

Taking the Byte Out of Cookies:

Privacy, Consent, and the Web

Daniel Lin

*Department of Computer Science
University of Illinois at Urbana-Champaign*

Michael C. Loui

*Department of Electrical and Computer Engineering,
Coordinated Science Laboratory, and Graduate College
University of Illinois at Urbana-Champaign*

POLICY '98
PRIVACY ISSUES

Abstract: We consider the privacy of personal information on the World Wide Web, emphasizing a concept of privacy as an aspect of social relationships between individuals. We make three contributions to understanding the right to privacy on the Web: (1) we highlight the role of informed consent as an important consideration for privacy, (2) we **identify** conditions under which the collection and centralization of personal information can be ethically justified, and (3) we offer an interpretation of a "reasonable expectation of privacy" for Internet cookies, a mechanism used by Web sites to remember information about visits to that site.

The views, opinions, and conclusions of this paper are not necessarily those of the University of Illinois. Preliminary versions of this paper were presented at the Seventh Annual Meeting of the Association for Practical and Professional Ethics, Dallas, TX, February 26-28, 1998, and the ACM Policy 98 Conference, Washington D.C., May 10-12, 1998.

Address for correspondence: Michael C. Loui, Graduate College, 801 S. Wright Street, Champaign, IL 61820-6210, e-mail: m-loui@uiuc.edu, telephone: (217) 333-6715, fax: (217) 333-8019.

1 Introduction

What is our right to privacy on the World Wide Web? Is it reasonable for us to assume that we should always have control over our personal information on the Web! These questions become increasingly urgent as we continue to unknowingly release our personal information into cyberspace.

In a recent Internet privacy survey directed by Alan Westin, 53 percent of Internet users and 57 percent of online service users were concerned that their Internet browsing behavior would be linked to their e-mail addresses and disclosed to other people or organizations [1]. Such concerns about privacy are not new. Many of us express similar concerns when we apply for a credit card or a car loan. What is new about our privacy concerns, however, is the environment in which we express them — the Web. According to Moor [2], information on the Web is "greased" and its manipulation occurs more easily and at a much grander scale. Because the Web is a new environment, there are few transactions on the Web whose impact is completely understood by the general public. Furthermore, unlike applying for a credit card or car loan, we may not even be aware that we are releasing personal information as we "surf" the Web.

For instance, many Web sites use a mechanism called a "cookie" which silently collects information about our visit to that site. The consequence of dealing with a new environment like the Web is that we are unable to make deliberate decisions about revealing our personal information. Simply put, we cannot make well-informed decisions because we do not have reasonable expectations of privacy on the Web.

In this paper, we make three contributions to understanding privacy and the right to privacy on the Web. First, we highlight the role of informed consent in the theory of privacy. Because we currently do not have a reasonable expectation of privacy on the Web, informed consent is important: if we do not have enough knowledge to make an informed decision about **revealing** our personal information on the Web, we should be given that knowledge before making our decisions. Second, we establish the conditions under which the collection and centralization of personal information are ethically justifiable. The collection and centralization of personal information on the Web affect our privacy in fundamentally different ways. While previous notions of privacy describe when such manipulations of information cause losses or violations of privacy, they do not address how such violations might be avoided. We address this issue by showing

that informed consent is sufficient for the collection of personal information to be ethical. Third, we offer an interpretation of what a “reasonable expectation of privacy” may mean for Internet cookies. In doing so, we distinguish between morally permissible and immoral uses of cookies.

Section 2 discusses dominant approaches to privacy and the importance of privacy. Section 3 outlines the argument for informed consent. In Sections 4 and 5, we develop the ethical boundaries for collecting and centralizing personal information. Section 6 explores the notion of a reasonable expectation of privacy in public places. In Section 7, we introduce the idea that our reasonable expectations of privacy on the Web should reflect the realization that the Internet is a public place. Finally, in Section 8 we apply our moral analysis to the current privacy concern with Internet cookies.

2 Ethical Theories of Privacy

While at first glance, the concept of privacy may seem simple, many have struggled to adequately describe what privacy actually is. In this section, we present a critical analysis of different theories of privacy.

2.1 Privacy as Nonintrusion

In their 1890 Harvard Law Review article, “The Right to Privacy,” Warren and Brandeis [3] wrote that privacy is the right “to be let alone.” For example, Bob loses some privacy when Alice rummages through his **desk**. In such a scenario, Alice is not leaving Bob alone. By defining privacy as the right “to be let alone,” however, we may relate privacy to situations which have no true connections to it. If Alice clubs Bob on the head with a baseball bat, she has not invaded his privacy. She has assaulted him. Nevertheless, she has indeed violated his right “to be let alone.”

2.2 Privacy as Control of Information

Fried [4], Westin [5], and Beardsley [6] define privacy as the control of personal information. That is, if we can determine how much personal information we can reveal and to whom we reveal that information, we can prevent violations of our privacy. If Alice rummages through Bob’s desk, finds his credit records, and reveals this information to Charles, then Bob has lost control of his credit information and suffers a violation of privacy. However, while control is an important aspect of privacy, privacy solely as control may erroneously describe instances which do not involve privacy. That is, there are many situations in which people lose or never have control of their personal information yet suffer no violation of privacy. Moor [9] uses the example of medical records. Bob’s medical records may be passed on to various doctors and nurses so that he receives proper medical care. While Bob has no control over this medical information, he does not suffer a violation of privacy.

2.3 Privacy as Undocumented Personal Knowledge

Seeking a better definition of privacy, Parent [7] defines privacy as the condition in which undocumented personal information is not possessed by others. For Parent, personal information consists of those facts which people do not wish to reveal about themselves. It also includes facts about which a person may be very sensitive about, such as weight or height. Undocumented information is any information which cannot be found in public documents such as newspapers or court proceedings. From these definitions, it follows that any personal information which is documented must have once been undocumented. Parent acknowledges that when personal information is first published, there is an invasion of privacy. He calls later uses of such information “gratuitous exploitation” rather than further violations of privacy. Suppose Alice is sunbathing naked on her private beach. If Bob takes a photograph of Alice and Star magazine prints the photograph, this personal information now becomes documented information. According to Parent, knowledge of Alice’s nude body is now publicly available, and therefore no privacy is lost the next time someone sees Alice nude. This conclusion seems counterintuitive to us.

2.4 Privacy as Restricted Access

Perhaps the most complete conception of privacy is based on restricted access, due to Gavison [8]. She introduces three aspects of privacy: Secrecy: The extent to which we are known to others. Anonymity: The extent to which we are the subject of others’ attention. Solitude: The extent to which others have physical access to us. A loss of privacy occurs when the degree of our secrecy, anonymity, or solitude decreases. Gavison makes an important distinction between the loss of privacy and the violation of privacy. That is, losses of privacy are not necessarily undesirable. Each situation must be assessed to determine whether the loss of privacy limits the functions of privacy. For Gavison, such functions of privacy include the following:

1. The creation of an environment where trust, love, friendship, and intimacy can be maintained.
2. Freedom from physical access.
3. Promotion of liberty of actions. By this we mean that privacy permits individuals “to do what they would not do without it for fear of an unpleasant or hostile reaction from others.” Specifically, it promotes our mental health and autonomy and protects us from censure and ridicule.

