Note: This is the full, unedited version of Gary T. Marx, *Windows Into the Soul* which became Chapter 12 of the book after cuts

Chapter 12 Techno-Fallacies of the Information Age

There is no doubt that we must conduct more detailed research into the connection between the practices of security professionals and the systems of justifications of their activities, as we ponder on how procedures of truth claims are formulated…

—D. Bigo 2006

This chapter is concerned with public policy, but not with specific laws, regulations, or guidelines. Rather it seeks to identify the broad justifications and assumptions underlying surveillance policies and practices. With the jokes, advertisements, visual representations and music considered in previous chapters, the political message is often oblique, requiring some interpretive work on the part of the consumer. The artistic quality may even increase, as does the subtlety or ambiguity of the message. But with spoken or written words offered by interest groups in the four satirical chapters, the message on the average is more direct and explicit in its adversarial intentions even as there can be unstated hidden agendas

Among the nations of the world, the United States most clearly reflects the optimistic, techno-surveillance worldview found within a broader technocratic and commercial celebratory ethos. And the satires all reflect a strong version of this view, as it is offered to the public by those broadly within "the surveillance community."[1] But the

ideational environment in which these technologies are nourished and in which they flourish needs to be better understood through examining this community's rationales for action and their empirical and value assumptions.

Sometimes these rationales and assumptions form a relatively coherent and self-conscious ideology, or at least a perspective, as with governments, political parties and interest groups such as the American Manufacturing Association, the International Association of Chiefs of Police, and the National Association of Security Companies. More often, however, the beliefs are dangling *ad hoc* snippets drawn on to justify an interest group's claims and actions.

As noted, the arguments in the narratives illustrating the basic surveillance contexts are paraphrases or direct quotes from specialists seeking to justify their behavior and convince wider audiences. Their surveillance worldviews do not represent ideology as a totalizing, monolithic, closed system, as the term initially meant. Rather they are loosely constructed worldviews or narratives created and communicated by knowledge and communication specialists.

This conception of the world and form of consciousness involve problem definitions, explanations, justifications and directions for action. And they share with more comprehensive, coherent and logically consistent ideologies a limited number of basic (and often transparent) assumptions about the social world, certainty about its truths, an intermingling of values and facts, and an action program related to these.

The kinds of views characterizing the four narratives illustrating basic surveillance contexts show elements of belief systems that Karl Mannheim (1955) identified as both ideology and utopia. For example, the bottom, I mean Bottoms doctrine

certainly is intended to serve the interests (however varied) of the more powerful and, as such, is one variant of a traditional ideology. Yet his narrative [?} also offer a utopian perspective—that is, the love affair with futuristic technology promises to be transformative, fundamentally altering the meaning of the human and the social. As always, reality is much richer than our efforts to corral it, but with Sisyphus and Oscar Hammerstein, you gotta' have a dream.

For Mannheim the beliefs of emotionally hooked activists are tied to their social location and interests and hence relative, partial and potentially disingenuous and distorted. In contrast Mannheim suggested that the free floating intellectual, divorced from traditional interest-group social pressures, who independently analyzed belief systems, could get closer to the truth than the autonomic believer. In contrast,such an analyst listening to all views and straining them through the lens of scholarly inquiry, could see the big picture beyond the fog of self-sereving ideological stances. nlice work if you can get it. My analysis of surveillance worldviews that follows seeks to be in that tradition, if more humbly and with awareness of the paradoxical nature of claiming that the outsider really could be fully outside.[2]

The analyst of ideology has traditionally had two tasks (Seliger 1976, Thompson 1990). The first is to report the central ideas of a worldview (weltanschauung), as was done in the preceeding units on artistic expressions and in the narratives. The next task is to analyze them. This chapter offers a logical, empirical and ethical critique of the worldviews in the satires.

The emphasis here is on showing how some aspects of this worldview are empirically wrong, logically inconsistent and morally questionable, but the analysis does not cover all possible fallacies.[3] While the previous narrative may give new meaning to the term “Rocky Horror Picture [?] Show,” the critique that follows is not a total rejection. The worldviews in the narratives intermingle compelling values and social analysis with the dubious and even the outrageous.

