

***This version of the article is a late working copy. Please do not quote exactly without consulting the final published version.**

An Ethics For The New Surveillance 1

Gary T. Marx
Professor of Sociology
University of Colorado
Boulder, Colorado

Address correspondence to:

E-mail: Gary.Marx@Colorado.edu.

Web: [HTTP://SOCSCI.COLORADO.EDU/~MARXG/GARYHOME.HTML](http://SOCSCI.COLORADO.EDU/~MARXG/GARYHOME.HTML)

"If it doesn't look right, that's ethics."

-Popular expression

"I'm in computer science. I took this class because eventually I want to do the right thing."

-M.I.T. student

"It's a remarkable piece of apparatus."

-F. Kafka, The Penal Colony

Abstract

The Principles of Fair Information Practice are almost three decades old and need to be broadened to take account of new technologies for collecting personal information such as drug testing, video cameras, electronic location monitoring and the internet. I argue that the ethics of a surveillance activity must be judged according to the means, the context and conditions of data collection and the uses/goals and suggest 29 questions related to this. The more one can answer these questions in a way that affirms the underlying principle (or a condition supportive of it) the more ethical the use of a tactic is likely to be. Four conditions are identified which, when breached, are likely to violate an individual's reasonable expectation of privacy. Respect for the dignity of the person is a central factor and emphasis is put on the avoidance of harm, validity, trust, notice and permission when crossing personal borders.

Keywords: surveillance, ethics, new information technologies, privacy, borders, reasonable expectation of privacy

In 1928 Justice Brandeis wrote "discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack to obtain disclosure in

court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping." (Olmstead, 1928) His haunting and prescient words clearly apply today, as the line between science and science fiction is continually redrawn and private sector data collection practices join those of government as a cause of concern.

New technologies for collecting personal information which transcend the physical, liberty enhancing limitations of the old means are constantly appearing. They probe more deeply, widely and softly than traditional methods, transcending barriers (whether walls, distance, darkness, skin or time) that historically made personal information inaccessible. The boundaries which have defined and given integrity to social systems, groups and the self are increasingly permeable. The power of governmental and private organizations to compel disclosure (whether based on law or circumstance) and to aggregate, analyze and distribute personal information is growing rapidly.

We are becoming a transparent society of record such that documentation of our history, current identity, location, and physiological and psychological states and behavior is increasingly possible. With predictive profiles there are even claims to be able to know individual futures. Information collection often occurs invisibly, automatically and remotely-being built into routine activities. Awareness and genuine consent on the part of the subject may be lacking. The amount of personal information collected is increasing. New technologies have the potential to reveal the unseen, unknown, forgotten or withheld. Like the discovery of the atom or the unconscious, they surface bits of reality that were previously hidden, or didn't contain informational clues. People are in a sense turned inside out and the cartilages are shrinking.

To be alive and a social being is to automatically give off signals of constant information-whether in the form of heat, pressure, motion, brain waves, perspiration, cells, sound, olifacteurs, waste matter, or garbage, as well as more familiar forms such as communication and visible behavior. These remnants are given new meaning by contemporary surveillance technologies. Through a value-added, mosaic process, machines (often with only a little help from their friends) may find significance in surfacing and combining heretofore meaningless data. The ratio of what individuals know about themselves (or are capable of knowing) vs. what outsiders and experts can know about them has shifted away from the individual. Data in diverse forms from widely separated geographical areas, organizations and time periods can be easily merged and analyzed. In relatively unrestrained fashion new (and old) organizations are capturing combining and selling this information, or putting it to novel internal uses.

Of particular importance are recent developments in electronic (audio, visual, telemetric), biochemical and database forms of information collection. The increased availability of personal information is a tiny strand in the constant expansion of knowledge witnessed in the last two centuries and of the centrality of information to the working of contemporary society.

Computer databases, video cameras, drug testing and work monitoring are routine. They are being joined by new means that may become equally prevalent in coming decades: DNA screening and monitoring for insurance and employment, personal electronic location monitoring devices via implanted chips, internet monitoring devices that keep a record what one has viewed and for how long, "intelligent" highway systems, "smart cards" that contain extensive personal

information, satellites, and "smart homes" in which data flows (whether electricity, communications, energy) into and out of the home are part of the same monitored system. These technologies constitute the new surveillance.²

Broadening the Principles of Fair Information Practice Most discussions of the ethics of computer surveillance are informed by the principles of fair information practice that received widespread public notice in 1973 when drafted by the U.S. Health, Education and Welfare Department. Colin Bennett's work done for the Canadian Standards Association has expanded these to include:³ 1) accountability 2) identifying purposes 3) openness 4) limiting collection 5) limiting use, disclosure and retention 6) accuracy 7) safeguards 8) individual access 9) challenging compliance. In offering publicity, complaint and compliance mechanisms these standards are clearly an advance over the minimalist standards of the earlier period.

The data protection model above forms the basis of the OECD Guidelines and most national legislation. This model has generally been seen as appropriate for the database forms of surveillance up to the 1980s. One concern of the conference at which this paper was presented was to ask if this model still applies with recent changes such as those involving cross-border data flows and the spread of internet usage. A related question is whether the model is (or ever was) adequate for other forms of the new surveillance-not just those that are exclusively computer based. The information superhighway is not the only road into or out of people's lives.

I argue that this model is not adequate and that a more encompassing framework is needed. For example, the conventional principles offer no criteria for deciding if a given means of data collection is ethically acceptable. Nor do they give adequate attention to the actual process of extracting the data. This is because the collection of the data entered into computers is usually not at issue-most often involving a biographical fact or a transaction. That is not the case for urine drug testing, the polygraph or hidden video cameras. Yet this issue will become more important for computers. As we move from data entered into a computer by an operator at a terminal to remote automatic entries based on visual, auditory and biometric forms of data, questions over the appropriateness of the initial data collection will become increasingly important.

The essence of the fair information practice code involves informed consent, unitary usage and non-migration of the data. These are essential, but they are of little help with respect to the appropriateness of the original goals, nor do they adequately cover the broader context within which the data are collected.

My concern here is to offer a broader set of principles for all forms of technological personal data collection and use, not just those involving computers.⁴ The fair information principles need to be located within a more general framework. They are not sufficient for many of the new technologies and uses.

Information technologies are controlled by laws, organizational policies, various protective counter-technologies and etiquette (Marx, 1994). Data gathering and protection efforts imply ethical assumptions that are often unstated. In what follows I suggest an ethical framework for thinking about personal surveillance and new information technologies (although the principles suggested also apply to traditional means such as informing and eavesdropping).

Public opinion polls consistently show that a very large percentage of Americans are concerned about their personal privacy. But the elements of this are muddled and muddied. Given

the newness of the technologies, value conflicts and the multiple components of privacy, opinion here is less well defined and coherent than is the case for many other issues. Persons often have trouble articulating what seems wrong with a surveillance practice beyond saying that privacy is invaded. Privacy is a vague catch-all phrase that includes a variety of concerns-e.g., respect for the personhood, dignity and autonomy of the individual including the sentiments behind the First, Fourth and Fifth Amendments, private property and solitude.

Many persons feel a sense of discomfort in the face of indiscriminate drug testing⁵, hidden video cameras, electronic work monitoring, and the collection and marketing of their personal information-even as they favor responsible behavior, efficiency, economic growth and credit card-aided consumption. But what is there about the new information technologies that is troubling? By what standards should we conclude that a given practice is right or wrong?

My initial goal as a social scientist is to understand the factors that can generate unease across a variety of contexts. I argue that at an abstract level there are shared expectations in American, and perhaps to a degree more generally in western and industrial-capitalist cultures, whose violation underlies the discomfort experienced in the face of new information technologies.