Moor [9] also adopts the framework of privacy as restricted access. He describes two kinds of privacy: natural privacy and normative privacy. Loss of natural privacy is not necessarily an invasion of privacy. If Bob is meditating in the Grand Canyon, he is enjoying his state of natural privacy. If a group of noisy tourists riding mules descends upon him, however, he cannot claim an invasion of privacy. On the other hand, Bob may be relaxing in his New York apartment, smoking a pipe and reading the paper. If the same

group of noisy tourists riding mules peers into his window, they are violating his normative right to privacy.'

2.5 The Value of Privacy

These different theories agree that privacy is an important part of our lives. The value of privacy has been described both as a means to achieve or maintain other important goals of our lives and as an end, having intrinsic or 'inherent value, itself *Rachels*[10] considers privacy as a means. For him, privacy is important because it enables us to create social context in our relationships with other people:

The value of privacy is based on the idea that there is close connection between our ability to control who has access to us and who has information about us, and our ability to create and maintain different sorts of relationships with different people. For instance, Bob may be aggressive, relentless, and unyielding in dealing with his business partners. At the same time, he may be tender and sensitive with his family and friends. Privacy, as a means, allows us to exhibit different patterns of behavior with different people, to maintain different social relationships. *Benn* [11] argues that privacy has intrinsic value. He claims that there is a general principle of privacy based on respect for persons. He begins by stating that people have a general liberty to do what they choose unless someone else has good reason for preventing it.'

For *Benn*, the principle of privacy offers such a reason to limit the general liberty of others to observe and report at will. For instance, imagine that Bob is unhappy that Alice is watching him. Bob's behavior is fundamentally changed by the mere fact that he knows Alice is watching him. Such unwanted observation does not treat Bob with the respect he deserves. Suppose, on the other hand, that Bob did not know that Alice was watching him. He would behave as if he were being unwatched, which is not the way he would want to behave. Covert observation is objectionable, as *Benn* states, because it deceives Bob about the context of his actions and treats him without dignity.

3 Ethical Theories of Informed Consent

Many violations of privacy could be avoided if an element of consent or awareness was introduced. Consider again, for example, the scenario presented in Section 2.3 about the theory of privacy as undocumented knowledge. The main problem, it seems, is that Bob did not ask Alice if she would mind being photographed. Similarly, Alice did not ask for permission before she rummaged through Bob's desk in Section 2.1. In Section 2.2, Alice did not think about Bob's feelings before she blurted out his credit record to all her friends. In each of these scenarios, had the victim been properly informed and given a choice, a violation of privacy might not have occurred. Consideration for the victim is the essence of the theory of informed consent.

To our knowledge, previous accounts of privacy have not emphasized the role of consent. Instead, they attempt to define precise boundaries around privacy. These accounts explain privacy by defining the circumstances under which an individual's privacy has been compromised. That is, they isolate the concept of privacy solely as an issue of safekeeping information, without consideration of social context. For example, *Parent's* [7] conception of privacy as undocumented knowledge precisely delineates what is private (undocumented personal knowledge) and what is not (documented personal knowledge). By introducing the concept of consent, our approach in this paper is to emphasize the concept of privacy as an aspect of the social relationship between individuals. Had Alice consented to being photographed after being fully informed about potential consequences, we do not believe she would have still suffered an invasion of privacy. Our approach essentially builds upon *Gavison's* [8] neutral concept of privacy. Recall her argument that different situations must be examined to determine whether a loss of privacy results in a violation. We will argue in Section 4 that linking consent to privacy provides a framework for deciding whether a loss of privacy may be a violation of privacy. In the following sections, we present a brief summary of the theory of informed consent in both medicine and engineering.

3.1 A Brief History of Informed Consent

The theory of informed consent has been most developed in the medical ethics. Historically, physicians did not believe that the consent of the patient was necessary. Consider *Hippocrates's* advice to future physicians. Perform [these duties] calmly and adroitly, concealing most things from the patient while you are attending him. Give necessary orders with cheerfulness and serenity, turning **his attention** away from what is being done to him; sometimes reprove sharply and emphatically, and sometimes comfort with solicitude and attention, revealing nothing of the patient's future or present condition. The term "informed consent" first appeared in 1957 in the decision *Salgo v. Leland Stanford, Jr. University Board of Trustees*. In that case the court asked whether the patient had been adequately informed before consenting to the medical procedure. By the 1970's and 1980's, concerns with civil rights, women's rights, the consumer movement, and the rights of prisoners and the mentally ill had brought informed consent to the attention of the medical community.

3.2 Informed Consent in Medical Ethics

Faden and *Beauchamp* [12] present five basic elements necessary for informed consent in medicine. Disclosure: All pertinent information must be disclosed to the patient before he makes a decision. This includes information which the patient may not have requested. Comprehension: The patient must understand the general nature of the illness, the risks and benefits of each treatment, and the reasons for and

against these options. **Voluntariness:** The patient should be under no pressure or duress when making the decision. **Competence:** The patient should be able to take responsibility for making the decision (not a child or someone who is severely mentally ill). **Consent:** The patient must be given the choice to decide which alternative to take. Gorovitz [13] feels that informed consent is necessary: If the patient understands what the physician proposes to do, and thus informed, consents to its being done, then the medical intervention is not imposed on the patient in violation of the patient's autonomy; rather, that medical intervention is properly viewed as a service provided to the patient at the patient's request. By providing the patient with a choice in his own treatment, informed consent promotes individual autonomy and encourages rational decision making. It also protects the physician against charges of assault from a patient who did not want a particular treatment. Like the theory of privacy, the theory of informed consent is formally grounded on the principle of respect for persons.

3.2.1 *Against Informed Consent*

Some physicians believe that informed consent is not only impractical, but may even be detrimental to the patient. They argue that it is not possible for the patient to develop a **sufficient** comprehension of the illness as dictated by the doctrine of informed consent. After all, physicians go through years of medical school and residency to develop such an understanding. Further, physicians have neither time, skills, nor sensitivities to properly inform a patient. Additionally, studies have shown that patients, even when properly informed, often do not remember what they have been told. Most likely, these physicians argue, the patient did not want to be given so much information in the first place. It is also argued that obtaining informed consent may even be dangerous to the patient. With limited understanding, patients may make decisions which are detrimental to their own well-being. They may even develop unnecessary fears and anxieties from a more thorough understanding of the potential risks and discomforts of the treatments. None of these arguments seem strong enough to counter the principle of respect for persons. In fact, a wrong "medical" decision may not be the wrong decision from a broader perspective of the patient's life. For example, Bob may decide to forgo an operation on his larynx because he makes his living as an opera singer. While his decision may be medically unwise, Bob knows that such an operation would ruin his career and even his life. As Gorovitz [13] writes, "the right to choose is not limited to the right to choose rightly."

3.2.2 *Exceptions to Informed Consent*

Lidz [14] identifies situations in which it may be acceptable not to obtain informed consent: **Emergency:** There is not enough time to obtain informed consent without seriously risking the well-being of the patient. **Incompetence:** The pa-

tient is unable to make a decision for the situation at hand. The patient may be, for instance, intoxicated, unconscious, or senile. In such a situation, it is appropriate to secure a surrogate who may make decisions for the patient. **Waiver:** Under no pressure to do so, the patient waives the right to informed consent. **Therapeutic Privilege:** This exception allows the withholding of information that the physician feels would be "harmful." Therapeutic privilege prevents violation of the physician's primary duty of doing what is beneficial for the patient solely because of a legal duty to obtain informed consent. Unfortunately, many different interpretations of this privilege exist, ranging from the most stringent to the most lenient.

