Towards a Theory of Privacy in the Information Age

CEPE'97

James H. Moor
Dartmouth College
James.Moor@Dartmouth.edu

Greased data

When we think of ethical problems involving computing probably none is more paradigmatic than the issue of privacy. Given the ability of computers to manipulate information – to store endlessly, to sort efficiently, and to locate effortlessly – we are justifiably concerned that in a computerized society our privacy may be invaded and that information harmful to us will be revealed. Of course, we are reluctant to give up the advantages of speedy and convenient computerized information. We appreciate the easy access to computerized data when making reservations, using automatic teller machines, buying new products on the web, or investigating topics in computer data bases. Our challenge is to take advantage of computing without allowing computing to take advantage of us. When information is computerized, it is *greased* to slide easily and quickly to many ports of call. This makes information retrieval quick and convenient. But legitimate concerns about privacy arise when this speed and convenience lead to the improper exposure of information. Greased information is information that moves like lightning and is hard to hold onto.

Consider, for example, listed telephone numbers which have been routinely available through a telephone operator and a telephone book but which now are available along with address information in giant electronic phone books on the internet. The Hanover, New Hampshire telephone book (the telephone book for where I live) is rather hard to locate in most places in the world, but now anyone in the world with access to the internet can easily find out my phone number, who my wife is, and where I live. One can even retrieve a map of my residential area. I don't consider this to be a breach of privacy, but I use it to point out how the same information, which has technically been public for a long time, can dramatically change levels of accessibility practically speaking when put into electronic form on computer networks. It is ironic that my name may be hard to find in the internet phone book in that it is listed there anachronistically in an abbreviated form. "James" is abbreviated as "Jas," an abbreviation I never use and have seen only in old print phone books, presumably introduced to save print space but mindlessly copied when put on the internet. Don't tell anyone.

The greasing of information makes information so easy to access that it can be used again and again. Computers have elephant memories – big, accurate, and long term. The ability of computers to remember so well for so long undercuts a human frailty that assists privacy. We, humans, forget most things. Most short term memories don't even make it to long term memory. Every time I go to a busy supermarket I am a new customer. Who can remember what I bought the last time I was there? Actually, a computer does. Most of the time I shop at a cooperative food store that gives a rebate at the end of the year. When I buy food, I give the checkout person my account number (I can remember at least that most days). The checkout person scans my purchases which appear on a screen by the name of the item and its price. This information is definitely greased. It appears as quickly as the checker can move the items across the barcode reader. Then my total is displayed and the information is added to my grand total of purchases on which I get a certain percentage back each year. Notice that in addition to the total of my purchases the market also has information about what I have purchased. It helps the market keep track of its inventory. But, it also means that the store has a profile on my buying habits. They know how much wine I purchase, my fondness for Raisin Bran cereal, and the kind of vegetables I prefer. In principle, such evidence could be subpoenaed if my eating habits were relevant to a court case. Does this accumulation of information violate my privacy. I suppose not, but it is greased so that it moves easily and is more accessible over a longer period of time than ever before. Practically speaking, the information is never forgotten. A documented history of purchases generates the possibility for an invasion of privacy that does not exist without it.

In the case of my food shopping the collection of information is obvious to me. I can see my eating habits and my limited will power flash on the display screen as the calories tumble by on the conveyor. But information about us can be collected subtlety when we don't realize it. The greasing of information allows other computers to capture and manipulate information in ways we do not expect. Consider a final personal example to illustrate this. Not long ago I lived for a few months in Edinburgh. On days I didn't feel like cooking, I would sometimes order pizza. The pizza was delivered to my apartment and hence was a convenient way to get a quick meal. However, I was somewhat taken aback the second time I phoned the pizza establishment. Without my placing an order the pizzamakers already seemed to know my address and my favorite pizza. Did I want to have another medium pepperoni and mushroom delivered? I hadn't been in Edinburgh very long. How could they possibly know my taste (or lack of taste) so quickly? The answer, of course, was their use of caller ID. No mystery here. I had called before and given in-

formation about my pizza preference and my delivery address, and they had linked it with my phone number. When I called the second time, my phone number was captured electronically by the pizza parlor and used to select the other information from my first call. Had my privacy been invaded? Probably not, but I confess that I initially felt some mild indignation that my pizza profile had been stored away without my knowing it. If I were a frequent customer in a fine restaurant and the waiter had memorized my tastes, I would feel complimented that he remembered me. But, as efficient as the caller ID/ computer system was, I found no gain in self worth by having a pizza parlor computer recall my intake of pepperoni and mushroom pizza.