I seek to identify the major normative factors that would lead the average person to feel that a surveillance practice is wrong, or at least questionable. I differentiate various elements of the surveillance setting which require ethical analysis. The reader may wish to look at Table 1, below, which lists 29 questions to be asked of the latter. These questions involve the tactic, the data collection context and the goals. Without claiming that they are morally equivalent, I argue that the more one can answer these questions in a way that affirms the underlying principle (or a condition supportive of the principle), the more ethical the use of the tactic is likely to be.

Table 1: Questions To Help Determine The Ethics of Surveillance

A. The Means

1. Harm: does the technique cause unwarranted physical or psychological harm?
2. Boundary: does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational or spatial border)?
3. Trust: does the technique violate assumptions that are made about how personal information will be treated such as no secret recordings?
4. Personal relationships: is the tactic applied in a personal or impersonal setting?
5. Invalidity: does the technique produce invalid results?

B. The Data Collection Context

6. Awareness: are individuals aware that personal information is being collected, who seeks it and why?
7. Consent: do individuals consent to the data collection?
8. Golden rule: would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?
9. Minimization: does a principle of minimization apply?
10. Public decision-making: was the decision to use a tactic arrived at through some public discussion and decision making process?

11. Human review: is there human review of machine generated results?
12. Right of inspection: are people aware of the findings and how they were created?
13. Right to challenge and express a grievance: are there procedures for challenging the results, or for entering alternative data or interpretations into the record?
14. Redress and sanctions: if the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behavior?
15. Adequate data stewardship and protection: can the security of the data be adequately protected?
16. Equality-inequality regarding availability and application:
 - a) is the means widely available or restricted to only the most wealthy, powerful or technologically sophisticated?
 - b) within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist
 - c) if there are means of resisting the provision of personal information are these equally available, or restricted to the most privileged?
17. The symbolic meaning of a method: what does the use of a method communicate more generally?
18. The creation of unwanted precedents: is it likely to create precedents that will lead to its application in undesirable ways?
19. Negative effects on surveillors and third parties: are there negative effects on those beyond the subject and if so can they be adequately mediated?

C. Uses

20. Beneficiary: does application of the tactic serve broad community goals, the goals of the object of surveillance or the personal goals of the data collector?
21. Proportionality: is there an appropriate balance between the importance of the goal and the cost of the means?
22. Alternative means: are other less costly means available?
23. Consequences of inaction: where the means are very costly, what are the consequences of taking no surveillance action?
24. Protections: are adequate steps taken to minimize costs and risk?
25. Appropriate vs. inappropriate goals: are the goals of the data collection legitimate?
26. The goodness of fit between the means and the goal: is there a clear link between the information collected and the goal sought?
27. Information used for original vs. other unrelated purposes: is the personal information used for the reasons offered for its collection and for which consent may have been given and does the data stay with the original collector, or does it migrate elsewhere?
28. Failure to share secondary gains from the information: is the personal data collected used for profit without permission from, or benefit to, the person who provided it?
29. Unfair disadvantage: is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?

The emphasis here is on the watchers rather than the watched, on avoiding harm rather than doing good⁶, on the individual more than the group⁷ and the short rather than the long run. This article suggests a perspective on ethical analysis for those who carry out the surveillance or data collection. It assumes that under appropriate conditions they may have a right to do this, but they also have a duty to do it responsibly. Reciprocally, those subject to legitimate surveillance may have duties as well (e.g., not to distort the findings), even as they also have rights not to be subjected to some forms of surveillance.⁸

Let us begin the analysis by making a distinction between 1) the means (instrument) of data collection 2) the context and conditions under which the data are gathered and 3) the uses/goals to which the data are put. There is a temporal sequence here as we start with the means and then move to collection and use.

These may of course overlap (as when a system of retinal eye pattern identification to which persons consent automatically results in access or its denial). But they are often distinct. A given means such as video can be used for a variety of goals and a given goal such as drug testing can be done in a variety of ways. Means and goals apart, the conditions under which these are joined also show enormous variation. The ethical status can vary from cases in which the means, the context and the use are all abhorrent to those in which they are all acceptable or even desirable, to varying combinations. Ethical analysis needs to consider all three factors. Beyond different value priorities and interpretations, disagreements in evaluation often involve persons emphasizing one rather than another of these elements.

The Means

Are there some means of personal information collection that are simply immoral, apart from how and why they are done? Torture is the obvious case. Other techniques that many observers find unethical include the polygraph with its tight fitting bodily attachments⁹, manipulation and questionable validity; a drug test requiring a person to urinate in front of another; and harming or threatening friends or relatives of a suspect in order to obtain information.

Similarly most persons recoil at the thought of certain coercive bodily intrusions such as pumping the stomach of a suspect believed to have swallowed evidence or removing a bullet from the body for ballistics matching (practices which the courts have generally also prohibited). Body cavity searches occupy an intermediate position. In contrast the non-consensual collection of hair, blood and fingerprints has greater acceptability.

For many moral theorists and much of society lying, deception and manipulation are a cluster of means that in and of themselves are ethically questionable.¹⁰ These come together in the case of undercover tactics. Such means (unlike many other surveillance means) always present a moral dilemma. This is not to suggest that under certain conditions and for certain ends they may not on balance be appropriate. But no matter how compelling the latter, this does not alter the fact that in our culture neither lying and trickery, nor physical force and coercion, are morally preferred techniques.

Having listened to the debates for a decade and examined a great variety of empirical data I think there is a folk morality that underlies judgments made about the collection of personal

information. A popular expression claims "if it doesn't look right that's ethics." And when the means do not look right, I hypothesize that the act of collecting personal data is likely to involve saying "yes" to one or more of the following questions: 1) Does the act of collecting the data (apart from its use) involve physical or psychological harm?¹¹ 2) Does the technique produce invalid results? 3) Does the technique cross a personal boundary without notice or permission (whether involving coercion or deception or a body, relational, spatial or symbolic border)? 4) Does the technique violate trust and assumptions that are made about how personal information will be treated (e.g., no secret recordings?)

To the extent that one or more of these concerns are present the means as such raise ethical concerns. While distinct, these factors can of course be related (e.g., in crossing a personal boundary the betrayal of trust can cause harm).

In spite of the fact that some data collection or surveillance means are inherently undesirable, most contemporary disputes do not involve the means as such, rather they involve the context and the ends. Ethical disagreements and problems are more likely to be found in the conditions around the data collection and/or in the use of the data than with the means. There is also an accelerating effort to develop "softer" and more valid technologies for which the answer to some of the four questions posed above is "no."

My argument reflects a more general perspective on ethics which stresses contexts rather than behavior or a technology as such. We often tend to act as if the material technology or behavior and their moral evaluation were one, instead of seeing the latter as a social construct whose application largely depends on the setting, not the technology or the behavior in and of itself.¹² For example contrast a weapon used to hunt food as against one used in the commission of a crime, or a location monitoring device carried by a skier as a protection against avalanches as against the surreptitious application of such a device to a person's car. Similarly omnipresent video surveillance, even in bathrooms is not treated as an inappropriate invasion of privacy in prisons for security and safety reasons, while in most other settings it would be.

B. The Data Collection Context

With respect to the context we ask how the technique is applied and in what social setting. Simply having a means which is morally acceptable, is not sufficient justification for taking action. We also need to attend to the context of its application and then to its use.

