G.T. Marx, draft 1/13 11,112 + 1822

This was originally Ch. 16 significantly shortened became Ch. 13 of *Windows Into the Soul.*

Ch. 16

An Ethics for the New (and Old) Surveillance

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

--popular expression

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

--M.I.T. student

This chapter stresses the difficulty of applying a single set of ethical standards to the rich variations in surveillance behavior and settings. As noted, to a significant degree, evaluations are contingent upon the context and the behavior within it.

The chapters in the first three sections of the book Chapters (1-9) sought social science objectivity. Those are my team’s rules. Yet at the end of a project dealing with social issues, the scholar who reports only the findings but fails to evaluate them runs the risk of moral abdication. The righteous witness of course faces others risks.

Underlying this inquiry and interlaced with the empirical questions are moral concerns. Is a given practice good or bad, desirable or undesirable? How should the new surveillance forms be viewed –as efficient, equal opportunity, scientific tools of productivity and protection in the face of ever-greater crises, or as crepuscular, sugarcoated tools of domination? A related question: how should neutralization efforts be viewed –as courageous and inspiring expressions of the human spirit in the face of the soulless domination of the machine in the service of the more powerful, or as sneaky and disheartening expressions of self-interest on the part of those who are inadequately socialized and disrespectful of the community’s rules?

These questions are at the core of surveillance as a contemporary issue. However, posing questions in such a general way is not helpful. The only honest answers are, “yes and no,” “sometimes,” and “it depends.” The empirical and normative task for etiquette, policy and law is to suggest what the evaluation of surveillance does, and should, depend on.

What’s Wrong With This Picture?

Public opinion polls consistently show that a very large percentage of Americans and indeed persons everywhere are concerned about surveillance issues (Zureik et al, 2010 provide international data, Westin (2003) summarizes many U.S. polls). But the elements of this concern are rather muddled, muddied and inconsistent. Many persons feel a sense of discomfort in the face of indiscriminate drug testing, hidden video cameras, electronic work monitoring, airport screens and the collection and marketing of their personal information--even as they favor security, responsible behavior, efficiency, economic growth and credit-card-aided consumption. Given the newness of the technologies, opinion here is less well defined and coherent than is the case for many more settled issues.

Persons often have trouble articulating what seems wrong with a surveillance practice beyond saying that it doesn't seem quite right –often with a vague reference to the invasion of privacy. What's the fuss all about? What is it about the new technology that is troubling, and why is it difficult to take a consistent position? By what standards should we conclude that a given practice is right or wrong or at least desirable or undesirable? How should surveillance activities be judged? Where is contention most likely to be found, and what does it involve?

Popular expressions such as, "if it doesn't look right, that's ethics" and "you don't treat people that way" speak to ethics embedded in folk culture. Data gathering and protection efforts imply ethical assumptions that are often unstated. In what follows I suggest an ethical framework for thinking about the surveillance of individuals whether involving the new or traditional means (e.g., such as informing and eavesdropping). At a very general level there are shared expectations in American culture, and perhaps to a degree more generally in western and industrial-capitalist cultures, whose violation underlies the discomfort, or at least ambivalence, experienced in the face of many personal border crossings.

This chapter suggests some basic questions for identifying factors that would lead the average person to view a surveillance practice as wrong or at least questionable --whether in general or in a specific case (or conversely, that it is acceptable). The chapter ends with a consideration of the values these questions imply.

The questions for judgment in this chapter build on efforts to inductively define *surveillance* and related terms such as *privacy* and *publicity*. In such efforts the analyst starts with an array of behaviors seen as right or wrong and builds up to some more general categories. William Prosser (1960), the godfather of this approach for privacy issues, sired an abundance of offspring. Among the most fulsome is the encyclopedic work of Daniel Solove (2008). Rich examples are also found in Alderman and Kennedy (1995), Smith (1993, 1997), Privacy Rights Clearinghouse (2011), and EPIC (2011). To illustrate a range of surveillance problems, I draw from the their examples, my interviews and participation in various policy inquiries, court cases and mass media accounts. The disparate violations or behavioral intrusions can be systematically located within a broader, real world field corresponding to the surveillance occasions and contexts noted earlier.

Have We Got Questions

This chapter's ethical analysis emphasizes the watchers rather than the watched, the potential harms that can result from the watching, the potential harm to the individual rather than the group or organization, the short rather than the long run, and domestic, non-crisis uses rather than exceptional and emergency uses. However, many of the ideas can be applied more broadly.

The perspective I offer applies to conventional domestic settings in a democratic society for those with full adult citizenship rights. In situations of extreme crisis such as war and pandemic or when dealing with very different countries or cultures, the incompetent and dependent, or those denied juridical rights such as prisoners, a somewhat different discussion is needed, and the lines in some ways will be drawn differently. Such cases of course call for extreme vigilance, but they also present a danger of exploiting the fear and of normalizing states of exception.[1]

The ethics and/or wisdom of a practice can be assessed at each stage of the surveillance occasion noted in Chapter 6 and with respect to their larger milieu. In most cases the evaluation questions presented (Table 1) are structured so that answering "yes" is likely to support a broader value and related principle. Given the book's emphasis on variation and complexity, no simple additive score is possible. Much depends. Yet other factors being equal, the more these questions can be answered in a way that affirms the underlying principle (or a condition that supports it), the more ethical and wise the use of a tactic is likely to be. This is often, but not always, in the form of a "yes" answer.

The Fair Information Practice Principles and Beyond

Many of the topics in this chapter come from the Fair Information Practice Principles developed in 1973 by the U.S. Dept. of Health, Education and Welfare. This pioneering effort sought to inform ethics and policy regarding privacy and computerization.

This approach fit well with the concerns of the early decades of computerization. More recently, based on work by Colin Bennett (1995) and others, the guidelines have been expanded to include principles of accountability; purpose identification; openness, collection limits, use, disclosure and retention limits; accuracy; safeguards; individual access; and compliance challenges. The expansion, which added issues related to publicity, complaint and compliance, is an advance over the minimalist standards of the earlier period.

However, the guidelines are too narrowly focused on issues of computers and privacy. The information highway is not the only road out of (or into) people's lives.

Privacy conceived of as an individual right to control electronic information is hardly the only important consequence, nor are computer databases the only technology. The essence of the fair information practice code involves informed consent, unitary usage and non-migration of data. These are essential components, but they are of little help with respect to reaching conclusions about the ethics of a given means, comparing means, or evaluating the appropriateness of the original goals and many of the actual processes of data collection and analysis. Nor are they much help with respect to broader issues such as the procedures for setting surveillance policy and long term consequences for subjects, agents and society.

When the principles were developed, computers were the only game in town, and the *collection,* or *meaning*, of data entered into computers (such as a biographical fact or a transaction) was usually not at issue. However collection and meaning are issues for techniques such as urine drug testing, found DNA and thermal imaging. Even for computers, as we move from data entered by an operator at a terminal to remote, automatic, involuntary entries based on visual, auditory and biometric forms of data, questions over the appropriateness of the initial data collection will become increasingly important.

The Fair Information Practice guidelines are not sufficient for many of the new technologies, uses and users, nor for some of the phases of the surveillance occasion. The questions suggested next (most of which can also be stated as principles) offer a broader framework.