3.3 Informed Consent in Engineering Ethics

Martin and Schinzinger [15] bring the theory of informed consent into the area of engineering ethics. They believe that socially responsible engineers must consider the informed consent of those who will use their products. Engineers should realize the consequences of designing and manufacturing a product. Customers must be given all pertinent information about a product so that they can rationally decide whether to purchase it. For instance, if Bob creates a new security device which identifies employees by scanning their retinas with a laser, he must reveal all the risks as well as benefits to those who are interested in the device. Martin and Schinzinger emphasize that information must be voluntarily presented even if the customer has not requested it. Therefore, even if the customer is not interested, Bob, as a responsible engineer, would be obligated to reveal the risks of his product.

4 Collection of Information

Computers have entirely changed the way we collect information. According to Johnson [16], not only has computer technology increased the scale of information gathering, it has also enabled new kinds of information to be collected. Without computer technology, for instance, the scientific information collected from NASA's recent Mars mission would not have been possible. In today's modern environment, we would likely find it impossible to eliminate or even limit the collection of personal information. Rather, our efforts should concentrate on balancing the privacy rights of the individual with the needs of the community to collect information. In this section, we link previously discussed theories of privacy and consent to provide a framework for determining when the act of collecting personal information is ethical.

4.1 Distinguishing Collection from Use

It is important to distinguish the collection of personal information from its use. When we do not distinguish collection from use, we may easily blame the tool which collects information for undesired consequences. Mainstream mov-

ies such as The Net and Hackers have popularized the notion that computers and the Internet are the root of privacy and information problems. Numerous individuals have been arrested or denied service because databases contained incorrect or inaccurate information. For example, according to Forester and Morrison [17], Barbara Ward was continuously refused accommodation by landlords because her name was in a database of names of people who had taken their landlords to court.³ Quittner [18] mentions examples of computer misuse, including Sara Lee's plan to collaborate with Lovelace Health Systems to match employee health records with work performance reports to find workers who might benefit from antidepressants. These examples, however, do not reveal anything about the actual ethics of the collection of information. They are, rather, consequences of the use or misuse of collected information.⁴ While it is important to examine ethical decisions in the use of information, we wish to explore the ethics of the act of collecting personal information.⁵

4.2 When Is Collecting Personal Information Ethical?

When does the collection of information result in the loss of privacy? Under Gavison's definition of privacy as restricted access, the collection of information results in a loss of privacy when our degree of secrecy or anonymity is compromised. We might term the collected information which results in such a loss of privacy as personal information. Nevertheless, such a loss of privacy is not necessarily a violation of privacy. Recall Benn's assertion [11] that privacy can be justified under the respect for persons argument. Therefore as long as the principle of respect for persons is maintained, the collection of personal information can indeed be ethical. Consider the question raised by Benn [11]: How reasonable is it, then, for a person to resent being treated much in the same way that a birdwatcher might treat a redstart? It is reasonable for Bob to resent being watched like a bird because he has no knowledge that he is being watched. Even if Bob knew he was being watched, he probably would not like to be treated like an animal or specimen. Likewise, Bob probably would not be happy if someone read his private journal (a collection of personal information) without his permission. In all these examples, poor Bob is being treated neither with proper respect nor with regard for his dignity. One way to collect personal information from Bob while still treating him with proper respect is to obtain his informed consent. Section 3.2 discussed the basic elements needed for informed consent in medical ethics. When we extend informed consent from medicine to the collection of personal information, the elements of disclosure and comprehension must include the consequences of revealing or not revealing personal information: how the information will be used, who will have access to the information, how long the information will be kept, etc. Only with this information can a truly informed choice be made. If Bob understands the

reasons we would like to obtain his personal information and knows the consequences of revealing such information, then he can make an informed choice whether to divulge such information. Obtaining Bob's informed consent shows that we respect him as an autonomous being capable of making rational decisions. Both the theory of informed consent and the theory of privacy can be grounded on the principle of respect for persons. Since informed consent preserves this principle of respect for persons, it ensures that a collection personal information will not result in a violation of privacy. 4.3 When Is Collecting Personal Information Unethical? Does collecting personal information without obtaining consent necessarily result in a violation of privacy? That is to say, while obtaining informed consent satisfies the principle of respect for persons, a lack of informed consent may not necessarily show a disregard for it. Recall Benn's [11] assertion that only a general principle of privacy can be based on the principle of respect for persons: General principles do not determine solutions to moral problems of this kind. They indicate what needs to be justified, where the onus of justification lies, and what can count as justification [11]. Such a general principle offers only a minimal right to immunity.⁶

We believe that the concept of a reasonable expectation of privacy answers Benn's questions of what needs to be justified, where the onus of justification lies, and what can count as justification. For instance, in order to show that Alice should not be able to observe Bob on grounds of general liberty, Bob must have a reasonable expectation of privacy not to be observed in that situation. If Bob does not have a reasonable expectation of privacy, then Alice does not need to justify her desire to observe Bob, and therefore obtaining informed consent does not seem necessary. If, however, Bob does have a reasonable expectation of privacy, and Alice still insists on observing him, then a violation of privacy does occur. In this case, Alice has collected personal information in an unethical manner. Informed consent can transform a potentially unethical collection of personal information into an ethical one. A collection of personal information is unethical when it does not comport with the reasonable expectation of privacy for the situation at hand. Obtaining informed consent in these situations is necessary to avoid violations of privacy. Not all collections of personal information exceed the boundaries of a reasonable expectation of privacy, however. That is, obtaining informed consent may be sufficient for an ethical collection of data, but it is certainly not necessary. Alice does not need Bob's informed consent to watch him walk through a public square because Bob's reasonable expectation of privacy in this situation is limited. He would not reasonably expect that his right to privacy would protect him from observers as he walks through a public square. Suppose, however, that Alice peers into Bob's apartment window. Such an action obviously does not fall within Bob's reasonable expectation of privacy. Alice is en-

gaging in an unethical collection of personal information, and therefore violating Bob's privacy. Had Alice requested permission to observe Bob, however, a compromise may have been reached. Thus, Bob may risk the loss of privacy, if Alice seeks prior consultation before her attempt to observe him. In such a situation, the principle for respect for persons is preserved, Alice is free to conduct her observations, and Bob does not suffer a violation of privacy.

5 Centralization of Information

In Section 4, we established that the collection of personal information does not necessarily result in an unethical loss of privacy. Specifically, if Bob gives his informed consent before releasing any personal information, the loss of privacy which he experiences is not a violation. When Bob does give his informed consent, he essentially weighs all the perceived costs and benefits and concludes that the desirable functions of privacy (environment for maintaining relationships, freedom from physical access, and liberty of actions) are still preserved. In this section, we distinguish the act of collecting information from the act of centralizing information. By centralization of information, we mean the process of aggregating large quantities of personal information which have been collected for different purposes, and using this aggregation of information for an entirely new purpose. We will argue that the centralization of information, in contrast to its collection, is unethical because centralization contravenes the desirable functions of privacy identified in Section 2.4.