A distinction here can be made between 1) the actual collection of the information and 2) the broader conditions surrounding this. In the first case we are again concerned with the presence of harm, invalidity, unwarranted border crossings, and violations of trust. In this case we assume that it is possible to collect the information in an ethically acceptable fashion that avoids these four conditions. We draw attention to the discretion surveillers have to behave within or beyond ethical bounds in their use of such a means.

1. Data Collection

Harm

With respect to harm during the process of information collection, tactics such as interviews, psychological tests, drug tests and searches can be done to minimize or maximize discomfort. Examples include intentionally inflicting pain in drawing blood (e.g., in the mandatory AIDS tests required of those in prison and the military); in a sexual mismatch in a strip search; or in a stressful application of the polygraph.

Invalidity

Validity here refers to whether the tactic is applied correctly and measures what it claims to measure. It is reasonable to expect that surveillance means will (in Chandler's [1957] words) reflect "the tangled web of fact" rather than the "austere simplicity of fiction". Some questions here include who has warrant to claim whether or not it is valid, where lines are drawn, how hazy data should be interpreted and what the costs are to those using invalid technologies. Situations in which invalid readings result (whether out of malevolence, incompetence, good faith errors, faulty machines or unaccounted for confounding factors) are obviously unfair and wasteful (not to mention the liability issues involved in wrongful application and use). There must be a means to verify results. It must not be assumed that fallible humans can design and operate infallible machines (or given the complexity, that machines are infallible).

The issue of validity as a principle is not publicly disputed. Privately surveillants are sometimes indifferent to validity because the means is seen as a scare tactic which deters, or those assessed are believed to be guilty or undeserving anyway, even if the test doesn't reveal it this time. Individuals may not discover the invalidity and the cost of increasing validity may be deemed to be too great.

Lack of validity may apply to an individual case as with the switching of a positive for a negative drug test or factors that can confound a drug test such as taking a prescription medicine or eating poppy seeds. Problems of validity can apply to a broad group as when a large number of false readings result because of faulty lab procedures (as in an unfortunate Navy case) or data entry errors (as with the case in a small New England town when all the credit records were deemed bad). A pattern of systematic errors is particularly troubling given what amounts to the institutionalization of unfairness.

Border and Trust Violations

The law makes a reasonable expectation of privacy and the "right to be let alone" central criteria. Yet judges apply this inconsistently depending on the offense (e.g., in drug cases the standard is less stringent and its legal meaning is vague).¹³ Apart from the law, under what conditions are individuals likely to feel that personal borders have been violated and/or that their information has been inappropriately gathered or treated?¹⁴ On the basis of interviews, observation, court cases, and mass media accounts, I hypothesize¹⁵ that this is likely to involve one or more of the following four conditions: 1. A "natural" border protective of information is unreasonably breached. The restriction here is on the senses. The assumption is that what you can "normally" or "naturally" see or hear when your presence is not hidden, you are entitled to perceive, although not necessarily to share. However, tools that extend the senses require special permission or notice.

There are several distinct categories here: a. clothes that protect parts of the body from being revealed (nakedness) b. observable facial expressions or statements or behavior, as against inner thoughts and feelings (masks) c. the assumed non-observableness of behavior behind walls, closed doors, darkness, and spatial distance (shields) d. skin and bodily orifices that serve, respectively, as protective shells or gates into the body (barriers) e. directed communications such as a sealed letter, telephone and E-mail messages which are sent to a particular person with physical protections intended to exclude consumption by other than the addressee (e.g., contrast expectations here with an open message on a bulletin board or yelling to someone across the room) (wrappers) 2. A social border assumed or expected to be protective of information is breached. This involves expectations about social roles such as a doctor, lawyer, or member of the clergy who violates confidentiality, a family member or friend who reveals secrets, or a bureaucrat who fails to seal or destroy confidential records when that is required. It would also extend (if not as strongly) to reading faxes (beyond the address) or photo-copy material left on the machine belonging to others.

The relationship between the data collector and the subject may condition evaluations, as may the place. Thus formal means of data collection are generally more appropriate in impersonal settings where there are fewer expectations of trust, than in settings where individuals have close personal relations. Contrast for example the extensive formal monitoring of those working in financial institutions with applying video cameras, drug tests, the polygraph and electronic location monitoring to children or spouses within a family. 3. A temporal or spatial border is breached which separates information from various periods or aspects of one's life. This involves assumptions about the compartmentalization or isolation of elements of personal biography including the past and the future and information in different locations. While the individual may have no clear interest in protecting any single aspect (age, education, religion, education, occupation) the picture significantly changes when a mosaic can be created from many diverse pieces. The sum becomes much greater than the individual parts. This overlaps #1 above in the sense that before linked computers there were "natural" barriers to combining this information even when it was publicly available.¹⁵

More abstractly physical barriers and time were traditionally similar in working against the aggregation of information. The presumed ability to simultaneously access and link the past, present and predicted future alter the traditional meaning of time and the information protection it offered.

Borders have legitimate and illegitimate crossing points and interstitial and gray areas. The collection of information in a public setting such as a street or park is different from that in a private setting. Even there, being invited in the front door is very different from breaking it down or sneaking in the back. Sitting on a park bench and leaning to overhear two people whispering is different from listening to a soap-box oration on the same bench. However the public-private place distinction may become hazy as when a person on a public street looks in the window of a home or loud music or cooking smells from a home go beyond it or in places with a mixed public-private character such as shopping malls, universities and business and industrial parks. 4. An assumption that interaction and communication are ephemeral and transitory like a river, and are not to be captured through hidden video or audio means. This is believed to encourage candor and intimacy. Similarly we assume that things that are discarded in the garbage will in fact

disappear and not be claimed by information scavengers. This is the "short shelf-life assumption". Other factors being equal, things that are said and the material artifacts of our personal life should not have a continued life after use.

This is a case where the garbage is not messy. One could argue that if you discard something unshredded on a public street, you are offering implied consent for whatever happens to it. But that is a weak argument. Why should one have to go to the added inconvenience of dealing with a shredder simply because others have the ability to access the garbage? Better to pass laws prohibiting such activity as Beverly Hills, California has done. Nor is the problem here the failure to inform. Telling people their garbage would be surveilled would hardly justify doing it.

Why should we have an expectation that our garbage will be private? Expended artifacts that have been within the protection of the home may still merit protection (bottles indicating the kinds of medications a person takes, correspondence, credit card bills or literature they read) for several reasons. Such protection may prevent the theft of identity, fraud and other crimes and harassment. It can prevent the aggregation of individual bits of personal data into a meaningful whole. When this isn't possible the backstage presentations that are central to self and organizational life are weakened (Goffman 1959). This may mean strategic disadvantage, stigma or merely embarrassment and a sense of being invaded. When personal information becomes public without our will, it loses its value as a currency in interpersonal relations.

Awareness and Consent

There are social roles that are granted the right to transcend personal boundaries without consent and sometimes even awareness, such as police and emergency medical personnel (if in principle under controlled and accountable conditions). For example there are cases where the presence of awareness or consent would defeat a legitimate purpose, as in undercover or audio/video recordings in criminal justice investigations and/or cases involving dependent persons. However in conventional settings the failure to inform, or a coercive lack of choice in extracting information is of a different order.

Personal border crossings and trust are related to (and even defined by) whether 1) individuals are aware that personal information is being collected (and by whom and for what purpose) and if so 2) whether they agree to the collection and subsequent uses of the data. An important issue is specification of when awareness, awareness and consent or neither ought to apply. To consent implies being aware but the reverse is not necessarily true.

These are difficult concepts since no one can be fully aware of all the possible consequences of the act of data collection, nor of subsequent uses. In the same way "consent" is always conditioned by the range of choices and their relative costs and benefits.