Questions are organized according to the following categories: initial conditions; means; goals; connections between means and goals; data collection and analysis; consequences for subjects and others; rights and resources for subjects; consequences for agents and third parties; and data protection and fate. Table 1 lists the questions.

Table 1 here about

Initial conditions: Policies, Procedures and Capabilities

Formal procedure and public input in the decision to adopt: Does the decision to apply a potentially sensitive technique result from an established review procedure in which affected parties (whether within or beyond the organization) are consulted? For example, are the conditions of computer and telephone work monitoring developed through a joint management-union or worker's council committee? Is the introduction of a new technology for delivering unlisted phone numbers subject to broad review via citizen input and a regulatory commission, or simply offered by technological fiat, as caller-ID initially was. Is a decision to introduce video cameras onto highways and public streets discussed by the city council and interested parties?

An important initial policy tool here is the *privacy impact* (or more broadly surveillance) assessment statement (Wright and de Hert 2012). Such inquiries consider a project’s feasibility, goals and a range of possible consequences based on prior experience, research and best estimates –with input from an array of those deemed to be “stakeholders.”

The extent of discussion and procedures followed in considering whether to adopt a tactic need to be factors in evaluation, apart from the tactic’s instrumentality. The presence of established procedures can serve as a brake on excessively fevered enthusiasm and can contribute to accountability and legitimacy and broaden the range of factors considered. When appropriate, giving “stakeholders” a chance to participate communicates respect for them and also serves as a form of notice, if not necessarily consent. Just who is judged to be a stakeholder can of course be contentious and depends on the context and its rules.

Also, in deciding whether to adopt a tactic, agents needs to consider questions involving role reversal, restoration, unwanted precedents, symbolic meaning, reversibility, written policies, and agency competence and resources. These broader factors stand apart from the specifics of the tactic.

Role reversal: Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects if roles were reversed? How would the agents who are now in the role of subjects view efforts to neutralize surveillance? This is an aspect of the golden rule, but one restricted to an imagined shift in the organizational role played. It relates to Kant’s consistency or reciprocity principle, which asks more broadly, “what if everyone used the means?”[2] This question reflects an aspect of equality (“turnabout is fair play”), but it may also have an instrumental quality as actors moderate their own behavior out of concern for receiving the same behavior in kind if situations were reversed. As Georg Simmel (Coser 1956) noted, in spite of intense conflict, those in opposition may share some standards and sentiments, or at least have some common interests.

Restoration: Does the proposed technique radically break with traditional protections for personal information? Can, and should, these traditional protections be re-established through other means (whether legal, informal expectations or technical)? Consider for example caller-Id in potentially ending the anonymity of the caller; infra-red or x-ray means that "see" through walls, clothes and skin; the revelation of potentially embarrassing or at least very private facts when hard to locate data become instantly available from online searches. or when mosaic images of the person are created by combining data that were previously scattered. The sudden omnipresence of accessible wireless cell phone and Internet data and the ease of third-party uses of data voluntarily provided (or at least that which the individual does not "choose" to protect) are further examples. It seems likely that the anti-wiretap protections that were gradually extended to wired communication in the 20th century will be extended to aspects of wireless communication in the 21st not now covered..[3]

An important strand of surveillance policy deals with re-establishing the conditions deemed worthy of protection before the development of the tool. Such changes relate to the interesting issue of the meaning of "reasonable" as expressed in the Supreme Court's (Katz) reasonable expectation of privacy standard. Reasonable should refer to the societal definition of appropriateness, not to what can reasonably be expected given public knowledge of what the technology can do.

Under some conditions restoration may not be desirable or possible, but then advocates must make the case for why undermining or outright destruction of the status quo is appropriate.

Unwanted precedents: Is the tactic likely to create precedents that will lead to its application in undesirable ways? What unwanted consequences might the tactic have for subjects, agents, third parties and society more broadly? Even if a new tactic is deemed effective, advocates must apply a longer-range perspective and consider where it might lead. The earlier discussion of surveillance creep or escalation and possible latent goals applies here. These questions need to be considered before a tactic is adopted.[4] How might traditional liberties and basic democratic values be affected? Will a tactic lead opponents to turn to the same tactic? Will agents face new risks? Once the foot is in the door, where might it lead? Is the slope slippery, or are there bumps and even barricades in the road?

Legislatures and organizations generally initiate a surveillance strategy (e.g., speed cameras at street intersections or metal detectors in high schools) with defensible goals in settings where a problem is seen to exist. However, surprising precedents that are subsequently established, undisclosed goals and unintended impacts are no less important to consider for being so much less visible. They need to come out from the shadows and be imagined as part of the decision process. Hindsight is unfortunately more available than foresight, and unintended consequences are often visible only over time. But lessons can be learned from experiences in other settings and countries. Explicitly asking about experiences elsewhere is a necessary component of impact assessment, as is imaging what might go wrong.

Two additional questions to be asked in the initial decision to adopt involve symbolic meanings and reversibility.

Symbolic meaning: Do the tool and the way it is applied communicate a view of citizens who are due respect and with rights appropriate for a democratic society? Or is the individual subject viewed as an object without rights who must be subservient to the interests and greater power of an organization entitled to apply invasive and even degrading techniques in any way it chooses?

The standards for assessing symbolic communication are more subjective than for many of the other questions. But asking if it “looks right” is a beginning. Some practices appear morally objectionable because they violate a fundamental principle such as respect for the dignity of the person. For example, the categorical suspicion associated with the indiscriminate application of a sensitive tactic implies that subjects are guilty until proven otherwise.

Reversibility: if experience suggests that the policy is undesirable, how easily can the means be given up in the face of large capital expenditures and vested interests backing the status quo? If answers to the above questions support adoption, one moves to a set of questions about polices and resources for managing the tactic.

Written policies: Does an agency have policies to guide use of the tactic, and are these periodically reviewed? Policies will cover who agents and subjects are and their rights and responsibilities; how and when data are to be collected, merged, altered, analyzed, interpreted, evaluated, used, communicated, challenged, protected, updated or purged; and how internal and external oversight will be handled. Do the policies and procedures seek to guarantee integrity, fairness and effectiveness and to guard against mistakes and abuses? Consistent with Rawls’ (1971) perspective, is the system designed so that those weakest and most vulnerable are not uniquely and unfairly disadvantaged relative to others as a result of their unequal status? Yet even with nice words on paper about an acceptable technique, an organization’s ability and will to apply policies should be a necessary condition for adoption.

Agency competence and resources: does the organization have the resources, skills and motivation to appropriately and effectively apply, interpret and use the tactic? Does it engage in critical self-reflection in the use of sensitive techniques? For example, in the case of undercover police practices, which can be very effective, the discussion is not about the worth of the tactic, but whether the risks it brings can be adequately managed given the agency's policies and resources. Similarly, some criticism of TSA (Transportation Security Agency) is not about its technology, but about whether the agency's personnel have adequate training and competence to apply it. Problems regarding training and competence are most likely during perceived crises, when authorities are under strong pressures to do *something*. Yet the potential to competently use a technique is not a sufficient criterion for adopting it, absent consideration of additional properties of the means, such as validity, human reviews and comparisons to alternative tools.