I mention these three examples, the internet phone book, the supermarket refund policy based on bar code data, and the pizza parlor caller ID, not because they represent some deep treachery but because they are perfectly ordinary activities and illustrate how effortlessly information is collected and transmitted without any of us giving it a second thought. Once information is captured electronically for whatever purpose, it is greased and ready to go for *any* purpose. In a computerized world we leave electronic footprints everywhere and data collected for one purpose can be resurrected and used elsewhere. The problem of computer privacy is to keep proper vigilance on where such information can and should go.

For the most part the need for privacy is like good art, you know it when you see it. But sometimes our intuitions can be misleading and it is important to become as clear as possible what privacy is, how it is justified, and how it is applied in ethical situations. In this paper I will assemble pieces of an overall theory of privacy and try to defend it. In the computer age during a period when information technology is growing rapidly and its consequences are difficult to predict more than a few days in advance, if at all, it is more important than ever to determine how privacy should be understood and guarded.

Grounding privacy

From the point of view of ethical theory privacy is a curious value. On the one hand, it seems to be something of very great importance and something vital to defend, and, on the other hand, privacy seems to be a matter of individual preference, culturally relative, and difficult to justify in general. Is privacy a primary value? How can we justify or ground the importance of privacy?

I will discuss two standard ways of justifying privacy, both of which I have used before, and describe the limitations of these two approaches. Then I will present a third way to justify the importance of privacy which I now find more defensible. Philosophers frequently distinguish between instrumental values and intrinsic values. Instrumental values are those values which are good because they lead to something else which is good. Intrinsic values are values which are good in themselves. Instrumental values are good as means; intrinsic values are good as ends. My computer is good as a means to help me write papers, send e-mail and calculate my taxes. My computer has instrumental value. However, the joy I gain from using my computer is good in itself. Joy doesn't have to lead to anything to have value. Joy has intrinsic value. And, as philosophers since Aristotle have pointed out, some things, such as health, have both instrumental and intrinsic value. This familiar philosophical distinction between instrumental and intrinsic values suggests two common ways to attempt to justify privacy.

Almost everyone would agree that privacy has instrumental value. This is its most common justification. Privacy offers us protection against harm. For example, in some cases if person's medical condition were publicly known, then that person would risk discrimination. If the person tests HIV+, an employer might be reluctant to hire him and an insurance company might be reluctant to insure him. Examples of this nature are well known and we need not amass examples further to make a convincing case that privacy has instrumental value. But, so do toothpicks. To justify the high instrumental value of privacy we need to show that not only does privacy have instrumental value but that it leads to something very, very important. One of the best known attempts to do this has been given by James Rachaels. Rachaels suggests that privacy is valuable because it enables us to form varied relationships with other people. [Rachaels, 1975, p. 323] Privacy does enable us to form intimate bonds with other people that might be difficult to form and maintain in public. But the need to relate to others differently may not ground privacy securely because not everyone may want to form varied relationships and those who do may not need privacy to do it. Some people simply do not care how they are perceived by others.

The justification of privacy would be more secure if we could show that it has intrinsic value. Deborah Johnson has suggested a clever way of doing this. Johnson proposes that we regard "privacy as an essential aspect of autonomy". [Johnson, 1994, p. 89] So, assuming that autonomy is intrinsically valuable and privacy is a necessary condition for autonomy we have the strong and attractive claim that privacy is a necessary condition for an intrinsic good. If privacy is not an intrinsic good itself, it is the next best thing. But, is it true that "autonomy is inconceivable without privacy"? [Johnson, 1994, p. 89]

I have proposed a thought experiment about Tom, an electronic eavesdropper, which, I believe, shows Johnson's claim to be incorrect. [Moor, 1989, pp. 61-62] In this thought experiment Tom is very good with computers and electronics and has a real fondness for knowing about you – all about you. Tom uses computers secretly to search your financial records, your medical records, and your criminal records. He knows about your late mortgage payments, your persistent hemorrhoids, and that driving while intoxicated charge that you thought was long forgot-

ten. Tom is so fascinated with your life that he has clandestine cameras installed which record your every movement. You know nothing about any of this, but Tom really enjoys watching you, especially those instant replays. "For Tom, watching your life is like following a soap opera – The Days of Your Life." [Moor, 1989, p. 62] I think most of us will agree that there is something repugnant about Tom's peeping. But what is it? It is not that he is directly harming you. He doesn't use any of this information to hurt you. He doesn't share the information with anyone else or take advantage of you in any way whatsoever. Moreover, you have complete autonomy, just no privacy. Thus, it follows that privacy is not an essential condition for autonomy. It is conceivable to have autonomy without privacy. Nevertheless, I would agree that some people, including myself, regard privacy as intrinsically valuable, not merely instrumentally valuable.