There are also degrees-such as full awareness that a tactic may be used vs. knowing that it will be used but not in precise detail where and when (e.g., location of a hidden camera, or whether or not there is a monitor/recorder behind a known camera). A nice example of the joining of being informed with consenting are some internet web pages that tell users that "cookies", a program that may enter a user's hard drive and chart what the individual views may be activated or blocked as the user chooses.¹⁶ The check off option offered by some magazine subscription

services with respect to not having one's personal information re-used is another.

One component of justice is fair warning --providing people with information about the rules, procedures, rewards and punishments they are subject to. Beyond showing respect for the person, full disclosure can be a means of shaping behavior as individuals know they will be assessed and may behave accordingly (e.g., paying bills on time to avoid being database-labeled as a bad credit risk).

Openness regarding data collection can also help bring accountability to the data collectors; since it comes with an address, responsible behavior on their part may be more likely as a result. In that regard it is similar to a supervisor walking behind and monitoring workers, as against having this done secretly via remote computer. The knowledge of who is doing the monitoring can be a constraint on how it is done.

We can also ask if consent has the quality of "opting in" or "opting out". In the latter case individuals are told that if they give their permission their individual data will be used for other than its original purpose. In the former individuals are told that their data will automatically be used for other than its original purpose, unless they request that it not be. Those with an interest in gathering the data strongly prefer the latter system of opting out-that is requiring persons to ask that they not be included. To be sure that is better than offering no choice at all. But since many persons will be ignorant of the possibility of opting out or not want to take the time, not remember, or be unaware of the potentially negative consequences of providing personal data, "opting in" is preferable.

In addition "opting in" symbolically shows greater respect for the person. Requiring the data collector to ask permission implies that the protection of personal information is the norm and its' use for secondary purposes is the exception for which special action is required (e.g., the individual needs to affirm that he or she is willing to give up the data, rather than passively giving it up by doing nothing, as with the failure to "opt out").

The concept of consent of course can be very problematic, given the role of culture in shaping perceptions and the fact that choice always occurs within situations that are not fully free, or within the making of the person choosing. For example, the meaning of choice with respect to agreeing to take a drug test is very different in a one-industry town from what it is in a setting where one can find equivalent work in which not all employers require such a test.¹⁷

In flying on a domestic Canadian airline, I saw the following sign: Notice: Security measures are being taken to observe and inspect persons. No passengers are obliged to submit to a search of persons or goods if they choose not to board our aircraft.

Rather than spend days in the car or on the train, I chose to fly and "agreed" to be searched. Most persons would do the same. But to claim the choice is somehow voluntary as the sign suggests is disingenuous in the extreme. The situation is the same for signs in some federal buildings which warn "In entering here you have agreed to be searched." In a related example during the controversy over the caller-ID service a telephone company representative said-"When you choose to make a phone call, you are choosing to have your phone number released." Choice, to be meaningful, should imply some genuine alternatives and refusal costs that are not wildly exorbitant.

We also need to ask "consent to what?" Thus a mass marketing executive reports "the data isn't out there because we stole it from them. Someone gave it away, and it's out there for us

to use." In a legal sense that is true. But the element of "giving it away" was not a willful choice in the obvious sense. Rather the data became available indirectly as a result of taking some other action such as a mail order purchase. At the time if individuals were to be asked if they agree to have their personal information used for marketing purposes, (as is the case with some purchases), there would be far less "out there" waiting for specious disclaimers about its non-theft.

We can also ask "who consents?" Thus when children follow the advice of a television clown telling them to hold their telephone receivers in front of the TV while a remote signal sent through the television set activates the phone sending its number over an 800 line, they have acted voluntarily. But they did not know that this was to be used for direct mail candy marketing and even if they did, the "consent" of small children obtained by a clown on TV seems specious.

This can also be approached by asking "who's informed and who needs to consent?" In phone transactions it is now common to be told "this conversation may be recorded to insure quality service". The employee is informed and may have consented. For the customer only the first reasonably applies (although in choosing not to hang up an implicit consent is offered, but again this can be a specious choice given the need for information or a service).

None of the principles offered here are unconditional. With the complexities and competing values, the absence of informed consent is not automatically a sign of unethical behavior (although situations where it could be offered and is, are clearly morally preferable to those where it is not). Nor is the presence of consent sufficient. Thus the law and morality set limits on what can be agreed to (e.g., limits on selling one's vote or selling oneself into slavery or agreeing to live in substandard housing for a reduced rent. (Radin 1996) Similarly to inform people of an outrageous tactic does not justify it. Neither a technology's potential, nor publicizing its use, or consent should be sufficient to define a reasonable expectation of privacy, though they relate to it.

Even if the data gatherer does not offer a formal choice, it may be possible to have the equivalent of choice by using a counter-technology to block the collection of personal information (assuming one is aware of the collection). If devices to prevent the unwarranted collection of personal information are widely available but nevertheless not used, then there is a sense in which persons do choose to release their private information. Yet that is not the case if such means are very expensive or difficult to use.

An element of choice may also be present when privacy becomes commodified such that persons can choose by payment or compensation the level of privacy they desire. Yet it is still important that privacy thresholds be available below which no one is unprotected.

Minimization

One aspect of harm and crossing possibly perilous personal borders involves going farther than is required or than has been publicly announced (and perhaps agreed to by the subject). To do so may be experienced as a kind of informational rape, violating dignity and trust. Here we ask does a principle of minimization apply to the collection of personal data?

Such a principle requires that one should go no farther than is necessary for the task at hand, in spite of temptations and incentives to go beyond. Granted that many of these tactics by

their very nature cross personal boundaries and may subject the person to feelings of embarrassment, shame, and powerlessness, we can still ask "was this done in a professional manner and only to the extent necessary to obtain the informational end, or does it go beyond that?" For example, is wiretapping applied in a categorical way such that all communications are listened to, or only those pertaining to the focused goal? If federal minimization rules are followed regarding wiretapping it will be only the latter. If a conversation is not relevant or involves parties not of legal interest, it is not to be monitored (of course this also offers a way of neutralizing it if one can assume that the rules will be followed). A related example is the very precise time and place limits of search warrants.

In contrast, many private sector data gatherers face no such limits. As an "insurance" policy, data collectors often favor gathering more information rather than less, because they can never be sure that sometime in the future they might not need it, or that a new way of using it might not be discovered. Consider large retail chains that routinely even ask cash purchasers for their name and phone number. Only recently have computer models become available to mine detailed retail transaction data for marketing purposes. Other examples of extraneous data collection are the unrelated questions about life style and social circumstances that accompany warranty forms. Medical samples taken for employment purposes may be analyzed for conditions for which informed consent has not been given. Or in a Washington DC case of Hitchcock's Rear Window meets the 90s, rotating cameras used to monitor traffic may focus on high rise apartment buildings during slack traffic hours near bedtime.

The potential to go too far is also found among the systems operators for many networked computers. For example some interactive computer games or other services that involve using software at a company's webpage give the company the opportunity to explore everything in a user's computer. There may be valid reasons for doing this (e.g., to see if a player has stolen or misused files) but there is no justification for looking at other unrelated files. In the same way providers of telephone and E-mail services may need to monitor communication to be sure their systems are working, but to listen to conversations or read E-mail beyond what may be technically required for service reasons is wrong for reasons of dignity, trust and property. Yet the temptation can be great.