Means

Validity: Validity is in part a socially constructed concept. As the philosopher Kenneth Burke observed, "Everyway of seeing is also a way of not seeing." Awareness of this brings the question, "Say's who?" regarding claims of validity. How, then, are claims of validity defined? What degree of certainty is deemed necessary for strong conclusions and actions based on the results? How are the lines drawn between "acceptable" vs. "unacceptable" levels of proof? Relevant here is the cost of failure, the ease of discovering it and the possibility of amelioration. Relevant also is whether the tactic is valid in both its potential for accurate measurement and a given application because a valid tactic can be applied wrongly or in error, or the tactic can be insufficiently reliable. Also, to what extent do specialists agree about the merits of a tactic?[5] Has adequate attention been given to the various sources of invalidity?

It is reasonable to hope that surveillance results will, in Chandler's (1957) words, reflect the potentially "tangled web of fact" rather than the "austere simplicity of fiction." Privately, however, agents are sometimes indifferent to validity because they believe that additional procedures (such as a confirming drug test) will discover any failings. And they may appreciate a less than perfect means as a scare tactic that deters, or they may believe that those assessed are guilty or undeserving anyway, even if they weren't caught *this time* because they were lucky or too clever. Agents thus may lack motivation to explore a tactic's validity, and they may in turn work in an unprofessional and ritualized fashion. That is particularly likely to be the case when the requirement to surveill results not from the organization itself, but from requirements of an external agency such as government or an insurer.

Human review: Are there means to verify results and periodically check the tool itself? Is there human review of machine-generated results –both basic data and (if present) automated recommendations for action? Machines are fallible, as are the humans who construct them. In many settings, human checking of automated findings and recommendations is vital given the acontextual nature of the data and risks of hardware and software failure. [6] This is particularly important where a decision has significant implications for life chances. Generally, individuals as interpreters of human situations are far more sensitive to nuance than are computers, even if they are more expensive and corruptible.

Alternative means: Is this the best available means? How does it compare to other tools with respect to ease of application, validity, costs, risks and measuring outcomes? Is there a tilt toward counting (in both senses) what can most easily and inexpensively be measured, rather than toward what is more directly linked to the goal but may be more difficult to assess? Goals must of course be considered alongside of means.

Goals

Clarity in goals: Are the goal(s) clearly stated, justified and prioritized (if more than one)? Where secrecy is appropriate and the goals are not publicized, have they been clearly defined within the organization?

Appropriate vs. inappropriate goals: Are the goals of the data collection legitimate and consistent with the information expectations of the setting? Is there a strong rationale for pursuing the surveillance goal within the environment in question?

Relatively non-controversial positive goals such as health and protection are easier to identify than their opposites. The negative, by their very nature, are likely to be hidden under the camouflage of acceptable goals. As one example, consider the agency that advertised its services as helping those with bad credit while their real goal was to create and sell lists of those with credit problems. Still, a data collection tactic acceptable in one context may be unacceptable in another as the goal shifts. Consider the following contrasting cases:

- Drug testing school bus drivers versus junior high school students who wish to play in the school band

- A doctor asking patients about their birth control and abortion history in a clinical setting versus asking this of all female employees (as one large airline did) without indicating why the information was needed

But even when a tactic is right for the setting because the goals have been clearly defined, if results of the surveillance spill over into other settings, controversy is likely. As chapter 3 suggested the frequent looseness and complexity of goals is a challenge to analysis. Controversy is likely when settings such as work and non-work conflict --as the case of the Omniscient Organization illustrates or when home and school conflict as with PISHI. For example, is it appropriate to use a pulmonary lung test to measure whether employees are complying with a company's non-smoking policy? Employees are told that this is a necessary health and cost-saving measure -- good for both the company and the employee. But some employees see this as wrong because it seeks to control their behavior away from the job –behavior they have a legal right to engage in. A company policy that says don’t smoke at work contrasts with one that says don’t smoke period. The same is the case for drug tests that have implications for what is done in a recreational setting.

Goals are most likely to be appropriate when subjects and agents share them, or they at least overlap, when there is a single overriding goal, and when there is no spillover into or from other settings,

Unitary usage: Are data used for the defined purpose, consistent with the subject’s understanding (and, where appropriate, agreement)? Do the data remain with the initial agent/owner, or do they migrate? If the latter is the case, is this because of a failure to maintain confidentiality and security of the data? In the United States to a much greater extent than in Europe, second, third, fourth (and more) users and uses are common and reflect the strong U.S. emphasis on property rights (that is whomever “has” the data can then sell it).[7] Using matching and profiling and data mining. merged databases are intended to provide a mosaic more useful than that from a single data source.

Connections Between Means and Goals

The presence of an acceptable means and a justifiable goal, of course, implies nothing about whether linking these is appropriate—that is, how well the two fit together, whether any action is needed at all, and whether the two are in proportion with each other, the topics discussed in the next section.

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? As noted, how well a test measures what it claims to--drug and alcohol use, miles driven, or location--is different from what it may mean in relation to goals only indirectly linked to the results of the measurement. A measure can be valid in its immediate empirical results without being effective with respect to a goal.[8]

Thus, as we move from the direct results of a measure that is immediately meaningful given the goal (e.g., detecting heat or location data from a sensor) to more removed goals based on probabilistic inferences about future behavior, as with profiles, usefulness of the data often lessens. A profile such as one used to predict airline highjacking (young males buying one-way tickets paid for with cash) involves very accurate data, but a very weak correlation to subsequent incidents.

Urine drug tests, when properly done and backed by a second confirming test, show high validity. Yet we still must ask whether drug test results are associated with the employment performance behaviors they are presumed to predict. In that regard, a test for transportation workers that directly measures reflexes may offer a better fit with the goal than the more inferential drug test.

Inaction as action: Where the only available tool is costly, risky, and/or weakly related to the goal because what is of interest is difficult to detect or statistically very unlikely to occur, has consideration been given to taking no action or to redefining the goal? For example, an argument for not enforcing marijuana laws is the belief that given the demand, the ease of obtaining the drug, and the high costs of limited enforcement, it is better to do nothing (legalization apart).

Proportionality: Do means and ends stand in appropriate balance? Answering this question requires attention to the potential problems and gains from the means and the importance of the goal. A sledge hammer should not be used to crack open a nut, nor a sprinkling can to put out a house fire. Hanging them all will likely get the guilty, while applying unduly stringent restrictions will mean subjects who deserve scrutiny (and worse) may escape.

In a heterogeneous society where claimants have rights and resources invested in pursuing their values and interests, obtaining consensus on either the costs of the means or the importance of the goal can be challenging. There is a danger that as the goal gains in importance, concern with the negative aspects of the means recedes without adequate discussion. Conversely, as noted, as the means become softer and easier to use, attention may be drawn away from continuing negative aspects. Pronounced power imbalances between agents and subjects can be conducive to lack of proportionality.[9]

Data Collection and Analysis

The criteria for the means, goals and their fit considered above are at a rather general level. Some more specific criteria involve the actual collection and analysis of the data with respect to how subjects are chosen, how much data is collected, what borders are crossed, or what harm may occur in collection.

Criteria for subject selection. Are universalistic standards applied? Where there are no grounds for treating persons differently, are all subject to surveillance, or do all have an equal chance of being surveilled, even if few are actually chosen.[10] For example, contrast categorical scrutiny within a group, as with checking names of all flyers against no-fly lists, with selecting a few travelers for an intensive search based on a table of random numbers. When agents have no easily identifiable correlates of what they are looking for, they may use preliminary superficial screening of everyone to identify cases for a more intensive gander.