Now let me consider a third approach to justifying the importance of privacy. I wish to maintain that there is a set of values, which I call the "core values", which are shared and fundamental to human evaluation. The test for a core value is that it is a value that is found in all human cultures. Here the list of some of the values that I believe are at the core: *life, happiness, freedom, knowledge, ability, resources* and *security*. My claim is an empirical one. I am claiming that all sustainable human cultures will exhibit these values. I am not suggesting for a moment that all cultures are moral or that these goods are fairly distributed in every culture. Regrettably, they almost never are. (An ethical theory requires an account of fairness as well as an account of the core values.) What I am claiming is that every viable culture will exhibit a preference for these values. Consider the most primitive, immoral culture you can imagine. As barbaric and repulsive as it is, its members must find nourishment and raise their young if the culture is to survive. These activities require at least implicit acknowledgment of the core values. To abandon the core values completely is to abandon existence.

Is privacy a core value? I wish it were. It would make the justification of privacy so much easier. But, upon reflection it is clear that it is not in the core. One can easily imagine sustainable and flourishing human cultures that place no value on privacy. Consider a man and a woman who live together but give each other no privacy and who could care less about privacy. Presumably, many couples live this way and have no trouble existing. Now imagine a family or a small tribe with equal disinterest in privacy. Everybody in the group can know as much as they want about everybody else. They might believe that their society functions better without secrets. An anti-Rachaelsean in the society might maintain that they have better and more varied human relationships just because they can know everything about everybody! The concept of privacy has a distinctly cultural aspect which goes beyond the core values. Some cultures may value privacy and some may not.

How then should we justify privacy? How is it grounded? Let me propose a justification of privacy by using the core values. The core values are the values that all normal humans and cultures need for survival. Knowledge, for example, is crucial for the ongoing survival of individuals and cultures. The transmission of culture from one generation to the next by definition involves the transmission of knowledge. I emphasize the core values because they provide a common value framework, a set of standards, by which we can assess the activities of different people and different cultures. [Moor, 1998] The core values allow us to make transcultural judgments. The core values are the values we have in common as human beings. To focus on the core is to focus on similarities. But, now let's focus on the differences. Individuals and cultures articulate the core values differently depending on environment and circumstances. The transmission of knowledge is essential for the survival of every culture, but it is not the same knowledge that must be transmitted. Resources such as food are essential for everyone, but not everyone must prefer the same kind of food. So, though there is a common framework of values, there is also room for a much individual and cultural variation within the framework. Let's call the articulation of a core value for an individual or a culture the "expression of a core value".

Although privacy is not a core value per se, it is the expression of a core value, viz., the value of security. Without protection species and cultures don't survive and flourish. All cultures need security of some kind, but not all need privacy. As societies become larger, highly interactive, but less intimate, privacy becomes a natural expression of the need for security. We seek protection from strangers who may have goals antithetical to our own. In particular, in a large, highly computerized culture in which lots of personal information is greased it is almost inevitable that privacy will emerge as an expression of the core value, security.

Consider once again the dichotomy between instrumental and intrinsic values. Because privacy is instrumental in support of all the core values, it is instrumental for important matters; and because privacy is a necessary means of support in a highly computerized culture, privacy is instrumentally well grounded for our society. Moreover, because privacy is an expression of the core value of security, it is a plausible candidate for an intrinsic good in the context of a highly populated, computerized society. Tom, the electronic eavesdropper, who doesn't harm his subject when he spies, nevertheless, seems to be doing something wrong intrinsically. The subject's security is being violated by Tom even if no other harm befalls the person. People have a basic right to be protected, which from the point of view of our computerized culture, includes privacy protection.