The Social Setting

The second aspect of the conditions of data collection involves the broader social context, rather than the direct application of the tactic as such. I identify seven procedural or enabling conditions and three negative conditions involving the social setting. The presence of the enabling conditions and the absence of the three negative conditions does not make a tactic ethical, but does increase the likelihood of ethically acceptable outcomes. Some procedural conditions: 1) Public decision-making: was the decision to use a tactic arrived at through some public discussion and decision making process? For example are the conditions of computer and telephone work monitoring of reservation and telephone receptionists jointly developed through a management-union or worker's council committee? Is the introduction of a new technology for delivering unlisted phone numbers (e.g., Caller-Id) subject to broad review via citizen input and a regulatory commission or simply offered by technological fiat? Is a decision to introduce video

cameras onto highways and public streets discussed by the city council? 2) Human review: is there human review of machine-generated results? This is vital given the acontextual nature of much of the data the technology generates and the possibility of hardware and software failure. Generally individuals as interpreters of human situations are far more sensitive to nuance than are computers, even if they are much more expensive.¹⁸ 3) Right of inspection: are people aware of the findings and how they were created? Fundamental aspects of procedural justice are being entitled to know the evidence and as the next condition suggests, to challenge it. The right to see one's file is related to a broader principle that holds that absent special conditions, there should be no secret personal databases in a democratic society. 4) Right to challenge and express a grievance: are there procedures for challenging the results, or for entering alternative data or interpretations into the record? 5) Redress and sanctions: if the individual has been treated unfairly and procedures are violated, are there appropriate means of redress and, if appropriate, for the destruction of the record? Are there means for discovering violations and penalties to encourage responsible surveillant behavior? Unlike Europe and Canada where there are official Data Commissioners who may actively seek out compliance, in the United States it is up to individuals to bring complaints forward. But in order for that to happen they must first be aware that there is a problem and that there are standards. 6) adequate data stewardship and protection: can the security of the data be adequately protected? There must be standards for who has access to the data and audit trails, for whether and when data is to be updated, for how long it is to be kept and the conditions under which it is to be destroyed.

Finally, four more general questions deal not with a given individual, but with broader social consequences: 1) equality-inequality regarding availability and application: This involves four questions: a) is the data collection means widely available or restricted to only the wealthy, powerful or technologically sophisticated? b) within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist? c) even in settings where differential application is appropriate, would the surveillants (both those responsible for the decision to use a technology and those who actually apply it) have enough confidence in the system that they would willingly submit to it themselves if they were in the situation? d) if there are means of resisting the unwarranted acquisition of personal information (whether technically, economically, or legally) are these equally available, or restricted to the most privileged?

The first question applies particularly to conflict and hierarchical settings and relates to Kant's principle of universalism or consistency which asks "Would it be acceptable if all persons or groups used the tactic"? The democratization of surveillance as a result of low cost and ease of use can introduce a healthy pluralism and balance (as well as reciprocal inhibitions in use for fear of retaliation). On the other hand this may also help create a more defensive and suspicious society with an overall increase in anxiety-generating and resource-consuming surveillance and counter-surveillance. ²⁰

The equal application of questionable means can hardly be cause for celebration. The value on equality here is not the usual one of valuing it for its own sake. It is more instrumental in that equality of access can serve as either a deterrent to misuse or as "turn about is fair play."

We can also apply a principle of consistency which asks whether the tactic is applied to everyone (which is different from asking what if everyone applied it?) Here we ask about

equality within a setting-is the tactic (particularly if it is controversial) applied to all, or only to some (usually those lower in status)? For example are executives drug tested and are their phone and e-mail communications subject to monitoring just as other employees? If a bitter pill must be swallowed on behalf of some presumably greater communal good, it seems easier administratively and fairer if all share the cost, rather than the least privileged or those least able to resist. If there is inequality we need to ask whether the rationale for differential applications is clear and justifiable.

Finally we need to consider (in the absence of being able to just say "no") whether there are means available that make it possible for people to maintain greater control over their personal information and if so, how widely available these are. Some means such as providing a false name and address when the request is irrelevant (as with paying cash for consumer electronics) or free anonymous E-mail forwarding services are available to anyone. In other cases privacy may come with a price tag-as with the purchase of a device for shredding records, having an unlisted phone number or possessing the technical skill to encrypt one's email or telephone communications.

2. The symbolic meaning of a method: What does the use of a method communicate more generally? Some practices simply look morally objectionable because they deeply violate a fundamental principle, such as respect for the dignity of the person. Something much broader than the harm to a particular individual may be involved. There is a sense in which a social value is undermined and the community as a whole may be harmed.²¹ This also has major implications for political action. As Priscilla Regan (1995), observes until privacy infringements come to be defined as social, rather than simply individual violations, the political will for strong privacy legislation will be lacking.

3. The creation of unwanted precedents: Is it likely to create precedents that will lead to its application in undesirable ways? Even if a new tactic seems otherwise acceptable, it is important to apply a longer range perspective and consider where it might lead. The social security number which has become a de facto national identification number, which Congress clearly did not intend when it was created, is an example.

4. Negative effects on surveillors and third parties: Are there negative effects on persons other than the subject? For example, what is the impact on the personality of a professional watcher or infiltrator? Super electronic sleuth Harry Caul in the film "The Conversation" is suggestive. Over the course of his professional career Caul becomes paranoid, devoid of personal identity and desensitized to the ethical aspects of surveillance. In another example, there is some evidence that police who use radar guns in traffic enforcement have higher rates of testicular cancer. Audio and video taping may record the behavior of suspects, as well as that of their family and friends. Surveillance tactics often have consequences beyond their intended target and their possible implications for others needs to be considered along with the possibility of mitigation.

Uses of Surveillance Data

Let us move from the tactic itself and the social context in which information is collected to its actual use. The first two may be ethically acceptable even as the uses to which the data are put are ethically unacceptable.

One approach is to adopt a principle of proportionality in which means and ends stand in appropriate balance. For example one does not use a sprinkling can to put out a house fire, nor

a sledge hammer to crack open a nut. The danger is that the more important the goal, the greater may be the acceptance of means that are less than ideal.²²

This principle encourages us to think comparatively about means. Where a less than ideal means is preferred we need to ask "Are other less costly means available?" Where they are not and the costs of the favored means are great, we need to ask "What are the consequences of taking no action?"

Obtaining consensus on either the importance of the goal or the costliness of the means is not an easy task in a heterogeneous society. I am not suggesting that the ends should justify the means, but in other than extreme cases, they are certainly relevant to a consideration of the means. Where means involve significant risks and costs, the case needs to be affirmatively made for why their use is appropriate given the goal and for the steps that are taken to minimize costs and risks.

Another related approach is to consider the type of goal and who benefits from achieving the goal. Thus it is easier to justify crossing a personal border when the goal serves the community rather than the personal goals of the data gatherer. For example a recent requirement that prospective air passengers provide personal identification or submit to x-ray body searches is undertaken for broad community serving goals. This action is also intended to serve the presumed goal of the individual flyer. Equivalent surveillance undertaken by a merchant is morally much less compelling since it directly benefits neither the community nor the individual. Similarly a ban on smoking in public places in which the goal is to protect non-smokers seems easier to justify than a ban on employees smoking outside of work, in which the goal is to lower company healthcare costs.

In considering goals it is easier to identify relatively non-controversial positive goals such as productivity, health protection, and crime prevention than it is to assess their relative importance. It is often more difficult to identify questionable goals, since by their very nature they are less likely to be publicized (e.g., DNA insurance exclusion examples based on future predictions). Questionable goals may involve an effort to force an employer's morality, politics or opposition to unions onto employees, to circumvent established procedures; or it may be an unreasonable quest for profit or strategic gain on the part of personal data-mongering entrepreneurs, illogic or ignorance.