If a controversial tactic justifiably crosses personal borders on behalf of some presumably greater communal good and there are no grounds for differential application, fairness suggests that all should be subject to surveillance or at least have an equal chance. But in practice, limited resources can work against this equality, and social stratification may favor the exclusion of the more privileged. For example, are executives subject to the same drug testing and communications monitoring as workers?

However, with much of what surveillance seeks, there are empirical reasons for differential treatment –that is, for applying surveillance not to everyone or randomly, but according to some criteria whose predictive power is presumed to have sufficient empirical validation to justify unequal treatment. Rationalized differential treatment is central to modern organizations, but are the reasons for it communicated and justified? When there are legitimate reasons for treating cases differently, it is necessary to ask whether persons in equivalent situations are in fact treated equally and what the evidence is for the equality of the treatment. As cases of ethnic, religious, gender, age or class profiling suggest, this is a major area for controversy. The aura of science may be seen as a cover for unwarranted discrimination.

Technologies differ in the breadth of data they generate. Contrast the selective reporting of an informer with the indiscriminate sweep of a video or audio device on a street corner. But even for the latter, decisions are made about *where* and *when* these devices are available, their range, who can use them, whether they can be turned off, and whether they are even used.

Charges of discrimination are less likely when the subject triggers the surveillance. Consider a subject who knows he will be monitored because he has access to a place or data requiring validation of identity compared with one who sets off an alarm as a result of being in a restricted area compared with an undercover agent who pretends to be drunk while exposing his wallet to see who will take advantage of a temptation).[11] When subjects self-select, a form of consent can even be seen—for example, if they are aware of the potential requirements and consequences of their actions, as in the examples just given. While agents make decisions about providing an opportunity structure for surveillance, the subject's behavior is decisive. The apple is offered, but the choice is Adam's--although factors such as how hungry and competent Adam is and how desirable the apple condition that choice.

Minimization: Have agents made an effort to gather only the amount and kind of personal information necessary for the goal? This cuts across other questions such as alternative means, goals, specificity in subject selection and data collection, and the related ability to control spill over. Other factors being equal, only personal information directly related to the goal should be collected. Tangential personal information that is private--as in not known by the agent as well as intimate or sensitive--should not be gathered. Nor, per the discussion in chapter 4, should data be collected and communicated in more forms (whether aural, visual, text, olfactory, or tactile) than is necessary.

A principle of minimization is seen in standards for wiretapping and in requirements that limit search warrants. In contrast, many private-sector data gatherers face no such limits. Communications monitoring in many workplaces can be applied in a categorical way such that all communication (phone, computer, even office conversations) are potentially monitored via sound, image, location and more. Note also the extraneous data collection involving questions about lifestyle and social circumstances that accompany many warranty forms and the requests for names and phone numbers from retail stores even with cash purchasers.

Agents can face contradictory pulls here. On the one hand they can have strong incentives and temptations (whether formal, as related to goals of an organization, or personal, as related to goals of the agent) to collect data beyond what is required for the immediate task. As a posterior-covering insurance policy, data collectors often favor gathering more information rather than less (see Slane Figure 1 p. 272 in *Windows*)). Not knowing exactly who or what they are looking for, combined with the possibility that information might be useful in the future, that new uses will be found. or that charges of discrimination could arise regarding the kind of data collected, agents tilt to fullness in what they collected and who they target.[12] However, agents also face needs for efficiency in discovery and the desire to avoid drowning in data and being accused of using dragnet tactics.

The issue of minimization involves not only the kind of information collected, but the kind of subsequent analysis performed on it and whether it is combined with other data to create new forms. Consider biological samples taken for employment or health purposes analyzed for other goals for which consent was not given, or combining distinct, compartmentalized forms of data to create a whole that is qualitatively different from its components considered separately.

A related aspect of minimization is whether the collected data are directly linked to a locatable, uniquely identified person or whether they are fully anonymized. For many transactions, a merchant or organization only needs proof that the potential subject is in a category entitled to, or eligible for, goods or services. This need not involve knowing additional information. For example, to grant someone access to toll roads or communication devices, an organization need only certify that the user has paid the fee, not his or her identity.

Keeping personal data from different contexts structurally disaggregated is another aspect of minimization. This is furthered using distinct identification numbers or symbols (rather than the same number for everything, such as social security or phone number). For many purposes, new numbers or symbols can be used for each transaction, or at least distinct means of identification can be used across organizations.[13]

Minimization also involves a tactic’s degree of invasiveness. Most persons would agree that a less invasive tactic or application is preferable to greater invasiveness. Agreeing on what invasiveness means is more difficult.

The term can be used literally, as when one crosses a physical border into the body or private space of another or more figuratively, as when one takes something from or imposes on another person. Entries into the natural physical borders of the person--as with breaking the skin to extract a bullet or take a blood sample for a drug test--contrast with the more (in one sense) voluntary action of providing a urine drug sample and the even less invasive drug test based on analysis of hair (although in both cases, an “invasion” of the body can be seen to occur). Is a search by computer of many innocent records looking for the smoking gun less invasive than a comparable search by a human? Is degree of invasiveness defined by the nature of what is discovered as discussed in chapter 4 (information on being left or right handed vs. more intimate or sensitive items such as religious and political beliefs).

The above factors regarding invasiveness are empirical and in a sense objective as seen by the outside observer. But invasiveness can also be defined with respect to perception and feelings, beyond anything observable in a behavioral sense, a distinction Tom I. Voire in chapter 12 selectively chooses not to understand. Consider the meaning of being involuntarily watched for an exhibitionist, as against a person of reticent disposition, or the voyeur's interest in watching, as against the recluse's interest in avoiding attention from others. A factor in thinking about invasiveness is what the subject feels, believes, and agrees to as well as what the agent intends.

Border crossings: Does the technique cross a potentially perilous personal boundary without notice or permission (whether involving coercion or deception or a bodily, relational, spatial or symbolic border)? If consent is given, is it genuine?

Violation of assumptions: Does the technique violate assumptions that subjects make about the conditions under which their personal information will be collected? Such assumptions can involve standard, often tacit, cultural expectations, such as that persons are who they claim to be, that conversations will not be secretly reported, that confidences will be respected, or that there will be no secret government blacklists. Violations can also involve failing to honor explicit policies or promises, such as that data will be destroyed.[14]

Harm in collection: Does the act of data collection involve physical or psychological harm to the subject? Some interrogation tactics (as against passive data collection) for example are based on the creation of fear and threats to inflict harm as a bargaining tool. Torture is the obvious example. But an interrogation need not involve the threat of violence to be stressful or ethically questionable.

Interviews, psychological tests, drug tests and searches can be done to minimize or maximize discomfort. Being questioned about sensitive subjects and having personal data gathered may necessarily involve some feelings of embarrassment, shame, discomfort, powerlessness and recalling or re-experiencing of painful memories. The agent’s manner and the conditions of data collection, however, can minimize or exacerbate these. For example, as exacerbation, the agent may go farther than is required or than has been publicly announced (and perhaps agreed to by the subject).