I have argued that using the core value framework privacy can be grounded both instrumentally and intrinsically – instrumentally, as a support of all the core values, and, intrinsically, as

an expression of security. I am, however, concerned that the traditional instrumental/ intrinsic understanding may be misleading. Traditionally, instrumental/ intrinsic analyses push us in the direction of a search for a *summum bonum*, a greatest good. We try to find the one thing to which all other things lead. In the core value approach that I am advocating some values may be more important than others, but there is not a *summum bonum*. Rather the model is one of an intersupporting framework. The core values, as the beams of a truss, are in support of each other. Asking whether a core value or the expression of a core value is instrumental or intrinsic is like asking whether a beam of a truss is supporting or supported. It is essentially both. The core values for all of us are mutually supporting. Some people will emphasize some values more than others. An athlete will emphasize ability, a businessperson will emphasize resources, a soldier will emphasize security, a scholar will emphasize knowledge, and so forth. However, everyone and every culture needs all of the core values to exist and flourish. Privacy, as an expression of security, is a critical, interlocking member in our systems of values in our increasingly computerized culture.

The nature of privacy

Understanding privacy as the expression of the core value of security has the advantage of explaining the changing conception of privacy over time. Privacy is not mentioned explicitly either in the United States Declaration of Independence or in its Constitution. [Moor, 1990] It is strange that a value that seems so important to us now was not even mentioned by the revolutionary leaders and statesmen who were so impressed with the ideals of individual freedoms. The concept of privacy has been evolving in the U.S. from a concept of non-intrusion (e.g., the Fourth Amendment to the U.S. Constitution offering protection against unreasonable governmental searches and seizures), to a concept of non-interference (e.g., the Roe v. Wade decision giving a woman the right to choose to have an abortion), to limited information access (e.g., Privacy Act of 1974 restricting the collection, use and distribution of information by Federal Agencies). Privacy is a concept that has been dramatically stretched over time as it. In our computer age the notion of privacy has become stretched even further. Now the concept privacy has become so informationally enriched [Moor, 1998] that "privacy" in contemporary use typically refers to informational privacy though, of course, other aspects of the concept remain important.

Consider a useful distinction that helps to avoid some misunderstandings about the nature of privacy. The term "privacy" is sometimes used to designate a situation in which people are protected from intrusion or observation by natural or physical circumstances. Someone spelunking by herself would be in a naturally private (and probably dangerous) situation. Nobody can see her in the cave she is exploring. In addition to natural privacy there is normative privacy. A normatively private situation is a situation protected by ethical, legal, or conventional norms. Consultations with a lawyer or doctor would be normatively private situations. Obviously, many normatively private situations are naturally private as well. We send mail in sealed envelopes. When an unauthorized entry is made into a normatively private situation, privacy has not only been lost, it has been breached or invaded.

Now if we put the evolving conceptions of privacy together with distinction between normative and natural privacy we get a useful account of the nature of privacy.

> An individual or group has normative privacy in a situation with regard to others if and only if in that situation the individual or group is normatively protected form intrusion, interference, and information access by others. [Culver, Moor, et al., 1994, p. 6]

I use the general term "situation" deliberately because it is broad enough to cover many kinds of privacy: private *locations* such as one's diary in a computer file, private *relationships* such as e-mail to one's pharmacy, and private *activities* such as the utilization of computerized credit histories.

The situations which are normatively private can vary significantly from culture to culture, place to place, and time to time. This doesn't show that the privacy standards are arbitrary or unjustified, they are just different. For example, at a private college faculty salaries are kept confidential, but at some state colleges faculty salaries, at least salaries above a certain level, are published. Presumably, the private colleges believe that protecting salary information will reduce squabbling and embarrassment; whereas state colleges (or the state legislatures) believe that the taxpayers who support the institution have the right to know how much faculty members are being paid. These are different but defensible policies for protecting and releasing information.

Clearly some personal information is very sensitive and should be protected. We need to create zones of privacy, a variety of private situations, so that people can ensure that information about themselves which might be damaging if generally released will be protected. With different zones of privacy one can decide how much personal information to keep private and how much to make public. Notice that on my account the notion of privacy really attaches to a situation or zone and not to the information itself. For instance, if an Internal Revenue Service employee uses a computer to call up and process a movie star's income tax return, then the employee is not invading the star's privacy. He is allowed in this situation to investigate the star's tax return. However, if that same employee were to call up that same star's tax return on his computer after hours just to browse around, then the employee would be violating the star's privacy although the employee may gain no new information! The employee has legitimate access in the first situation but not the second.