The gray area here is large, even if cases at the extremes are clear. For example is use of a pulmonary lung test to measure whether employees are not smoking (in conformity with a company's non-smoking policy) a necessary health and cost-saving measure good for both the company and the employee, or is it a wrongful crossing of the boundary between work and nonwork settings? We also need to be alert to the possibility that the publicly-stated goals may mask other less desirable goals. Even when that is not the case, moral worth must be sought in the consequences of the use beyond the good intentions of those applying the technology.

To help in assessing the "use" issue the following questions need to be asked. Other factors being equal, the first response suggests an ethical use and the second an unethical use. 1. Appropriate vs. inappropriate goals: Are the goals of the data collection legitimate? Are they publicly announced? Consider the following contrasting cases * drug testing school bus drivers vs. junior high school students who wish to play in the school band * a doctor asking a female patient about her birth control and abortion history in a clinical setting vs. asking this of all

female employees (as one large airline did) without indicating why the information was needed * asking about the religious beliefs and practices of prospective clergy vs. asking this of prospective factory workers * a polygraph examiner for a national defense agency uses his knowledge of female job applicants to offer advice about hiring vs. another examiner who in addition uses the extensive personal data collected to decide who to date 2. The goodness of fit between the means and the goal: is there a clear link between the information sought and the goal to be achieved? How well a test measures what it claims to--drug and alcohol use, miles driven, or location -can be differentiated from second- order inferences made about goals only indirectly related to the actual results of the measurement. A measure can be valid without being effective. As we move from the direct results of a measure that is immediately meaningful given the goal (e.g., a drug test to determine whether a person has abided by the conditions of his/her parole), to more remote inferences about goals, questions may arise. For example, some research suggests that drug tests may not be associated with the employment performance behaviors they are presumed to predict. In that regard a test for transportation workers that directly measures reflexes is preferable to a more inferential drug test. 3. Information used for original vs. other unrelated purposes: is the personal information used for the reasons offered for its collection and for which consent was given? Do the data stay with the original collector, or does it migrate elsewhere? For example the results of medical tests undertaken for diagnostic and treatment purposes may be sold or otherwise obtained by potential insurers, pharmaceutical companies and employers, to be then used for their own goals?

Using data for unrelated purposes may violate the individual's expectations for full disclosure and data security. When information is used without permission for other purposes we need to ask was this done with prior planning by the original gatherers or by others who bought, found, stole or deceptively obtained the data. For the original collectors there is a responsibility to keep both their word and to protect confidentiality. 4. Failure to share gains from the information: are the personal data collected used for profit without permission from, or benefit to, the person who provided them (or at least participated in their generation)? This implies a private property defense of personal information and contrasts with a definition based on universal human or democratic citizenship rights. To sell another person's information without asking him or her and without letting the supplier share in the gain might even be seen as a kind of theft. The issue of ownership of personal information raises novel copyright issues, e.g., involving sale of information about a person's purchases or a clone of the person's cell structure. 5. Unfair harm or disadvantage: Is the information used in such a way as to cause unwarranted harm or disadvantage to its subject? There is of course much room for debate over whether these occur and whether they are warranted. Yet some major types can be identified and extreme examples are easy to find: a) an unfair strategic disadvantage or advantage with respect to a situation in which there is a conflict of interest (for example a bugged car sales waiting room which permits the seller to learn a customer's concerns and maximum payment) b) unfairly restricting social participation as in denying someone an apartment, insurance coverage or employment based on information that is invalid, irrelevant, acontextual, discriminatory, (e.g., not hiring someone because their DNA suggests they have a better than average chance of developing a serious illness in the future, or not renting to someone because of the person's ethnic background) c) the unwarranted publication or release of personal information that causes

embarrassment, shame, or otherwise puts a person in a negative light. The emphasis here is on the subjective harm the individual experiences as a result of the release of confidential information, apart from its validity.²³ State laws that protect against the "tort" of privacy invasion apply here. Direct, tangible, material harm can more easily be determined than subjective harm involving embarrassment, shame, stigma, humiliation and the creepy feeling of being invaded.²⁴ d) betrayal of confidence. The failure to maintain confidentiality and security or to use information only as promised applies here. This can involve friends telling something they shouldn't, violations of professional confidentiality, a phone company revealing unlisted numbers through a new service such as caller-ID, or malicious acts (whether by data custodians or transgressors) such as informing persons that medical tests for HIV were positive when that wasn't the case. e) intrusions into solitude. An important element of privacy is the right to be left alone in a busy world. The indiscriminate traffic in personal information may result in unwanted mass marketing and other communications intrusions via telephone, mail, email, or face-to-face solicitations. f) manipulation and/or propaganda appeals based on hand-tailored very specific messages designed for narrow-casting, segmented marketing. Such messages may be more effective than general broadcasting aimed at an undifferentiated mass market. Consider a candy company's mailing to diet workshop participants of a special discount offer.²⁵ The issue here (and with a number of the other issues) is not whether data collectors and users have a legal right to such actions (they clearly do) but rather is it the right thing to do? g) use of communication resources without permission such as sending unsolicited faxes, calling a cellular phone number (which requires the recipient to pay) and flooding an E-mail address with unwanted messages ("spamming") which can disable a system.²⁵

But Where is the Normative Argument?

A reviewer of this article, perhaps coming from a background in academic philosophy, was critical because many of its' conclusions about ethical behavior (however qualified) are not adequately grounded in a formal normative argument that offers justifications for the principles, indicates their logical implications and leads to clear conclusions. Such an argument would anticipate and respond to likely objections and would be consistent across types of justification (for example it would not mix arguments based on categorical first principles with those based on empirical consequences as is done here.)

Nice work if you can get it! While some philosophers may lust after a Rosetta stone of clear and consistent justifications, a central argument of this paper is that in matters so complex and varied we are better served by an imperfect compass than a detailed map. Such a map can lead to the erroneous conclusion that ethical directions can be easily reached or to a statement so far in the stratosphere that only angels can see and apply it. Maps of uncharted terrain are hard to come by. A chart of new territories needs to begin with simple coordinates and rough estimates.

Given the variety of tactics for extracting personal information and the conditions under which they are applied, an ethics of surveillance must be very general. Categorical imperatives mandating prohibition, or use, based on a single overriding principle are difficult to defend. It is unrealistic to expect a general principle to apply equally in all contexts and across all technologies. But we can talk in relative terms and contrast tactics, situations and uses as being

more or less ethically acceptable depending on the interplay of the factors discussed.

The questions asked here about the means, data collection, context and use offer an ethical guide for assessing surveillance tactics. The more the principles implied in these questions are honored the more ethical the situation is likely to be, or conversely the fewer of the principles respected, the less ethical the surveillance. I intend this additive approach as a sensitizing strategy and do not suggest that equal moral weight necessarily be given each factor. But hopefully they do take into account the major ethical elements.

There are no simple evaluative formulae for the varied and complex situations in which personal data are collected and used. Suggesting an ethics for a particular tactic such as computer databases or drug testing can be worthwhile in offering more focused guidelines, but it is also important not to ignore the commonalities or the broader social picture. Regardless of the tactic, asking the 29 questions in Table 1 will hopefully yield better results than ignoring them.

The 29 questions in this table summarize the argument of the paper. I think they should be asked when considering the ethics of any surveillance activity. They can help answer the question "is it right or wrong?" While each of these questions implies broader normative justifications, I have not taken this further (beyond space and my own limitations) because the analytic distinctions and hypothesized empirical factors offered here are a necessary first step before a more formal ethics of surveillance is possible (if ever). This paper is about the societal norms that I believe both do and should inform an ethics for surveillance. More systematic empirical research and a more rigorous and consistent set of arguments supporting or attacking the above is most welcome.