Consider intentionally inflicting pain in drawing blood (e.g., in the mandatory AIDS tests required of those in prison and the military) or adding stress in the application of the polygraph (e.g., by making the cuff tighter than necessary). A sexual mismatch in a strip or pat down search is an obvious case, although perhaps on the average, that would be more unsettling for women than for men. But even with same-gender monitoring, subjects may experience discomfort and feel violated (e.g., by video cameras in bathrooms and changing areas).[15]

Other forms of harm may result from the way data are used, and surveillance results may disadvantage subjects and/or others in multiple ways, the subject I turn to next.

Consequences for Subjects and Others

A key question regarding consequences is whether the results of the surveillance are used to cause unwarranted disadvantage or harm to the subject, the agent, or third parties. There is of course much room for debate over this question and whether disadvantage should be defined in objective or subjective terms and whether the intentions of the agent should be considered apart from measurable consequences.

By way of informing this debate, I present some of the ways that subjects may be disadvantaged:

Surveillance used to gain unfair strategic advantage in discovering information that a subject wishes to withhold because of a legitimate conflict of interest. Consider a bugged car sales waiting room that permits the seller to learn a customer's concerns and maximum payment; corporate espionage; or a college admissions officer who looks at other schools' admittance web pages to gain advantage in recruiting students.

Surveillance used to gain manipulative advantage in persuading or influencing a subject, whether involving consumption or politics. At the extreme are blackmail and intimidation. But consider a more benign form, in which a candy company mails a special discount offer to a list it had purchased of diet workshop participants. Merging various kinds of information and databases permits detailed profiles and very specific narrow-casted messages in which the agent may know a great deal about the subject, while the subject knows very little about the agent. To the extent that there is a significant imbalance in what parties know about each other in settings where goals are not fully shared, claims of unfairness are more likely.[16]

Surveillance used to restrict social participation or otherwise unfairly treat persons based on information that is invalid, irrelevant, acontextual or discriminatory. Many examples can be found in health insurance, banking, housing, employment and even in opportunities for consumption.[17]

Surveillance that damages a subject's reputation as a result of unwarranted publication or release of personal information. The concern here is with the subjective harm to the individual's self-image and perhaps with feelings of embarrassment, shame or humiliation as the individual imagines how others will view him or her as a result of the release of confidential, or not widely known, information. The harm is compounded when the information is invalid and the person is wrongly put in an unfavorable light.[18] State laws that protect against privacy invasion, false light and defamation attempt to remedy this.

S*urveillance that betrays confidences and violates trust* because of procedural violations and exaggerated claims (i.e., efforts to create the myth of surveillance) even if the information is neutral or positive for the subject. Learning that an organization is engaged in secret data collection or that it has failed to maintain confidentiality and security, or to use information only as promised can cause paranoia and chill inquiry, political expression and organization. Trust is a central element in spontaneity, sociability and communality. Its absence makes cooperative group action difficult. A belief that one is continually monitored can inhibit innovation and experimentation and eliminate risk taking. It can engender the creepy feeling of invasion by distant, unknown observers.

Surveillance(both its collection and its use) that involves unwanted intrusions into solitude, as individuals lose the ability to control the access others have to them. The act of data collection may perturb the individual’s sense of personal space and expectation of being left alone. Even imposing on a person’s attention (a scarce energy and temporal resource) can be seen as a violation.[19]

The indiscriminate use of discriminate results may prompt targeted marketing and uninvited use of the subject’s communication resources (fax, phone, computer) and time. The architecture of the Internet, data harvesting, and improved analytic techniques have resulted in an avalanche of communication intrusions directed toward clients, customers, donors or voters via telephone, internet banners, spam emails and regular mail.

Automatic solicitations may additionally bring reminders of things best forgotten. Consider the harm from a pseudo-personalized mass mailing that begins by congratulating persons assumed to be parents on their child's first birthday and a continuing annual card each year. The advertising goal is to sell parents things a one year old needs, and the company purchased the data from health care providers. How does a couple who had a miscarriage that is not reflected in the database feel when they receive such solicitations? Such insensitive mailings (an actual case) can cause a particular kind of harm.[20] Or consider a mass mailing to recently retired persons advising them of the advantages of cremation over burial. Certainly these are not issues to run to the barricades over, and they are modest on a scale of unethicality, but they are a bother and at some point, they can overwhelm resources and emotions. *Surveillance that profits the agent but not the subject whose data are being marketed* Is the additional benefit or profit a company or a data warehouse gains from selling an individual’s personal information shared with the subject? Has the individual given permission for the reuse and sale of the data? For example, some magazines offer readers an extra month's subscription if they agree to have their information sold.

To sell another person's information without asking or letting the supplier share in the gain can be seen as a kind of theft in which a property right is violated. The subject's "work" in one sense has produced the data. If one can copyright a short story, why not copyright the story of one's life, or at least name and records of behavior?[21] These questions involve the gray area of intellectual property, which has become much grayer as a result of computerization.

The concept of harm or disadvantage, whether in the collection or use of data, is often debatable: should harm be measured objectively or subjectively, and how should individual and cultural differences in defining it be viewed? What criteria differentiate legitimate from illegitimate forms? These questions warrant caution and reflection. However, it is a moral cop-out to use cultural relativism to argue that the definition of harm must never transcend varying group and individual definitions. Even with a definition of harm that varies considerably across individuals and groups universal standards may still be identified.

Moreover, in drawing ethical conclusions, we need to distinguish between harm only to an individual's interest, such as denying a loan or benefit request (whether justified or not), and that with broader social consequences, such as denying a loan or benefit request because of the subject's race or religion. The concern there is with socially reverbative harm. What wrongly harms the individual may also bring more diffuse harm to a community, as well as to particular subgroups, as with those singled out by a perhaps statistically accurate profile that may not hold in any individual case.

The issue of harm to a group rather than to an individual has received scant attention. Consider damage via stigmatization and discrimination if a group is labeled as having a disproportionate statistical tendency toward some undesirable outcome.[22] Consider the case of aggregate data on distinct groups indicating lower average IQ scores, higher arrest rates, or higher than average rates (or potential as predicted by DNA analysis) for a disease.[23] Harm at the group level may also be seen in the damage to community and politics that occurs when trust is violated via deceptive or invalid surveillance. As Regan (1995) observes, privacy has a social as well as an individual component.

Rights and Resources of Subjects

Right of inspection: Are subjects aware of the findings and how they were created? Fundamental aspects of procedural justice involve the right to know and to challenge the evidence in the face of the kind of bureaucratic illuminosity described by Franz Kafka and experienced under authoritarian and totalitarian governments.[24] In the case of government, the right to have access to one's file is related to a broader principle that, absent special conditions, a democratic society should not maintain secret personal databases.

Right to challenge and express a grievance: are there procedures for challenging the results and for entering alternative data or interpretations into the record?

Redress and sanctions: if the individual has been wronged, are there means of discovery and redress and, if appropriate, for the correction or destruction of the record?[25] Are there means for minimizing or preventing problems that require redress and sanctions? Are there audits and sanctions to encourage responsible surveillance and fair and just outcomes?

Unlike in Europe and Canada, where official Data Commissioners may actively seek out compliance, in the United States it is generally 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.[26] Internal agents such as inspector generals, auditors and public interest watch dog groups are other means of identifying problems. Recently, some organizations have created the position of privacy officer. How independent and effective they can be given their host is a challenging organizational question.