The theory I am proposing is a version of the restricted access view of privacy. [Moor, 1990, pp. 76-80] The major opposing view is the control theory of privacy. One proponent of this view Charles Fried writes, "Privacy is not simply an absence of information about us in the minds of others, rather it is the *control* we have over information about ourselves." [Fried, 1984, p. 209] I agree that it is highly desirable that we control information about ourselves. However, in a highly computerized culture this is simply impossible. We don't control vast amounts of information about ourselves. Personal information about us is well greased and slides rapidly through computer systems around the world, around the clock. Therefore, to protect ourselves we need to make sure the right people and only the right people have *access* to relevant information at the right time. Hence, the restricted access view puts the focus on what we should be considering when developing policies for protecting privacy. However, the restricted access account, at least in the form I am proposing it, has all of the advantages of the control theory for one of the goals in setting policies to give individuals as much control (informed consent) over personal data as realistically possible. For this reason I will label my account as a "control/restricted access" theory of privacy.

The control/restricted access conception of privacy has the advantage that polices for privacy can be fine tuned. Different people may be given different levels of access for different kinds of information at different times. A good example occurs in a modern, computerized hospital. Physicians are allowed access to on-line medical information which secretaries are not. However, physicians are generally not allowed to see all the information about a patient that a hospital possesses. For example, they don't have access to most billing records. In some hospitals some medical information such as psychiatric interviews may be accessible to some physicians and not others. Rather than regarding privacy as an all or nothing proposition – either only I know or everybody knows – it is better to regard it as a complex of situations in which information is authorized to flow to some people some of the time. Ideally, those who need to know do, those who don't don't.

The control/restricted access also explains some anomalies about private situations. Usually, when we consider privacy, we are thinking about situations in which individuals possess possibly damaging personal information they want to keep others from knowing. But situations can be private in other circumstances. Imagine a situation in a restaurant with scores of people dining. A couple begin to argue loudly and eventually each shouts to the other about a marital problem they are having. They go into excruciating detail about various kinds of sexual dysfunction and bodily needs. Everyone can hear them and many patrons of the restaurant feel uncomfortable as they proceed with their meal. Finally, the waiter, who thinks he can help, cannot stand it anymore. He walks over to the couple and asks whether they would like his advice. The couple in unison tell him, "No, it's a private matter."

As ironic as their comment may be, it does make sense on several levels. In private situations the access to information can be blocked in both directions. This couple did not want to allow information from the waiter although they themselves had been indiscreet in revealing details to the entire population of the restaurant. Moreover, in our culture some activities are required to be done in private. Discussions of one's intimate marital problems may be one of them. Privacy is a form of protection and it can protect the general population as well as individuals.

Setting and adjusting policies for private situations

So far I have commented on the greasing effect computerization has on information and the potential problems for privacy computerization poses. I have proposed a justification for privacy as an expression of one of the core values and as an essential member of the central framework of values for a computerized society. I have characterized the nature of privacy as an evolving concept which has become informationally enriched with the development of computing. And I have argued that privacy is best understood in terms of a control/restricted access account. Now it is time to focus on practical policies for the protection of privacy. As an example I will use information gathered from genetic testing. This is an interesting case because, practically speaking, genetic testing would not be possible without information technology and with information technology genetic testing is one of the greatest potential threats to our individual privacy. Improper disclosure of our genetic information may be the ultimate violation of our privacy.

Suppose a patient decides to have herself tested for a breast cancer gene. She does not have breast cancer, but breast cancer runs in her family and she wants to know whether she is genetically disposed to have breast cancer. She goes to the hospital for tests for the gene and the results are positive. The results are put in her medical record so that the information is available to physicians to encourage aggressive testing for the disease in the future. The information will be computerized, which means that many heath care providers throughout the state may have access to the information. The patient's health insurance company will also have access to it. Information of this kind could be detrimental to the patient when obtaining life insurance or future health insurance, and eventually, if the information slides through enough computer networks, it could be detrimental to the patient's children when obtaining insurance and applying for employment though they have shown no signs of the disease and have never been tested.

