property would be the same. Whether I disable a company's computer system or the machinery in its manufacturing plant, I have still interfered with its right to conduct business. In both cases, the right of the owner of the intellectual property or the computer system or the manufacturing plant imposes a duty on others not to steal the intellectual property or to disable the system or machinery.

Finally, we examine the issue of hacking from a fairness and justice perspective. According to this perspective, the moral act is the one which treats similarly situated people similarly, with regard both to procedures and to outcomes. In a fair social system, those who have created something of value, individually or corporately, would not be forced to give free access to anyone who sought it. The issue here is similar to that examined earlier in regard to software piracy. Fairness in procedure requires that those who produce software or who own or administer systems be able to limit access to that software or those systems. In other words, the software or systems can be treated as proprietary, and access to them can be limited to those who are authorized. Therefore, attempts to gain unauthorized access for whatever reason are not fair or just.

What if the hacking is only designed to gain access, but not to appropriate information from a system or cause it any harm? Is this not innocent, and morally acceptable? Again, the administrator who becomes aware that his or her system has been accessed without authorization does not know whether information has been appropriated or whether the system has been harmed in some way. Thus the result of such "innocent" hacking still causes unfair burdens to fall on those who own or administer the software or system. Obviously, if the hacker gains the use of private information from the system, or crashes or corrupts the system, the results for the owner or administrator are not fair and just. Other possible users of the system also are not treated fairly or justly, because they pay for access to the same information that the hacker gets free. If the hacker crashes or corrupts a system, those who are entitled to its use are denied that use, which again violates fairness and justice.

In summary, all three methods of ethical analysis conclude that hacking is not ethical or moral. Hackers are sometimes glorified as clever or whimsical technical geniuses, busily testing their genius. The results of their efforts do not stand up under moral scrutiny. To some extent, ethical analysis is a matter of clear thinking, and once the issues are separated and identified as we have done here, the answers become obvious.

SUMMARY AND CONCLUSION

Technological change in hardware and software proceeds at a very rapid pace. The coming of the new millennium provides a natural opportunity to reflect on changes and similarities as information technology evolves. Because current and future technology provide means of gathering, storing and disseminating information which have never before been available to humans, questions are bound to arise about standards for doing so. One way of dealing with these questions is through legal mechanisms, and this is being done, although legal standard setting is often reactive rather than proactive. In this chapter we have taken a different approach, and introduced an approach rooted in philosophy. Ethics, or the study of moral right and wrong, is a very old discipline. Most of the influential authors in the field lived before information technology as we know it even existed. However, the

principles for deciding about the morality of what humans do have not changed over time.

After a brief introduction to the way philosophers approach issues, we have elaborated three basic approaches to ethical analysis which reflect much of the thinking of mainstream philosophy. One advantage of the philosophical approach is that some of the thinking involved has already survived one (and in some cases two) previous millenial events. Few people in the history of the human race have written anything that was still considered worthy of serious consideration hundreds or thousands of years after their death. Some philosophers are among these few.

We have analyzed three topics pertaining to information technology security using the three approaches to ethical reasoning. This was done not because these are the only, or even the most important topics, but to give a representative example of how a philosopher would approach such analysis. Hopefully, by seeing how ethical analysis is done on three different and important topics, the reader can see how such principles might be used to analyze other topics that might be of interest. As technology continues to develop in this new millennium, we can be sure that new issues will arise that we cannot yet foresee. However, as long as the principles used for ethical analysis remain the same, the fact that the issues to which they are applied are new does not present any insuperable problems.

The results of an ethical analysis are useful for individuals or groups concerned about doing the right thing. The results of such analysis will usually, but not always, agree with the results of legal analysis. Not all thoughtful people, or even all trained philosophers, will always come to the same conclusion as a result of an ethical analysis. What can be said for this approach is that it incorporates principles developed over a long period of time by thoughtful people. The principles involved have been reviewed and debated for many generations and have been found to be worth serious consideration even after extended examination and challenge. If the humans who design and administer ever more advanced information systems consider their actions as humans (not as technicians or attorneys or accountants) and proceed along paths they consider morally right, much will have been accomplished. Awareness of moral issues, and methods of thinking them through have been the two goals of this chapter. To the extent they have been accomplished, designers and users of information technology will be well served for the next millennium.

NOTES

1. For a relatively nontechnical introduction to philosophy, see Will Durant, *The Story of Philosophy: The Lives and Opinions of the Great Philosophers of the Western World*, (New York: Simon & Schuster, 1961), and Bertrand Russell, *A History of Western Philosophy* (New York: Simon & Schuster, 1972).
2. Two book-length treatments of this topic are Lawrence Kohlberg, *The Philosophy of Moral Development* (San Francisco, Harper and Row, 1981) and James Rest, *Moral Development: Advances in Research and Theory* (New York: Praeger, 1986).
3. For a selection of articles covering a wide variety of approaches to and applications of ethics, including some non-Western views, see Peter Singer, editor, *A Companion to Ethics* (Cambridge, Mass.: Blackwell, 1981).
4. Many textbooks on business ethics lay out basic ethical principles of ethics and apply them to specific business topics. For a typical example, see Richard DeGeorge, *Business Ethics*, 4th edition (Englewood Cliffs, NJ: Prentice Hall, 1995).

REFERENCES

Aristotle (1953). *The Nichomachean Ethics*, J Harper, translator. Baltimore, MD: Penguin Books.

Freeman, R. Edward (1984). *Strategic Management: A Stakeholder Approach*. Boston: Pittman.

Mill, John Stuart and Jeremy Bentham (1987). *Utilitarianism and Other Essays* Alan Ryan, editor. London: Penguin Books.

Rawls, John (1971). *A Theory of Justice*. Cambridge, Mass.: Harvard University Press.

Wilson, James Q (1993). *The Moral Sense*. New York: Free Press.