Equal access to surveillance tools: In settings of reciprocal (or potentially reciprocal) surveillance, are the means widely available, or are they disproportionately available (or restricted) to the more privileged, powerful or technologically sophisticated? Contrast the ability to use satellite imagery with the cell-phone camera. Must doctors reveal personal information (e.g., investigations by professional boards) to patients, just as patients may have to agree to a search of a database to see if they have ever sued a doctor? Such cases contrast with a doctor asking a patient about drug use or sexual behavior in a clinical setting with the expectation that in this context the patient will not ask equivalent questions of the doctor.

Equal access to neutralization tools: In settings where neutralization is legitimate (whether because the rules permit it or because unwarranted agent behavior may be seen to justify it), are the means widely available or limited to the most privileged, powerful or technologically sophisticated? Some means of maintaining control over personal information such as providing a false name and address when the request is irrelevant (as when paying with cash at a store) or free anonymous E-mail forwarding services are available to anyone. In other cases, protecting information may require technical skills or come with a price, as with the purchase of a shredder, an unlisted phone number, or a subscription or membership that (after initial vetting) grants a higher level of privacy (as with various Trusted Traveler Progams)..

However, in some contexts, the use of a tool may be prohibited (even if it can be legally purchased) and/or its use restricted to government. The ethical question is, are the restrictions (or their absence) justified? Just who should have access to such tools is frequently contentious and subject to negotiation. Consider whether citizens are entitled to use cell phones or other video means to record police behavior. There are also interesting cross-border issues here, as when tools that are prohibited in one country are available in another –whether weapons or eavesdropping equipment.

Consequences for Agents and Third Parties

Harm to agents: Does the tactic have undesirable impacts on the values and personality of the surveillance agent? Can the risks be reduced or mediated? Consider super electronic sleuth Harry Caul in the film *The Conversation*. Over the course of his professional career Caul becomes paranoid, devoid of personal identity, and desensitized to the ethical aspects of his work. Undercover police agents face a variety of risks--from attack to crime temptations to psychic and family costs. There have been claims that police who use radar guns in traffic enforcement might have higher rates of testicular cancer (Police 1992). The policy implications differ depending on whether the potential for harm lies in a poor fit between the characteristics of the agent and the means or in the nature of the work, regardless of who plays the role.

Spillover to uninvolved third parties: Can the tactic be restricted just to subjects? Can undesirable affects on others be avoided? How focused and contained is the tactic? Audio and video taping may record the behavior of subjects as well as that of their family and friends, and DNA may offer information on family members whose DNA was not collected.

Data Protection and Fate

An important aspect of decent data is relevance and timeliness, including policies for reviewing the system of data collection and determining what to do with the data over time. Records that are dated and that fail to take account of changes are a common problem.

Periodic review: Is the system regularly reviewed for effectiveness, efficiency, fairness and operation according to policies (or the need for new or revised policies)? Are there audit trails and inspections?

Data fate: are there rules regarding the retention or destruction of the data, and are these honored?

Questions about Questions

As suggested, the more the principles implied in these questions are honored, the more ethical the situation is likely to be, other factors being equal --which of course they rarely are, given, among many other concerns, the importance of prioritizing and weighing values. The questions thus require several kinds of evaluation.

First, do the procedures and policies cover the basic areas? Once we have this answer, we can move to questions about substance: Are they good policies? Are the policies followed in practice? Does the organization (or others) regularly check on itself through audits and inspections? Is the subject likely to be aware when a policy fails?

Inquiring as to whether the policies are followed can be looked at across all, or a sample, of cases as well as in any given case. For example, the validity and consequences of a specific type of drug testing as a class can be considered. But questions can also be asked about the application of a particular form such as a urine drug test to a given individual or at a specific location. The point is that a means that meets general standards for validity can still be incompetently or erroneously applied. Distinctions are also needed between rejecting, limiting or revising a tactic—say, the polygraph--because of questions about its efficacy, as against rejecting a particular flawed application of a tactic.

When failings are identified, the next question is whether they are idiosyncratic and seemingly random or systemic (as was the case when congress limited use of the polygraph). Is it the apple or the barrel? How often do individual problems have to appear before agents conclude that the problem is in the system rather than an unfortunate, but tolerable, occurrence? If it is the former, can it be mediated in the given case?

Context and Comportment

> Systematic reasoning informed by practical wisdom and artful judgment that guides us away from missteps, suggests heuristics and rules-of-thumb, and clarifies what is at stake in these dilemmas may point the way to better if not certain judgments."
>
> Helen Nissenbaum, Privacy in Context

The analysis thus far has hopefully demonstrated a central point of the book: *surveillance is neither good nor bad but context and comportment make it so* (at least most of the time). The variation in tactics and contexts presented here illustrates the importance of making distinctions and identifying assumptions –whether for purposes of social science or judgment.[27] As the examples and argument throughout the book suggest, a situational approach to analysis and ethics is needed. This broader approach stresses the need to look at the setting, to go beyond (but make room for) important variables such as the tool in question or the type of data, and to consider structural conditions such as reciprocity and whether state or non-state actors are involved, or whether an over-arching first principle such as privacy or publicity is at stake.[28] These factors need to be seen within a specified context, rather than in isolation from it.

The irony and much of the sense that something is off in the stories of the Omniscient Organization, Pishi, Tom Voire and Rocky Bottoms are related to a mismatch between surveillance behavior and what seems right for the milieu in question (work vs. home, personal vs. impersonal relations, the state vs. civil society). A key factor in this mismatch is the interplay of various personal and institutional borders as seen in the fit between technologies, rules, expectations, setting and behavior. The surveillance occasion (ch. 5) viewed as a dynamic process over time needs to be broken into its sequential strips and interrogated by the questions in Table 1.

In seeking to understand and evaluate the privacy-related problems raised by new information technologies, Helen Nissenbaum (2010) creatively develops ideas of contextual integrity. She calls for detailed analysis of how a change—say, for example, the increasing ease of communicating information or aggregating it in combined databases--affects the goals sought and traditional expectations regarding factors such as who the information is about, what kind of information it is, and what the principles are for its transmission.

As the many examples considered thus far suggest, building up from the facts on the ground to reach conclusions is central to understanding and judging surveillance. The emphasis on context with its direct acknowledgement of the variation in settings of personal information is a key to a more comprehensive understanding. A perspective such as Nissenbaum's is necessary for analyzing the roots of the many concerns over the new technologies. My approach is even more general in seeking ways to judge all surveillance –whether traditional or new and whether or not it comes to be defined as problematic.[29] Privacy is only one of the major issues raised by surveillance and can be subsumed within it.[30]

In treating established information norms as the standard against which any new means should be compared, Nissenbaum does not necessarily favor the status quo. She notes that sometimes new information-gathering means will better meet the dominant goal(s) of a given context such as health care or voting than did traditional means. My initial concern however goes beyond comparing new and old to suggesting ways to judge the desirability of traditional means, apart from any change brought by emerging means, and to identifying the correlates of disagreements (or structural roots as they say).