5.1 Creation of a Dossier Society

In 1986, Laudon [20] warned about the danger of the dossier society, in which personal files from different government agencies are integrated into a permanent national database. Advances in technology in addition to the government's loose interpretation and enforcement of the protections of the Privacy Act of 1974 had made the dossier society a real possibility. Not only did the development of a dossier society threaten the traditional American desire for a limited role in government, it had harmful cultural consequences as well:

From the individual's point of view, the most significant characteristic of the dossier society is that decisions made about us as citizens, employees, consumers, debtors, and supplicants rely less and less on personal face-to-face contact, on what we say, or even on what we do. Instead decisions are based on information that is held in national systems, and interpreted by bureaucrats and clerical workers in distant locations. The decisions made about us are based on a comprehensive "data image" drawn from diverse files [20].

What concerned Laudon most was the aggregation of power that a dossier society would bring to the federal gov-

ernment. He feared the necessity of explaining an "official life" to any government official who demanded such an explanation. Such concerns led him to criticize the potential development of the FBI's plan to create a national computerized criminal history into a general purpose national information database. Twelve years later however, we realize that fears about the dossier society are not limited solely to "official" information held by the federal government. The integration of commercial databases in industry has also created a de facto national database which is less official and more personal, even detailing preferences and habits. Culnan and Smith [22] describe the public uproar in 1991 over Lotus Marketplace: Households, a CD-ROM database which contained information, including lifestyle and purchasing propensities, of 120 million individuals in 80 million U.S. households. In June 1996, Lexis-Nexis launched its P-Trak service, advertised as the digital equivalent of the phone directory [23]. The P-Trak service, again, caused public concern because it gave access to Social Security Numbers. Within days of its launch, Lexis-Nexis, realizing the potential dangers of revealing such personal information, removed access to the Social Security Numbers.

5.2 Economic Theory of Information

The Lotus Marketplace: Households and Lexis-Nexis P-Trak controversies showed that centralized information could be easily accessible to everyone. Economic theory suggests that the cost of acquiring information guides behavior. For instance, if the perceived cost to Bob of learning how to select the very best apple in the supermarket is greater than its perceived benefits, Bob may decide to select a relatively good apple rather than the very best. Decreasing the cost of acquiring information, easily accessible databases increase the chance that persons will search for information that they would not otherwise seek because the cost would have been too high. Because there is such a low cost for obtaining the information, people may even acquire information which is neither pertinent nor reliable for the decisions they need to make. Imagine if Bob's business competitors and his intimate friends could easily obtain the same comprehensive data image which detailed not only his tax and credit records but his culinary preferences and purchasing habits as well. Easy access to an integrated federal and industry database seems devastating to our notions of privacy.

5.3 Violation of Privacy Without Loss of Privacy

Is there an ethical basis to our fear of the centralization of personal information? To the extent that no extra information is collected in the centralization process, how can there be any additional loss of privacy? While there may not necessarily be a loss of privacy, there is an unethical violation of privacy. Samet's [24] points out that we consider it a violation of privacy if Bob looks into our window and takes note of what we are doing. However, we experience no violation

of privacy if Bob looks out of his own window and notices what we are doing **outside**.⁹

In addition, let's assume all of Bob's family and friends also record what they see about us out their windows. Later that week, they all get together to share and compare notes. There is something disturbing about the detailed personal profile that Bob's family and friends would be able to compile.

According to **Rachels**[10], privacy is important because it provides the proper context for us to create and maintain different sorts of relationships with different people. Centralization of personal information is unethical because it destroys this important context which privacy provides. The comprehensive data image created in a centralized database denies us the ability to engage in the "different patterns of behavior associated with different relationships." While we have not consented to divulging certain information to certain parties, all parties who use the comprehensive data image can acquire that information. We might even say that a comprehensive data image is a portrayal of person that really does not exist. That is to say, at no single moment in time, do we display all behaviors that may be revealed in the comprehensive data image. Rather, we maintain different faces and behaviors in different contexts and relationships. Further, such a comprehensive data image permits subsets of information that are not personally or socially meaningful. The centralization of information creates an unsound profile because it takes information out of its original context and uses it in a different context. While certain information may be accurate in the context for which it was initially collected, it may be inaccurate when it is moved into a different context in a process of centralization. We may observe Bob as a careless free spirit at the racy nightclub which he frequents on the weekends. This certainly does not mean that he exhibits the same characteristics in his decisions as CEO of his company or as a father to his children. For these reasons, we conclude that centralization violates privacy. By changing the context in which information was initially collected, it counteracts a key function of privacy: the ability to create and maintain different relationships." 5.4 Informed Consent and Centralization of Information In section 4.3, we suggested that obtaining informed consent is sufficient for an ethical collection of information. How does obtaining informed consent affect the centralization of information? As discussed in the previous section, we believe that the centralization of information is *prima facie* unethical. Unlike the collection of information, which can be ethical even without obtaining informed consent, there are no conditions under which centralization of information can be ethical without obtaining informed consent. In fact, in situations where personal information is centralized, it is often impractical or impossible to even obtain the informed consent of the individuals.

For example, **Parker** [25] describes the ethical conflict faced by a scientist who finds two different kinds of data on the same subject pool. The scientist believes that there would be significant scientific value in merging and analyzing the data. Unfortunately, while informed consent had been obtained from the subject pool for collecting their personal information for the earlier studies, the subjects have now dispersed, and it is impossible to obtain their informed consent for this centralization of information. By merging the data, the scientist would be unethical. Parker suggests that the solution is to obtain the informed consent of a proxy, or representative of the subject pool, such as an independent committee. The proxy would weigh the benefits of the research against the violation of privacy to decide whether the merging should be allowed.

Parker's solution of a proxy may be sufficient for his scenario because the amount of centralization is small. We do not believe, however, that the solution of obtaining informed consent through a proxy can be extended to scenarios with large amounts of centralization. That is, when the scale of centralization is large enough to create a digital dossier, it is unlikely that an individual will consent to such a portrayal. Such profiles are dangerous because the superfluous information they provide affects how decisions are made. Furthermore, large scale centralization of information is a violation of privacy because the data images it creates are used out of context, and counteract the ability to create and maintain different relationships.

6 Reasonable Expectations of Privacy in Public Places

From the foregoing discussion, it does not seem that we necessarily have a *prima facie* right to privacy outside of that based on **Benn's** general principle of privacy. In fact, **Ware** [26] suggests that society will not and should not protect an individual's privacy at all costs. There is inevitable conflict between an individual's right to privacy and a community's rights. Such conflict may be manifested in monetary terms, inefficiencies to systems, or denial of desirable social services. This awareness of community rights is particularly pertinent to the right to privacy in public places, a concept introduced by **Nissenbaum** [27].

6.1 Privacy in Public Places

For **Nissenbaum**, current theories of privacy (Section 2) do not adequately address the relevance of privacy in realms other than the intimate and personal. Previous works on privacy ([4],[5],[6],[7],[28]) attempt to define a distinct and mutually exclusive boundary between an intimate personal realm where privacy is protected and a public realm where privacy has no relevance and all information is available to everyone. **Nissenbaum** [27] points out that while "there is a broad consensus on what information may be classified

personal and intimate, there is, on the other hand little, if anything, that people universally would admit into a completely public realm if by that we mean that it is governed by no norms of privacy whatever.” Rather than viewing a context as purely private or purely public, we might view the context as having both private and public elements. Nissenbaum criticizes the notion that there is a relationship between a place and information which might be obtained in that place. That is, we should not assume that information is public simply because the place in which it was obtained is public. For instance, “shoppers may not object to using open shopping carts but may sense violation if inquisitive neighbors noted and reported on their purchases” [27]. For Nissenbaum, a conception of privacy should extend consideration to all information, including information which is obtained in public places.