Yet underlying these questions are a cluster of value justifications. The most overarching and important is the Kantian idea of respect for the dignity of the person. When the self can be technologically invaded without permission and even often without the knowledge of the person, dignity and liberty are diminished. Respect for the individual involves not causing harm, treating persons fairly through the use of universalistically applied valid measures, offering meaningful choices and avoiding manipulation and coercion. These in turn depends on being adequately informed. Viewing personal information as something the subject has a property right in (not unlike a copyright) can be an independent justification, but autonomy over the use of one's information also shows respect for the person. Another major value is trust and its implications for community. When trust is violated through deception or the failure to honor agreements and implied contracts in data collection, the value of community is undermined.

Twilight or Dawn?

The new technologies require new cultural standards and public policies even as they offer wonderful possibilities. Yet they are also reminiscent of Franz Kafka's short story *The Penal Colony* in which a prison officer invents a sophisticated machine for punishing inmates. The story ends with the officer being killed by the machine he created. There is no guarantee that hard-won rights will stay won or be extended in the face of continual social and technical change-absent knowledge, wisdom and vigilance.

Former Supreme Court Justice William O. Douglas has written that the Constitution and the Bill of Rights "...guarantee to us all the rights to personal and spiritual self-fulfillment. But

the guarantee is not self-executing. As nightfall does not come at once, neither does oppression. In both instances, there is a twilight when everything remains seemingly unchanged. And it is in such twilight that we all must be most aware of change in the air--however slight--lest we become unwitting victims of the darkness." (Vrofsky, 1987). We are in such a time period now with respect to new information technologies.

There is the possibility of becoming an even more stratified society based on unequal access to information in which individuals live in glass houses, while the external walls of large organizations are one-way mirrors. There is a significant (and perhaps growing gap) between the capabilities of the new surveillance technologies and current cultural, legal and technical protections.

Powerful social and psychological forces work against any easy assumptions that a decent society is self-perpetuating. The masthead of a black civil rights era newspaper in Sun Flower County, Mississippi reads "Freedom is a Constant Struggle". This heralds an important truth. There are no permanent victories in democratic society. As past and contemporary events of this century indicate, liberty is fragile.

Notes

1. This article extends a paper delivered at the 1996 University of Victoria conference on "Visions of Privacy in the Twenty-First Century". It is part of a broader project based on the Jensen Lectures delivered at Duke University which will eventually appear in *Windows Into the Soul: Surveillance and Society in an Age of High Technology*. I am grateful to Hugo Bedau, Richard Leo, Helen Nissenbaum, Greg Ungar, Mary Virnoche and Lois Weithorn for their critical reading and suggestions. The paper was prepared while the author was a Fellow at the Center for Advanced Studies in the Behavioral Sciences. I am grateful for financial support provided by the National Science Foundation Grant # SBR-9022192.
2. A more developed statement of the new surveillance and its expression in the maximum security society can be found in ch. 10 of Marx (1988). See also the discussions in Rule (1973); Foucault (1977); Laudon (1986); Clark (1988); Lyon (1994 and 1996) and Gandy (1993).
3. Canadian Standards Association (1996), Bennett (1995). For related discussions see Flaherty (1989), Bennett (1992) Regan (1995) Smith (1994).
4. Our discussion is based on conventional domestic settings in a democratic society for those with full adult citizenship rights. In situations of extreme crisis such as war, when dealing with very different countries or cultures, children, the ill, the incompetent or those juridically denied certain rights such as prisoners, a different discussion is needed and the lines in some ways will be drawn differently. That however does not negate the value of the principles to be discussed here as ideals that should apply more broadly, other factors being equal.
5. There is an interesting conflict here between discriminate and indiscriminate use of a technique.

Categorical application of a means such as drug testing to all employees (including managers) satisfies a value of equality and universalistic treatment. But given its invasive nature, it violates the principle behind the Fourth Amendment that there must be some reasonable grounds for suspicion before a personal border is crossed.

6. The fact that something is not bad does not necessarily make it good. The idea of doing good is implicit in calling for appropriate goals. But given the moral component of both means and ends a good goal is never enough, any more than is a good means apart from its use.

7. The issue of harm to a group rather than to an individual has received scant attention. As the idea of group as against individual rights gains increased prominence, we will no doubt see more attention to the former. One form is the damage to community that occurs when trust is violated. Another is the damage via stigmatization and discrimination that can effect a specific group if it is labeled as having a statistical tendency toward some undesirable outcome. Genetic testing is a case in point.

8. One must avoid the demonology and glorification involved in viewing data gatherers as invariably up to no good and surveillance subjects as helpless victims whose rights are always trampled. Yet given the tilted nature of the private sector playing field in which powerful interests and organizations are relatively unopposed in emphasizing their rights to gather and use personal information rather than their duties, my emphasis is on creating an ethics that applies to those doing the surveillance. Yet it is also well to note that we all play multiple roles and rotate between being surveillers and surveilled, if hardly equally.

9. This becomes even stronger when the polygraph is applied in such a fashion as to intimidate, as recommended by some early instructional manuals.

10. For example see Bok 1978.

11. Of course the concept of harm, whether in the collection or use of the data, can be made problematic: should harm be measured objectively or subjectively and how should we respond to individual and cultural differences in defining it? This warrants caution and reflection. However it is a moral cop-out to use cultural relativism to deny that the definition of harm must never transcend varying group and individual definitions. In that regard currently popular pay for level of privacy schemes must not be accepted uncritically. This broad imperative may conflict with that of choice. But what is life without interesting complications?

12. However as Winner (1988) notes there are conditions under which some technologies clearly have political and social (and by indirection) ethical implications. For example the decision to use nuclear power will of necessity imply centralization and high levels of security. Enormous capital expenditures in the creation of a system will exert pressures to continue it.

13. Even then it is inconsistent. For example in *Delaware v. Prouse*, 1979 the Court held that

warrantless searches of luggage on a train by sniffing dogs violated a reasonable expectation of privacy. But that was not the case with dogs sniffing luggage at airports (U.S. v. Place, 1983).

14. I use the method of analytic induction (Katz, 1983) in which one starts with empirical cases and asks if they can be coded within the categories. In this case I have drawn on examples gathered over the last decade and the useful compilations in Smith (1993 and 1997) and Kennedy and Alderman (1995). In dealing with these more general organizing concepts the key point is not whether any given story/instance is factually correct (although that is vital for journalists or lawyers), but whether the concepts adequately capture the range of events. Sometimes the restriction is on the technology as such (as with parabolic mikes) and other times on the type of record (e.g., video rental but not book or medical records). In federal and most state jurisdictions secretly recording sound is a legal infringement, but a secret video recording is not, at least not yet. In the absence of an agency to anticipate and recommend policy changes (as is found in Canada and Europe) in response to new technologies the most common pattern is one of invasive practices often followed by legislation.

15. Helen Nissenbaum (forthcoming) offers a useful conceptualization of this problem of privacy in public. 16. Failure to block this may make future visits to the site easier, but also makes possible using one's viewing behavior for marketing purposes and even invites the potential exploration or alteration of the contents of the hard drive.

17. In the former there may be no choice but to follow Arlo Guthrie's words in "Alice's Restaurant" to "walk in" and get "inspected, detected, infected, neglected and selected". This of course can be mischievously defined as choice.

18. For example in an early Massachusetts computer matching case a list of those on welfare was compared to a list of those with more than \$5,000 in the bank (the cut off point for being on welfare). Those on both lists had their welfare payments automatically terminated with no further checking. Among cases inappropriately cut off were a woman whose money was legally held in trust to be used for her funeral expenses and a student who had temporarily deposited his student loan money in his mother's account while waiting for school to start (Marx and Reichman, 1984).