In studying undercover police practices I stressed the importance of rules and of less formal expectations in specific contexts as against the intrinsic elements of a tool or universal principle in reaching conclusions. This also holds for other forms of surveillance. As noted, a given means can be used for different goals (contrast a location-monitoring device carried by a skier for protection in an avalanche with the surreptitious application of such a device to a rival's car.) A given goal, such as the prevention of drug use, can be sought and evaluated with respect to a variety of means from mandatory to voluntary testing of various kinds, to informers, stings, dog searches, education, supply restriction and methadone (or Antabuse for alcohol) and various treatments. [31]

Simply having a technique that is morally acceptable is obviously not a sufficient condition for its use anymore than a good goal is justification for using a morally challenged or unduly risky or costly means. But even with appropriate means and ends, ethical concerns can also arise at other stages noted in chapter 5, such as collection, analysis, data protection and data fate.[32]

The ethical status of a technique can vary from cases in which the means, goals, conditions of use and consequences are wrong or even abhorrent, to those in which they are all acceptable or even desirable, to varying combinations. A more precise and richer analysis is possible when judgments are related to the distinctions the book suggests.

To be sure, some means of personal information collection strike most observers as wrong or at least troubling, apart from how and why they are done, and whether or not they appear to be valid and effective. Torture is the obvious case. Harming or threatening innocent friends or relatives of a subject is another. Similarly, most persons recoil (and the courts tend to prohibit) information collection involving 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.

Other surveillance means such as lying, deception and manipulation (as in undercover work), while not automatically beyond consideration, are hardly initially preferred. As Sissela Bok (1978) argues with respect to lies, they should be used only under limited circumstances and when a convincing case for them has been made. Such means always present a moral dilemma. No matter how compelling the justification for use in a specific setting, in our culture neither lying and trickery, nor physical force and coercion, are morally preferred techniques.

initially preferred, though not automatically beyond consideration. As Sissela Bok (1978

Yet viewed against the astounding number of surveillance events occurring daily, publicly acknowledged use of tactics that are abhorrent or of last resort are uncommon.[33]

The law, concern with public relations and reciprocity, the values of the agent, and the move toward soft means of data gathering can block or temper the harsher applications. While some data collection means are inherently undesirable and even prohibited, categorical prohibition of a means is rarely an issue. Most contemporary disputes over domestic practices do not involve the means as such; rather, they are more likely to be found in a disjuncture between the context and the means and/or the goal, or to involve concern over faulty or absent rules or the failure to follow appropriate standards for collection, analysis and data protection and use.

Values

Context and the specifics of a situation apart, the questions presented in this chapter imply some broader principles or values that can be sources of conflict. The unifying function of values lies in their level of abstraction and vagueness of meaning. But given the lack of clarity in definition, there is much room for disagreement. What does the value mean? When values conflict, how should they be prioritized? When does a value apply?

Even when the meaning of values is not disputed, conflicts between values are often present—for example, liberty and order or publicity and privacy; rights and obligations of the individual over the community; universalism and particularism; individual rights and efficiency, effectiveness, rationalization; free markets and regulation; freedom of religion and gender equality; freedom of expression and honesty.

When values conflict, rather than rejecting them outright, people often disagree over how they should be weighed. Since 9/11 supporters and opponents of the Patriot Act and enhanced surveillance argue endlessly about the relative importance of security and privacy.

When the meaning or prioritization of a value is not in dispute, people may disagree over when it applies. Disagreements about transitions between the borders of social positions are an example. Consider parents and teenage children --with parents justifying surveillance because they see adolescentsas irresponsible, or at least in need of guidance, while the latter argue that they have become responsible (whether of legal age or not). The conflict here is about whether the teenager is an appropriate subject of surveillance.

A related disagreement is about what value should apply to an object. There is little debate about the reasons for protecting information contained within the first-class letter, nor about the accessibility of information offered by a post card. But when a new means of communication, such as email, appears should it be treated like a first class letter or like a postcard?

Complexity Yes, Abstention No

On the best of all possible planets for the philosopher, an ethical theory needs to be grounded in a formal normative argument that offers justifications for its 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).

Like a kaleidoscope with a unifying light source, an integrated ethical theory should illuminate and link the varied shapes of surveillance.[34] It would be nice if the world had been created such that a simple deductive Rosetta stone for judging surveillance was possible. But given the world in which we live, such an effort would need to be so general and banal as to be of modest interest or use ("do good, avoid harm").

The alternative offered here –an inductive approach that asks about the ethics of heterogeneous settings and behavior also has limitations. A comprehensive consideration of the myriad factors that can go wrong or right with surveillance may overwhelm the observer. Casting such a wide, yet thinly meshed, net brings the risk of being unwieldy and unrealistic, let alone unread –even by those with time to reflect and the will to read more than an executive summary who do not have to take immediate action.[35]

This can easily lead to the search for quick solutions that ignore complexity and the potential fallacies of quantification--falling back on automatic bureaucratic decision making based on ethics by the numbers (e.g., simply counting up the "yes" and "no" answers to the questions in table 1 and declaring that the majority wins). Equally troubling is to ignore moral conflicts and the dangers that come of failing to acknowledge the "dirty harry problem."[36]

I have sought an intermediate position --casting a net broad enough to capture the major variations and filtering these through some basic values. This chapter's emphasis on surveillance agents reflects concern over the abuses associated with the tilted nature of private-sector, organizational, and authority playing fields and unequal access to surveillance resources. At the same time, I try to 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.

We all play multiple roles and rotate between being agents and subjects. Organizations and those in positions of authority are prone to emphasize their rights to gather and use personal information over their duties or the rights of subjects. In turn, subjects generally show greater interest in protecting their own information than in the informational rights of others and are relatively unaware, or uninterested, in the information of organizations.

Under appropriate conditions agents have a right and even an obligation to surveil, but they also have a duty to do it responsibly and accountably. Reciprocally, those subject to legitimate surveillance have obligations as well (e.g., not to distort the findings or threaten agents), even as they also have rights not to be subjected to some forms of surveillance.

The multi-dimensional nature of personal information, the extensive contextual and situational variation related to this, the value conflicts, and the dynamic nature of contested social situations prevent reaching any simple conclusions about how crossing informational borders will (empirically) and should (morally) be evaluated. Such complexity serves well when it introduces humility and qualification, but not when it immobilizes. Real analysts see the contingent as a challenge to offer contingent statements rather than throwing up their arms in despair. The point is that in spite of all the factors (whether contextual or inherent in values) that work against broad generalizations about the ethics of surveillance, some moral threads that swirl within and between the questions can be noted.

Some values are desirable as ends in themselves—for example, honesty, fairness. But values may also be a means to some other ends --for example, democracy as a support for legitimacy, privacy as a support for intimacy or political organization, transparency as a support for accountability. Asking why (and when) a value is important as an end itself as against as a means to other valued ends and offering standards for prioritizing values is central to the ethics of surveillance. In democratic societies operating under the rule of law, a cluster of value justifications underlie the questions in Table 1. The most overarching and important are the Kantian idea of respect for the dignity of the person and respect for the social and procedural conditions that foster a civil society.

At the beginning of the book I noted that its central questions involved empirical description, conceptual elaboration, cultural analysis, and finally, ethics and policy. This chapter, which treated the latter, concludes the effort. The final chapter briefly returns to these themes and also explores some broader questions, such as where is our society headed with respect to dystopian and utopian claims? How should we think about the verdant trends, counter-trends, ironies, conflicting goals and emerging questions the topic brings? What are the major unresolved and emerging issues in the social study and regulation of surveillance? I conclude with some directives to guide future researchers.

[1] Note Governor George Wallace's call in the 1960s to "let the police run this country for a year or two" to stop the disorder. (Kazin, 1998) On states of exception more broadly see Agamben (2005).