6.2 Reasonable Expectation of Privacy

The protection of privacy in public realms cannot be as strong as in intimate realms. While we should extend consideration of privacy to the public realm, we must also acknowledge the limitations of privacy in the public realm. Moor’s [9] concept of a naturally private situation captures the essence of the limitations of our right to privacy. A naturally private situation seems to be nothing more than the experience of isolation in a public place. Recall the sudden interruption of Bob’s peaceful meditation in the Grand Canyon by the rude mule riding tourists. Although the intrusion is annoying and unfortunate, Bob has no right to privacy in this public place. The protection of privacy in such a public realm is limited, and his loss of privacy cannot be a violation.

How, then, do we determine what is reasonable in our expectation of privacy in public places? Bob may experience a loss of privacy when he purchases some books at the local bookstore because the bookstore may record Bob’s purchasing preferences for inventory purposes. Such a collection of personal information would reduce Bob’s secrecy and anonymity. The collection of this information seems reasonable because such public transactions are a necessary aspect of everyday life in society. Nevertheless, Bob may also reasonably expect that the information obtained by the bookstore will not be shared with third parties because such sharing was not the initial purpose for collecting the information. Our expectation of the protections of privacy should consider the needs of society’s other entities such as industry, government, and community. A reasonable expectation is one which considers the practical harms which accompany a loss of privacy. That is, a claim of privacy seems reasonable only if there might be potential harm caused by the loss of privacy. For instance, Bob’s claim of privacy would not be reasonable if Alice merely observed the nice red shirt he was wearing. A reasonable expectation of privacy should also consider the dynamic nature of the hierarchy of rights: depending upon the context of the situation, there may be other

intrinsic principles and rights which may be more important than privacy. When Bob is in his house, his right to privacy may take precedence over Sally’s right to observe him. If he is in a public square, however, Sally’s general liberty to observe may take precedence over Bob’s right to privacy. Another example of the dynamic nature of rights is the revelation Bob’s past history of drug addiction in his criminal trial. In normal circumstances, such a revelation may be inappropriate and a violation of Bob’s privacy. In a criminal trial, however, the principle of social justice takes precedence over the principle of individual privacy. Reasonable expectations of privacy in public places must change as our social environment changes. Having expectations of privacy is particularly relevant when we consider the effects of the fast pace of information technology on our moral norms. For instance, until 1967, when the Supreme Court decided in *Katz v. United States*, that telephone conversations should be private, some considered these conversations to be property of those who owned the telephone equipment. In response to the publication of Robert Bork’s videotape rental records in the newspaper, the Video Privacy Act of 1988 reversed the status of video rental records from public to private [27]. More recently, the Violent Crime Control and Law Enforcement Act of 1994 limited access to drivers’ records, which were previously regarded as public records [“no-holds barred”] [27]. Our use of information technology will continue to reveal new issues of privacy in public places, shifting our societal judgments and affecting our moral norms. Our expectations of privacy will change with such developments.

7 Privacy and the Internet

We maintain that the Internet, in its current state, is a public place. Recall Nissenbaum’s separation of place from information [27]. That is, although we may be sitting in a private place (our own homes), when we access the Internet, we are engaging in transactions and exchanging information with other entities (companies, government, educational institutions, etc.) which are definitely not part of our intimate and personal realms. Although we may be in a physically private location, the transactions that take place on the Web strongly parallel those transactions that occur every day in our public lives. If the Internet is a public place, what then should be our reasonable expectations of privacy? Currently, reasonable expectations of privacy on the Internet are neither formally rooted nor well developed. Because Internet technology facilitates the manipulation and collection of information, losses of privacy occur continually, and unfortunately, it is often difficult to determine what constitutes an ethical or unethical collection of data. For example, each time Bob views a page on the Web, that Web site collects several important pieces of information about him: the name of his computer, the time of the request, and the address of the previous Web page he was viewing. As previously discussed,

one way to avoid the **unethical** collection of personal information is to obtain informed consent. But obtaining informed consent every time Bob moves to a different Web site would be impractical.

It is helpful to compare new Internet situations to more familiar situations, in which our expectations of privacy are better developed. For instance, is making a purchase, on the Web similar to purchasing a candy bar from a **vending** machine? Or is it more similar to purchasing a candy bar from the local supermarket? In order to purchase something on the Web, we must release personal information such as our name, address, and perhaps credit card information. The analogy of the supermarket, then, seems more appropriate than the vending machine. Because we release personal information to a supermarket when we apply for discount cards, we would reasonably expect the supermarket to track our purchases for the purposes of maintaining customer satisfaction and proper inventory. Likewise, we might reasonably expect similar forms of information collection from a Web site.

Such analogies can take us only so far. What should the reasonable expectations of privacy be when we visit virtual galleries or adult sites on the Web? Are and should we be afforded complete anonymity when engaging in online chat groups? It may take time before our moral norms develop in this new Internet context. As we discover new situations in which privacy may be violated on the Internet, we will continue to adjust and reformulate our moral norms.

8 Internet Cookies

Internet cookies provide a test for our claims about the collection and centralization of information. Since early 1996, when an article in the San Jose Mercury brought cookies to public awareness, there has been much concern over cookies' effect on our privacy [29]. Nonetheless, popular sentiment, like the following statement expressed on a public message board on the Internet, demonstrates a failure to distinguish the tool from its use (see section 4.1): I hate cookies. .. They [those who use cookies] may think it's harmless but they are taking something without permission and without payment [30]. Although reasonable expectations of privacy on the Internet are not yet well developed, in this section, we offer an interpretation of a reasonable expectation of privacy with regard to the use of Internet cookies. Once the public has developed a reasonable expectation of privacy for cookies, we can determine what uses of Internet cookies require informed consent. We will show that some uses of cookies are morally permissible while other uses are immoral. Based on our analysis of the collection and centralization of information and our discussions of public places and reasonable expectations, we will identify the conceptual muddles which cookies present and explain how cookies can be used in both morally permissible and unethical ways.

8.1 What are Internet Cookies?

When we visit a Web site, that Web site may give our Web browser a block of text, which is usually a name, value pair. On each subsequent visit to that Web site, our browser sends that specific block of text back to the Web site. Upon receiving that text, the Web site can act in a variety of ways. For instance, it recognizes our browser as a repeat visitor, and may provide us with customized service. It can also change the value of the block of text depending on our behavior at that Web site. Our Web browser remembers this block of text, commonly known as a cookie, by storing it on our hard drive. Not all cookies store information on our hard drives. Transient cookies are stored in the memory of the computer only for the duration of the current web browsing session. For example, Bluestem, the WWW Identification Service at the University of Illinois at Urbana-Champaign uses these transient cookies to store authentication information once users have logged onto the secure system. Mallard, a Web based interactive learning environment developed at the University of Illinois also uses cookies in its authentication system."

In both cases, the cookies are removed when the user logs out of the system or quits the Web browser. Because these transient cookies seem to pose no apparent ethical problems, the remainder of this paper will focus on the persistent cookies, which are stored on a user's hard drive.

8.2 Argument Against Cookies

Mayer-Schoenberger [31] presents four major reasons why cookies are an invasion of our privacy. In this section we show that the conceptual muddles created by cookies weaken his argument against them.