20. In a related fashion it might also be argued that the more expensive and difficult to use a technology is, the greater the disincentives to use it and the less frequent its use. From this perspective the real problems (at least quantitatively) begin when tactics become widely available (as with miniature voice or motion activated audio or videotape recorders hidden in familiar objects). Yet given what we know about the temptation to abuse power, in the absence of this, one can hardly be optimistic about elite monopolization over a technology.

21. We have emphasized how surveillance may cause unjustified harm to the individual. As well we should give some consideration to the reverse—the abuse or erroneous use of surveillance data that helps an undeserving individual. For example a police chief in a small town (in an

anti-surveillance move) erased his son's record of drunk driving from the computer. However the latter is much less likely to come to public attention and seems to have less moral bite (that is, the cost of unfairly helping someone does not seem as great as unfairly hurting them). Of course in zero-sum situations these are related (altering data so that a less deserving person gets a job denied a more deserving person). But much of the time the harm is to an impersonal and the damage done is symbolic. It offends shared values. The social costs of having a bad driver on the road can be great but are likely to be more distanced, and not initially centered on harm to a particular person.

22. In simplified form, combining degree of importance for goals and risks/cost for means suggests four types. The moral implications of using a costly means for an unimportant or undesirable goal, or a non-costly means for an important goal, are clear. What is more difficult and interesting are cases where the goal is very important and the means very costly.

23. This could be greatly elaborated. Consider for example the harm from a pseudo-personalized mass mailing that begins by congratulating persons assumed to be parents on their child's first birthday. The goal of the advertizing is to sell them things a one year old now needs. The data has been purchased from health care providers. How does a couple who had a miscarriage that is not reported feel when they automatically receive such solicitations? Such insensitive mailings (an actual case) can cause a particular kind of harm. Or consider a mass mailing to recently retired persons advising them of the advantages of cremation over burial. Certainly this is not an issue to run to the barricades over, but it does suggest the kind of subtle manners question that the purchasers of databases ought to consider.

24. Here we need to separate embarrassment caused by an invalid result (for example having an alarm go off by mistake as one walks through a detection device in a store or library) from accurate results. But even the latter can be troubling if confidentiality is due and is not respected. One of the grounds for non-public figures suing for privacy invasion is to be put in an unfavorable public light, even if true.

25. Of course if phone numbers or addresses are obtained by simply calling every possible number or mass mailings to occupant via regular post, the situation is different. Under normal circumstances it is hard to imagine prohibiting mail or phone messages (although there could be various schemes to increase the cost to the sender of the communication and technologies are available for screening). The recipient is certainly under no obligation to respond. This is also an issue of manners and evolving expectations (e.g., re what appears to be a hesitancy on the part of marketers to call cells phones).

Bibliography

- Clarke, R. 1988. Information Technology and Dataveillance. *Communications of the ACM*.31: 29-45.
- Bennett, C. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the*

- United States*. Ithaca, N.Y.:Cornell University Press.
- 1995. *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association*. Rexdale: CSA.
- Bok, S. 1978. *Lying: Moral Choice in Public and Private Life*. Lying: New York: Pantheon.
- Chandler, R. 1991. *The Big Sleep*. New York: Random House.
- Flaherty, D. 1989. *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.
- Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison*.
- Gandy, O. 1993. *The Panoptic Sort*. Colorado: Westview Press.
- Katz, J. 1983. "A Theory of Qualitative Methodology: The Social System of Analytic Fieldwork" in R. Emerson, (ed.) *Contemporary Field Research*. Prospect Heights, Ill.: Waveland Press.
- Kennedy, C. and Alderman, E. 1995. *The Right to Privacy*. New York: Knopf.
- Laudon, K. 1986. *The Dossier Society: Value Choices in the Design of National Information Systems*. New York: Columbia University Press.
- Lyon, D. 1994. *The Electronic Eye The Rise of the Surveillance Society*. Cambridge, England: Polity Press.
- Lyon, D. 1996. *Computers, Surveillance and Privacy*. Minneapolis: Univ. of Minn. Press.
- Olmstead v. United States, 277 U.S. 438 (1928).
- Marx, G. 1988. *Undercover: Police Surveillance in America*. Berkeley, Ca.: Univ. of California Press.
- 1994 "New Telecommunication Technologies Require New Manners," *Telecommunications Policy*. Vol. 18:
- Marx, G. and Reichman, N. 1984. "Routinizing the Discovery of Secrets: Computers as Informants." *American Behavioral Scientist*. Vol. 27: 423-452.
- Nissenbaum, H. forthcoming. "Toward An Approach to Privacy in Public: Challenges of Information Technology", *Ethics and Behavior*.
- Radin, M.J. 1996. *Reinterpreting Property*. Chicago. Univ. of Chicago Press.
- Regan, P. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press.
- Rule, J. 1973. *Private Lives, Public Surveillance*. London: Allen-Lane.
- Smith, J.1994. *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: Univ. of North Carolina Press.
- Smith, R.E. 1993 and 1997. "War Stories. Vol. I and II." Providence, R.I.: Privacy Journal.
- Vrofsky, M., ed. 1987. *The Douglas Letters*. Bethesda, Md.: Adler and Adler.
- Winner, L. 1988. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: Univ. of Chicago Press.

To obtain a sample copy of The Information Society (TIS), choose one of the following:

Print the form below and mail to the Taylor & Francis Office nearest to you. In North America, send email to: sample-tis@taylorandfrancis.com Outside North America, fill out an electronic form that is available via Taylor & Francis' web site. Follow the path to "sample copy".

To purchase individual copies of The Information Society (TIS), visit the Taylor & Francis Journal Ordering Page. Single back issues are available for each journal, the price being obtained by dividing the institutional subscription rate by the frequency + 10%, which is currently about US\$42 (as of early 1999).

Contact Peggy Pagano, Journals Manager ppagano@taylorandfrancis.com OR 1-800-821-8312 (EXT.117) OR 215-269-0400, OR FAX: 215-269-0363.

Taylor & Francis retain a 2 year back stock of journals. Older volumes are held by our official stockists: Dawson (UK)Ltd, Back Issues Division, Cannon House, Folkestone, Kent CT19 5EE, UK to whom all orders and inquiries should be addressed. Tel: +44 (0) 1303 850101; Fax: +44 (0) 1303 850440.

To subscribe, clip the following form and mail to the address below:

THE INFORMATION SOCIETY
Published quarterly, ISSN 0197-2243

- Please enter my institutional subscription at US\$140 (starting with vol 15)
 Please enter my personal subscription at US\$69 (starting with vol 15)
 Please send me a free sample copy

Payment options:

Check/Money Order Enclosed
(please make checks payable to Taylor & Francis, US\$ only)

Please charge my: VISA MC Amex
Card # _____ Exp date: _____
Signature: _____
Telephone: _____
(required for credit card purchases)

or BILL TO: (please print)

SHIP TO (if different):

Name _____
Institution _____
Address _____
City _____
State _____ Zip _____

Name _____
Institution _____
Address _____
City _____
State _____ Zip _____

Mail this form to:

Taylor & Francis Inc.
47 Runway Road
Levittown, PA 19057
Toll free- 1-800-821-8312 or
Phone- 215-269-0400
Fax- 215-269-0363

Outside the U.S. contact:

Taylor & Francis Ltd.
Rankine Road
Basingstoke, Hampshire
RG24 0PR, United Kingdom
tel: +44 (0) 256 840366
fax: +44 (0) 256 479438