[2] Other strands of a broader equality question: "are the tools equally available to all in situations where reciprocity is appropriate?" and "is the tool applied equally to all subjects?"

[3] Consider the 2012 controversy over Google's streetview which ostensibly was taking only images but was revealed to be garnering wireless data. Reuters, April 15, 2012)

[4] Surveillance agents may begin with the most easily justified and innocuous uses, anticipating that familiarity and routine use will later make it easier for broader uses. That contrasts with more radical uses introduced swiftly during times of crisis.

[5] For federal criminal justice the Federal Rules of Evidence determine this for what is admissible of evidence.

[6] 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)

[7] Unsurprisingly, the property rights justification does not usually extend to the subjects having a say in how data are used, nor in their profiting from subsequent uses.

[8] Valid that is in what it measures. It can also be effective but not valid as a result of the causal mechanisms claimed. Note the polygraph that "works" when individuals confess in the belief that the machine can tell if they are lying.

[9] Beyond the unjustified harm surveillance may cause to the individual, consider the reverse:-the abuse associated with the misuse of surveillance data that helps an undeserving individual. For example several decades ago I encountered a case in which a police chief in a small town erased his son's record of drunk driving from the computer, --with appropriate software and audit trails that would be harder to do today. Such actions are much less likely to come to public attention and seem to have less moral bite (e.g., compare unfairly helping someone with unfairly hurting them). This rarely questioned sentiment underlies the belief that it is better to let the guilty go free than to imprison the innocent. 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 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. This also involves issues of challenge and public awareness. Those who are wrongly harmed are more likely to bring the fact to public attention than are those who are wrongly helped. Another neglected category of harm is that from the *failure* to surveil.

[10] **The consistency principle here which asks whether the tactic is applied to everyone is different from asking what if everyone applied it.**

[11] **Agents still have a role in deciding whether to have surveillance present, e.g., where to put the pretend drunk or how tempting to make the offer, not to mention discretion regarding what is presented to the prosecution.**

[12] **The case of preserving race horse urine is a nice example. Consider also the initial claim that saved DNA collected for identification purposes had no other use. Subsequent developments proved that wrong.**

[13] **Questions must also be asked about whether anonymization is in fact possible and guaranteed.**

[14] **This is particularly likely to be an issue for political data bases. Note the LAPD and other cases where records were to be destroyed and they weren't. The failure to create documents --e.g., not having audio-visual equipment on, or failing to record and save when the rules require that be done, presents an opposite problem.**

[15] Alderman and Kennedy (1995) report a particularly egregious Chicago prison search.

[16] Businesses generally know far more about consumers as individuals and as members of statistical categories than consumers do about the personnel, products or policies of companies. The same imbalance holds for advocacy and non-profit groups that engage in public fund raising and communication, whether universities or political parties.

There can be advantages for both agents and subjects to more focused solicitations and agents have rights to communicate. The issue as with many controversial cases is not whether data collectors and users have a legal right to such actions (in general in the U.S. they do), but rather is it the right thing to do?

[17] For example Oscar Gandy (1993) has noted how market research on consumption behavior can work to the disadvantage of the least privileged.

[18] There may be a procedural violation in the initial collection or in the wrongful release of the information. These two kinds of harm are further compounded when the information is wrong. The embarrassment to the falsely accused, labeled or identified is a rarely considered form. A mild form is in the momentary (and widely experienced) inconvenience caused as a result of a search that leads to an invalid conclusion such as having an alarm go off by mistake as one walks through a detection device in a store or library) or the rejection of a valid credit card. In contrast, less sympathy is likely for revelations regarding those shown to be guilty

and/or worthy of being embarrassed or worse, even if the means of discovering or releasing the information is wrong.

[19] Derber (2000) treats the rarely studied issue of demand on another's attention as a stratification issue. This overlaps norms regarding information seeking, protection and revelation.

[20] The ironic inauthenticity here relates to categorizations that are correct in the aggregate but need not be in individual cases. As the case of Allison Portchnik from the film *Annie Hall* mentioned in ch. 4 indicates, this is a perennial issue in any kind of profiling or generalizing.

[21] Advocates claim they have a right to consume, add value to, repackage and sell data they can access. For example, they argue that if a person engages in a business transaction with a company, offers their image in a public place, puts trash out on the street, and leaves fingerprints or DNA on a glass or a discarded cigarette, they have chosen to give up control over their information. As Rocky Bottoms might have said, "if you are in the data stream you better paddle with the current."

[22] This may also unfairly advantage members of the favored statistical group, who while sharing aggregate attributes of the category, may in fact not behave as predicted by the model.

[23] Profiling is a clear example. In the case of disproportionate stops of minorities and the young … (Toch 2012)

[24] Among the more harrowing of U.S. examples is the experience of …Pim? His case differs in degree from Figes' (2006) extensive documentation of Soviet practices. But the potential for abuse is the same for secret (whether their existence or content) government data bases which are beyond review by independent sources (even if within government) and in which there is no due process or challenge possible for subjects. A principle from the 1973 HEW Code of Fair Information Practices involves no secret government data bases and a citizen's right to see and amend (or at least offer a comment on) personal data held by government.

[25] What mediation is possible once the informational paint has spilled over the global floor?

[26] This is the discovery of dirty data issue. Among common means of discovery are accidents, tests, informers, deduction and coercion. Marx (1984)

[27] Conceptual differentiation is a central aim of the book, even as there are cognitive and pragmatic, if not natural science, limitations on how many angels can find room at the inn or on the pin. Natural science limits however may apply in locating the angels.

[28] 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 in the face of evidence that it does not work as well as other means or has other unwanted consequences.

[29] This of course makes room for contrasts as in Ch. 2 between traditional and the new surveillance and between practices that the analyst as outside observer using the framework the book develops would see as problematic but which are not seen that way by the public, as well as the reverse. This is the classic issue of whose point of view is being expressed –the person in the situation or the removed outside observer.

[30] Refer to S and S discussion re Bennett if not done in ch. 1

[31] Disagreements about surveillance may occur because actors are referring to different components of the surveillance occasion and talking past each other. Untangling these may bring greater clarity to the discussion.

[32] These may overlap as when a system of retinal eye pattern identification instantly results in access or its denial). But they are always analytically (and usually) temporally distinct.

[33] Infrequency is hardly a justification, but it is a factor in considering what is likely to receive policy attention.

[34] Thus it would need to take account of the behavior of individuals, organizations, states and the international order as these involve crossing borders to impose upon, and to take from subjects; the rights and obligations of various parties; the ethical

meanings of doing good and avoiding harm; and various levels of analysis such as kinds of institutions and roles, the cross-cultural and the short and long run.

[35] **There is an eternal tension between the compulsion to get it all down and the realization that if a conceptual space involves more than 3 variables most persons won't bother to absorb an argument (if then). Furthermore, the failure to go the Kantian imperial, deontological route and offer over arching first principles puts one at the risk of being captured by those with the most powerful megaphones and the most passion. To argue on a case by case basis also risks being accused of *ad hoc*, inconsistent and partial responses. As the case of Tom Voire suggests, clever advocates, whether lawyers or not, can usually find a way to justify behavior that seems outrageous to others.**

[36] **This is wisely discussed by Klockars (1980). Failure lies in not acknowledging and analyzing a moral dilemma in which there is gain and loss no matter what path is chosen.**