Cookies are stored on the user's computer without his consent or knowledge. The typical computer user also has no knowledge that cache files, temporary files, and log files are being stored on his computer. In fact, most of these files fill much more space on the hard disk than the small **block** of text of a cookie. This objection, then, cannot be about cookies, but **about** the use of computers and technology in general. We might think of a computer as an incomprehensible system. That is, just as we do not necessarily know how our automobile transmission operates, we cannot know about everything which occurs in our computers. In the automobile, we don't need the driver's consent to shift gears. Similarly, we probably do not need consent for a program to store a small **file** on our hard disk. In fact, it would be counterproductive to our use of computers if we were informed every time an application wanted to change the internal state of our computer. The advantages of Web technology seem to far outweigh the tiny harm of a small block of text set on our hard drive. The cookie is clandestinely and automatically transferred from the user's machine to the Web server. The typical computer user is unaware of much information which is automatically transferred from his computer into the **net-**

worked world. Each time we visit a Web site, for instance, our computer transmits much information to the Web server including our IP address, the current time, and the previous Web page we were visiting. If our computer is linked to the networked world, it is, without our knowledge, continuously transferring information about its location and existence to other computers. E-mail is not sent directly to the intended receiver, but is automatically transferred through numerous machines of which we have no knowledge. Such automatic transferral of information is essential to our use of current technology. Because cookies allow the Web server to set an expiration date, they violate the “accuracy” and “timeliness” principles in the European Union Directive on the Protection of Personal Data. This argument seems to mistake the tool for its use. In fact, the expiration date option allows the realization of the accuracy and timeliness principles. Of course it is possible for someone to abuse this option thereby violating the principles in the Directive. The cookie, itself, does not violate the principles.”

Once the cookie is set, it is freely accessible to Web servers. This argument is technically inaccurate. Only the Web server which set the cookie can access that cookie. Additionally, no other Web server would understand or have use for the cookie except the Web server that set it.

8.3 Morally Permissible Uses of Cookies: Collection of Information

It is important to keep in mind that cookies are merely a tool which is used to collect personal information. As we have discussed previously, the collection of personal information does not necessarily result in a violation of privacy. Imagine that Bob visits his local grocery store. When Bob enters the store, Carol, the store-keeper, immediately recognizes him as a valued repeat customer. She greets Bob with a firm handshake and shows him the new shipment of ripe apples, Bob's favorite fruit, which just arrived. Bob fills his shopping cart with the best fruits and vegetables he can find. He purchases his goods, and takes off down the street, munching on a delicious newly purchased apple. The fact that Carol recognized Bob and remembered what he liked would be considered “doing good business” on the part of Carol. Each time Bob has visited her store, Carol has noticed what types of fruits and vegetables Bob likes to buy. Bob returns to Carol's grocery store because he appreciates the customized service he receives there. When cookies are used for site personalization and online ordering systems, they are an effort to “do good business” on the Web. There are benefits for both the Web site and the Web customer. If Bob likes the ease of service and the personal attention he receives at a Web site, he may return there often. In these situations, the collection of information performed by cookies does nothing more than mimic the memory of Carol. As a repeat customer to Carol's grocery store, Bob has implicitly consented to having Carol remember his preferences.

That is to say, Bob's reasonable expectation of privacy in this scenario is that Carol may recognize him after multiple visits. Likewise, since a large component of the Internet parallels similar purchasing scenarios, it is also within a reasonable expectation of privacy for a Web site to recognize Bob as a repeat visitor. In both cases, the information collected by Carol or the cookie does not result in a violation of privacy because of Bob's reasonable expectations as a repeat customer. Notice that outside the grocery store, Carol knows nothing about Bob. She may not even know Bob's name. Similarly, cookies are useful to a Web site only when we visit that Web site. The Web site may recognize Bob only as someone who has visited before. It does not know his e-mail address, phone number, or home address unless he has explicitly given the Web site such information. Garfinkel [33] describes how cookies may, in fact, be used to protect privacy. Used properly, cookies can eliminate the need for central data banks. Generally, a cookie is a unique number which is used to reference a databank of information stored at the Web site. For instance, Bob may have a cookie which has the value 007 stored on his computer. When Bob visits the Web site, his Web browser sends the number 007 to the site. With that number, the Web site can look up information in its databank and find out that visitor 007 has visited ten times before and likes to read the articles about the apple industry which are available on the site. However, as Garfinkel describes, rather than using the cookie as a unique identifier, the actual preferences might be stored in the cookie itself, eliminating the need for a central databank. For instance, instead of a cookie which has the value 007, the cookie might now consist of:

visits = 10; articles = apple

Therefore, when Bob leaves, he takes his cookie filled with personal preferences with him, leaving the Web site unable to remember anything about him until he returns.¹³

8.4 Immoral Uses of Cookies: Centralization of Information

Not all uses of cookies are ethical. The use of cookies by the target marketing industry to track our behavior on the Internet is an attempt to centralize personal information. In Section 5, we criticized the centralization of information for taking information out of its intended context and putting it in a new, foreign context. Target marketers' use of cookies is a special case of centralization of information. Their initial purpose in the collection of information is the centralization of information. Target marketers have developed a technique to track us all over the Internet by adding cookies to the advertisement banners on so Web pages. Such uses of cookies do not seem to fit within a reasonable expectation of privacy on the Web. Consider the following scenario: Bob visits the Web site www.dailynews.com to read about the happenings of the day. On that page, he notices an advertisement banner for Jazzy Widgets. The advertisement banner was placed on the www.dailynews.com Web page by a target

marketing company named Banners-R-Us. Unknown to Bob, as he is reading the daily news, a cookie has just been set on his computer by www.bannersrus.com (not www.dailynews.com!). After he finishes reading the news, the www.dailynews.com site asks him to register for additional access to the site. Bob happily divulges his name, e-mail, phone, and address because he has enjoyed the Daily News site. However, he does not consent to sending that registration information to Banners-R-Us. Bob completes his visit at www.dailynews.com and decides to visit his favorite online compact disc shopping site, www.columbiahut.com, to purchase some new CDs. At www.columbiahut.com, he notices an advertisement banner for Classical Widgets. Again, the Classical Widgets banner was placed at the Columbia Hut Web site by Banners-R-Us. Again, through the advertisement banner for Classical Widgets and unknown to Bob, the Banners-R-Us cookie previously set at www.dailynews.com is sent to www.bannersrus.com. Banners-R-Us now knows that Bob enjoys reading the news at the Daily News site and purchasing CDs at the Columbia Hut site. If it received any of the registration information Bob gave to the Daily News site, it may even be able to connect his name and e-mail address with his Web browsing behavior [34]. Banners-R-Us will continue to track Bob and gather information about his browsing behavior wherever he bumps into advertisement banners placed by Banners-R-Us on the Web.

The use of cookies to track users as they move from site to site is an unethical invasion of privacy. Such use violates our privacy because it creates an undesirable loss of anonymity and secrecy. No consent has been obtained by target marketers before they collect information about us. Recall from Section 4.3 that the lack of consent does not necessarily render an act unethical. In this cookie case, however, consent seems necessary to legitimize the collection of data. The reason is that such a setting of cookies does not fall within the realm of our current reasonable expectation of privacy for the Web. The cookies set by target marketers differ significantly from those set at a Web site we are actually visiting. When we visit a Web site, it is reasonable to expect that site to collect information about us (recall the example with Carol the storekeeper). When Bob frequents a Web site, he is actively establishing a relationship with that site. With target marketers, however, Bob has no intention nor inclination to establish a relationship with them. For them to obtain information about him without his consent, then, is beyond a reasonable expectation of privacy.