In formulating policies we should try to minimize excess harm and risk. In cases like this, it may be hard to do. Clearly, the medical records should be treated confidentially but that may

not be enough to protect the patient. Because the records are computerized, and hence well-greased, information will be sent rapidly along networks and gathered by third parties who may find their own self-interested uses for it. New legal policies might be helpful here including the passage of statutes protecting patients from discrimination on the basis of genetic testing. Also, the hospital might consider setting up a zone of privacy for patients who want only predictive testing done. There is a difference between predictive genetic testing in which the patient is tested for genetic information that may be indicative of future disease and diagnostic testing in which the patient is tested for genetic information that may confirm a diagnosis of an existing disease. The hospital could establish a private situation for predictive testing so that the patient's records were not incorporated into the regular medical file. These records would be computerized but not accessible to all of those have access to the general medical record. This is a way of adjusting the access conditions to increase the level of privacy for the patient. Of course, the patient should be told what will happen to the test information. The patient might prefer to have the information included in her medical record.

One of the principles that should guide the establishment of policies for privacy is the Publicity Principle.

The Publicity Principle: Rules and conditions governing private situations should be clear and known to the persons affected by them.

In effect, we can plan to protect our privacy better if we know where the zones of privacy are and under what conditions and to whom information will be given. If an employer can read one's e-mail, then applying for a new job is done more discreetly by not using e-mail. The publicity principle encourages informed consent and rational decision making.

Once policies are established and known circumstances sometimes arise which invite us to breach the policy. Obviously, policy breaches should be avoided as much as possible as they undermine confidence in the policy. However, sometimes truly exceptional circumstance occur. Suppose that after some predictive genetic tests are run, new information about the consequences of the test results are uncovered. New scientific evidence in combination with the test results show that the patient surely must have transmitted a devastating disease to her offspring but that the disease can be treated effectively if caught in time. In such circumstances it would seem that the hospital should notify not only the patient but also her adult offspring even though that was not part of the original agreement. The harm caused by the disclosure will be so much less than the harm prevented that the breach is justified.

The Justification of Exceptions Principle: A breach of a private situation is justified if and only there is a great likelihood that the harm caused by the disclosure will be so much less than the harm prevented that an impartial person would permit breach in this and in morally similar situations.

These exceptional circumstances should not be kept secret from future users of the policy. Hence, we need a principle for disclosure and adjustment in the policy statement itself.

The Adjustment Principle: If special circumstances justify a change in the parameters of a private situation, then the alteration should become an explicit and public part of the rules and conditions governing the private situation.

In this example those who continued to have predictive genetic testing would know what information would be released in the stated exceptional circumstances. They would know the possible consequences of their decision to have predictive genetic testing and could plan accordingly. The control/restricted access theory can give individuals as much personal choice as possible while still be concerned about information flow beyond individual control.

Conclusion

In a computerized society information is greased. It moves like lightning and will have applications and reapplications that are impossible to imagine when initially entered into a computer. In a computerize society the concern for privacy is legitimate and well grounded. Privacy is one of our expressions of the core value of security. Individuals and societies that are not secure do not flourish and do not exist for long. It is, therefore, imperative that we create zones of privacy that allow citizens to rationally plan their lives without fear. The zones of privacy will be contain private situations with different kinds and levels of access for different individuals. It is important to think of privacy in terms of a control/restricted access account, because this conception encourages informed consent as much as possible and fosters the development of practical, fine grained, and sensitive policies for protecting privacy when it is not. ◆

References

Culver, Charles, James Moor, William Duerfeldt, Marshall Kapp, and Mark Sullivan. "Privacy." *Professional Ethics* 3. Nos. 3 & 4 (1994): 3-25.

Fried, Charles. "Privacy." *Philosophical Dimensions of Privacy.* Ed. F. D. Schoeman. New York: Cambridge University Press, 1984. 203-222.

Johnson, Deborah G. *Computer Ethics.* 2nd ed. Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1994.

Moor, James. "Ethics of Privacy Protection." *Library Trends* 39.1 & 2 (1990): 69-82.

Moor, James. "How to Invade and Protect Privacy with Computers." *The Information Web.* Ed. Carol C. Gould. Boulder: Westview Press, 1989. 57-70.

Moor, James. "Reason, Relativity, and Responsibility in Computer Ethics." *Reader in Global Information Ethics* Ed. Terrell Ward Bynum and Simon Rogerson. Oxford: Basil Blackwell, 1998.

Moor, James. "What is Computer Ethics?" *Metaphilosophy* 16.4 (1985): 266-275.

Rachaels, James. "Why is Privacy Important?" *Philosophy and Public Affairs* 4. Summer (1975): 323-333.