In Section 8.3, we mentioned that a Web site cannot obtain a user's e-mail address, phone number, or home address by setting cookies. According to Cranor [32], however, "multiple Web sites sometimes share access to cookies. A user who reveals personal information to one Web site may unwittingly reveal that information to other sites." Specifically, if Web sites have agreements to share information

with target marketers which have advertisement banners on those sites, information which users may reveal to that particular Web site through registration forms may ultimately be linked to their Web browsing behavior, obtained by target marketers through their use of cookies to centralize information. This is one technique which might be used to generate lists for unsolicited bulk e-mail.

8.5 Cookies and Consent

In section 8.4, we argued that the setting of cookies by target marketers is immoral because such a collection of information is not within a reasonable expectation. We have argued that consent is necessary when a collection of personal information does not comport with a reasonable expectation of privacy.

During the early stages of this paper, the current version of the Netscape Web browser, Netscape Navigator 3.01, had the option to set a "cookie alert" which would warn the user when a site wanted to set a cookie. The alert notification would give the user the option of either accepting or rejecting that cookie. The default setting of Netscape, however, was to accept all cookies unconditionally. Furthermore, there did not exist an option to completely reject all cookies.

Currently, the new Netscape Communicator 4.04 has extended its cookie options. Not only can users set the "cookie alert" option, they also have options to accept all cookies, only cookies that are returned to the originating server, or completely disable cookies. Notice that the option to accept only cookies that are returned to the originating server distinguishes our morally permissible and immoral cookies. The default setting, however, remains the unconditional acceptance of all cookies.¹⁴ In addition, these cookie warnings appear only when a Web site desires to set a cookie on a user's hard drive. Technically, no loss of privacy has occurred at this point. Loss of privacy occurs later, when the cookie is collected and transmitted back to the Web site on subsequent visits. Users must also be informed when such transmission of cookies occur. Mayer-Schoenberger [31] raises the point that the cookie warnings provided by popular Web browsers are cryptic and hard to understand for the typical user. Indeed, these cookie warnings may not provide enough information to be considered informed consent. However, because the default behavior of popular Web browsers is the unconditional acceptance of cookies without notification, only users who are already "cookie savvy" enable the alert option and receive notification. Most users do not even know what a cookie is. Additionally, with the abundant use of cookies on the Internet, cookie warnings soon become a hindrance rather than a help. As Cranor [32] observes, "when such disruptions occur frequently, individuals are unlikely to pay close attention to them."

Cookie preferences should be configured similarly to the security options found on popular Web browsers like Netscape and Internet Explorer. By default, these security

options, unlike cookie options, are enabled. For instance, we are always warned whenever we may be sending unencrypted information to a Web site. To disable this warning, we simply click an option which appears in the warning window itself. In contrast, in order to configure cookie preferences, the user must first know about cookies and then have the patience to find the options in the various browser menus. By default, Web browsers should inform the user about the setting and transmission of cookies. Additionally, the warning windows should then contain the various options to enable, distinguish, and disable all cookies. These options would allow users to configure their cookie preferences “on the y,” for example, if the cookies warnings become too annoying.

Another possible solution is to include privacy policy choices (cookie options) in the setup phase of software installation. When installed on a computer, typical software packages must go through a one-time setup phase. During the setup phase, the user is asked to give information which is needed by the software program. Therefore, the setup phase is an ideal place to obtain informed consent from a user. Recall in Section 3.2 that the disclosure of all pertinent information (whether or not the user is interested) is necessary for informed consent. While typical users may not be interested in privacy policies, they must all endure this setup phase in order to use the software. Placing privacy options in this setup phase then forces the user to become informed about the potential privacy losses and violations related to the software. With the recommendations of the previous paragraph, this mechanism would inform users about cookies and give them the ability to change their personal preferences concerning cookies “on the y.” Cookies are so prevalent on the Internet that completely disabling them would likely limit the capabilities of the Web browser. We reemphasize that is unnecessary to disable all cookies since typical uses lie within reasonable expectations of privacy. What is important in developing cookie configuration policies, then, is distinguishing morally permissible cookies from immoral cookies.

9 Summary and Conclusions

The Internet provides a new context in which to explore our ideas about privacy. The scale and ease of personal information collection and centralization have caused general concern and confusion regarding our rights to privacy in such an environment. We have offered a framework for evaluating the ethics of the manipulation of information on the World Wide Web. We believe that there are both ethical and unethical ways to collect personal information.

Specifically, collection of information is unethical when such collection lies beyond our reasonable expectation of privacy for the situation. Obtaining informed consent before collecting personal information, however, is a sufficient

means for preventing violations of privacy. While collection of personal information can be ethical, we believe that centralization of personal information is inherently unethical because it undermines the basic function of privacy to create and maintain personal relationships.

Finally, we described the Internet as a public place and offered an interpretation of a reasonable expectation of privacy for certain situations on the Web. Specifically, we explored the the issue of Internet cookies and concluded that the use of cookies for online shopping and for customer preferences is morally permissible. In contrast, the use of cookies by target marketers to monitor consumer habits is unethical not only because such collection lies beyond a reasonable expectation of privacy but also because the collected information is unethically centralized. ♦

Acknowledgments:

We thank Willem Bakker II and Helen Nissenbaum for providing direction to this project, James Wallace for the references to the literature on informed consent, Mike Stangel for information on Mallard, and Lorrie Faith Cranor, Lillian Hoddeson, Andrew Pickering, Warden B. Rayward, Ron Szoke, and Marsha Woodbury for suggestions on earlier drafts of this paper.

Notes:

1. Moor asserts that normative privacy is culturally determined: situations which ought to be private should be open to rational and moral argument.
2. Good reason, in this sense, must be a reason grounded on moral principle such as freedom of others, justice, respect for persons, or avoidance of needless pain
3. Ward had taken her landlord to court because he had failed to deal with the cockroaches and rodents which infested her apartment.
4. In his article “Private Life in Cyberspace”. Barlow [19] reflects on the Lotus Marketplace: Households decision. He contrasts today’s misuse of information and technology to the restraint exhibited in small towns, where everyone knows information about everyone else, but cares enough to use the information in a respectful manner.
5. We ate not saying that the tool itself has no effect on people’s behavior. Johnson [16] argues that because computers facilitate the collection of information, people engage in activities which would have not otherwise been possible. Computers, as tools, therefore are an important factor in how people make decisions.
6. An activity is immune if it is not appropriate for unauthorized persons to watch it.
7. As Martin and Schinzinger [15] have observed, most people tend to accept risks which arevoluntarily undertaken.
8. The Privacy Act of 1974 forbade the executive branch of the government from sharing information among distinct government program areas. Use of information was limited to “routine use,” or a “purpose which is compatible with the purpose for which it was collected.” Unfortunately, interpretations of “routine use” were so loose, they left the Privacy Act ineffective. In addition, the Office of Management and Budget, the agency designated to enforce the Privacy Act, essentially refused to uphold the principles of the Act. Both Laudon [20] and Shattuck [21] provide informative sections about the Privacy Act of 1974.
9. Under Gavison’s definition of privacy, there may indeed be a loss of privacy. That is to say, because we are the subject of Bobs attention, a degree of our anonymity is lost [8]. However, according to Moor, this would be a loss of natural privacy which is not necessarily a violation of privacy [9]
10. It might be argued that although the centralized information exists, this does not mean that everyone will choose to use it. However, as discussed in 5.2, centralization reduces the cost of obtaining information and makes it more likely that someone will choose to access it. In this sense, it is very much a factor in determining how people act. This argument is similar to the argument Johnson [16] uses to show that tools such as computers are a factor in determining what people do.
11. For mote information on Mallard, consult <http://www.cen.uiuc.edu/Mallard>.
12. The European Union Directive on the Protection of Personal Data includes five conditions: (I) personal data must be “processed fairly and lawfully” and only

- “collected for a specific, explicit, and legitimate purpose”; (2) no further processing which is incompatible with the original legitimate purpose is permitted; (3) processing must be “adequate, relevant, and not excessive in relation to the purpose” as well as “accurate, and when necessary, kept up to date”; (4) data may be stored for “no longer than necessary for the purposes for which the data was collected”; (5) processing may take place only if the person to whom the personal information refers “has unambiguously given his consent.”
13. The contents of the cookies in the above examples are quite simplified. For a detailed description of what cookies actually look like, consult the book by Garfinkel and Spafford [33].
14. While Internet Explorer 4.0 has options to warn, always accept, or disable cookies, it does not distinguish morally permissible cookies from immoral cookies, as Netscape Communicator 4.04 does.

References

- [1] Motin, Richard, “Cruising the Internet...but Warily,” in *The Washington Post National Weekly Edition*, June 23, 1997, page 35.
- [2] Moor, James H., “Towards a Theory of Privacy in the Information Age,” in *Computers and Society*, September 1997, pp. 27-32.
- [3] Warren, Samuel D. and Louis D. Brandeis, “The Right to Privacy,” in Schoeman, Ferdinand David, ed., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Massachusetts: Cambridge University Press, 1984, pp. 75-103.
- [4] Fried, Charles, “Privacy,” in Schoeman, Ferdinand David, ed., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Massachusetts: Cambridge University Press, 1984, pp. 203-222.
- [5] Westin, Alan F. *Privacy and Freedom*, New York, Atheneum, 1967.
- [6] Beardsley, Elizabeth, “Privacy: Autonomy and selective disclosure,” in Pennock, J.R. and J.W. Chapman, eds., *Nomos XIII: Privacy*, New York: Atherton Press, 1971.
- [7] Parent, W.A. “Privacy, Morality, and the Law,” in *Philosophy and Public Affairs*, vol. 12, no. 4, Fall 1983, pp. 269-288.
- [8] Gavison, Ruth, “Privacy and the Limits of Law,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 332-350.
- [9] Moor, James H., “The Ethics of Privacy Protection,” in *Library Trends*, vol. 39, nos. 1 and 2, Summer/Fall 1990, pp. 69-82.
- [10] Rachels, James, “Why Privacy is Important,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 351-357.
- [11] Benn, Stanley I. “Privacy, freedom, and respect for persons,” in Schoeman, Ferdinand David, ed., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Massachusetts: Cambridge University Press, 1984, pp. 223-234.
- [12] Faden, Ruth R. and Tom L. Beauchamp, *A History and Theory of Informed Consent*, New York: Oxford University Press, 1986.
- [13] Gorovitz, Samuel, “Informed Consent and Patient Autonomy,” in Callahan, Joan C., ed., *Ethical Issues in Professional Life*, New York: Oxford University Press, 1988, pp. 182-187.
- [14] Lidz, Charles, Alan Meisel, Eviatar Zerubavel, Mary Carter, Regina M. Sestak, and Loren H. Roth, *Informed Consent: A Study in Decisionmaking in Psychiatry*, New York: The Guilford Press, 1984.
- [15] Martin, Mike W. and Roland Schinzinger, *Ethics in Engineering*, McGraw-Hill publishing Company, 1989.
- [16] Johnson, Deborah G. *Computer Ethics*, 2nd ed., Upper Saddle River, New Jersey, Prentice Hall, 1994.
- [17] Forester, Tom and Petty Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, 2nd ed., Cambridge, Massachusetts: The MIT Press, 1994.
- [18] Quittmet, Joshua, “Invasion of Privacy” in *Time*, August 25, 1997, pp. 28-35.
- [19] Barlow, John P. “Private Life in Cyberspace,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 310-313.
- [20] Laudon, Kenneth C. *Dossier Society: Value Choices in the Design of National Information Systems*, New York: Columbia University Press, 1986, 30.
- [21] Shattuck, John, “Computer Matching is a Serious Threat to Individual Rights,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 305-309.
- [22] Culnan, M.J. and H.J. Smith, “Lotus Marketplace: Households... Managing Information Privacy Concerns,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 269-277.

- [23] “Where is our Data?” in *Secure Computing: The Magazine for the Protection of Information*, August 1997, pp. 18-22.
- [24] Hunter, Larry, “public Image,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 293-298.
- [25] Parker, Donn B., *Ethical Conflicts in Computer Science and Technology*, Arlington, Virginia: AFIPS Press, 1979.
- [26] Ware, Willis H., “The New Faces of Privacy,” in *The Information Society*, vol. 9, 1993, pp. 195-211.
- [27] Nissenbaum, Helen, “Toward an Approach to Privacy in Public: Challenges of Information Technology,” in *Ethics and Behavior*, vol. 7, no. 3, 1997, pp. 207-219.
- [28] Getety, Tom, “Redefining Privacy,” in *Harvard Civil Rights- Civil Liberties Law Review*, vol. 12, no. 2, 1977.
- [29] Malcolm’s Guide to Persistent Cookies <http://www.emf.net/~mal/cookiesinfo.html>
- [30] Andy’s HTTP Cookie Notes: <http://www.illuminarus.com/cookie.fcgi>
- [31] Mayer-Schoenberger, Viktor, “The Internet and Privacy Legislation: Cookies for a Treat?” in *West Virginia Journal of Law and Technology*, vol. 1, issue 1, March 17, 1997, at <http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm>.
- [32] Cranor, Lottie Faith, “The Role of Technology in Self Regulatory Privacy Regimes,” prepared for the National Telecommunications and Information Administration, December 1996, at <http://www.research.att.com/~lorrie/pubs/NTIA.html>, 31.
- [33] Garfinkel, Simon with Gene Spafford, *Web Security and Commerce*, O’Reilly & Associates, Inc., 1997.
- [34] Privacy section at <http://www.cookiecentral.com/javacook2.htm>.
- [35] Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers Ethics & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995.
- [36] Nissenbaum, Helen, “Can We Protect Privacy in Public?” in *ACM SIGCAS Conference in Computer Ethics*, June 1997, Rotterdam, The Netherlands.
- [37] Moot, James, H., “What is Computer Ethics,” in Johnson, Deborah G. and Helen Nissenbaum, eds., *Computers, Ethics, & Social Values*, Upper Saddle River, New Jersey: Prentice Hall, 1995, pp. 7-14.

Permission to make digital/hard copy of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication and its date appear, and notice is given that copying is by permission of ACM, Inc. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

POLICY '98, Washington, DC © 1998 ACM 1-58113-038-4/98/0500 \$5.00