Thus, I make no claim that the worldviews discussed here necessarily stand apart from other ideological systems, which also contain inconsistencies, self-serving claims disguised as high principle, deceptive facades, misleading statements, empirical errors, and both unsupported and irrefutable claims. The dominant surveillance discourse is not necessarily richer in these than the belief systems of opponents (a task for systematic empirical research to determine). However consistent with Gramsci's (Forgacs 2000) observations, it is *dominant,* and individuals clearly have socially patterned differential access to the ability to create and propagate surveillance worldviews. As such, there is a case for analyzing it in more detail.[4]

Techno-Fallacies

In listening to surveillance rhetoric over several decades I often heard things that, given my knowledge and values, sounded wrong, much as a musician hears notes that are off key. These involve elements of substance as well as styles of mind and ways of reasoning.[5] Below I identify 44 "information age techno-fallacies." Sometimes these fallacies are frontal and direct; more often they are tacit --buried within seemingly common-sense, unremarkable assertions. It is important to approach the commonplace in

a critical fashion—for groups with which we feel an affinity, and those with which we don't.

This approach to analyzing technology advocacy rhetoric follows in the broad tradition of Mumford (1934), Ellul (1964), Weinnberg 1966, Winner (1988), Postman (1992), Tenner (1996), Scott (1998) and Rosner 2004 and in the more focused work on topics such as computers, the environment, energy and crime (e.g., Wiener 1967, Weizenbaum 1976, Morozov, 2011, Mander 1992, Hilgartner, Bell and O'Connor 1998, Marx 1995, Grabosky 1996). While I could have identified fallacies (as well as truths) unique to particular information extractive tools (e.g., Corbett and Marx 1991) and contexts, this chapter offers ideas that apply across the surveillance field.

Beliefs may be fallacious in different ways. Some are empirically false or illogical. With appropriate evidence and argument, persons of good will holding diverse political perspectives and values may be able to see how they are fallacious, or in need of qualification.

Fallacies may also involve normative statements about what matters and is desirable. These reflect disagreements about values and value priorities. To label a normative belief a fallacy more clearly reflects the point of view of the labeler and goes beyond Mannheim's methodological neutrality. However, normative positions are often informed by empirical assumptions (for example, favoring a hidden rather than overt watching because it is believed to be more effective). In sniffing out fallacies, one must identify and evaluate the intermingling of fact and value and the quality of the facts (Rule 1978, Bell 1997). At a very general level, people often agree on values (though they often dissent over prioritizing and implementing these). Disagreements are also common over

what evaluation measure(s) and specific tools for judgment are most appropriate and over how evidence is to be interpreted –both with respect to what it says empirically and to its meaning for a given value.

Below I discuss 44 surveillance-talk assumptions I find questionable, or worse. This discussion is illustrative, and if I have failed to comment on a given assertion, this should not be taken as evidence of concurrence, although even I view certain statements within the surveillance rhetoric as eminently supportable.

While some of these techno-fallacies overlap, I group them into 5 broad categories (see table 15.1):

1. Fallacies of technological determinism and neutrality
2. Fallacies of scientific and technical perfection
3. Fallacies involving subjects
4. Fallacies involving questionable legitimations
5. Fallacies of logical and empirical analysis

[Table 15.1 here]

A. Fallacies of Technological Determinism and Neutrality

The fallacies in this group involve the failure to see the role played by humans in developing and applying technology, and they reduce issues of cultural and political dispute into matters to be resolved by the application of technology.

1. THE FALLACY OF AUTONOMOUS TECHNOLOGY AND EMANATIVE DEVELOPMENT AND USE

This fallacy follows a key piece of advice from the Wizard of Oz. I refer to the scene in which the dog Toto pulls away a curtain revealing an ordinary mortal, rather than an all-powerful wizard, and a voice tells Dorothy and her friends to "pay no attention to the man behind the curtain," the justification being that "the Great Oz has spoken."

The idea is that the technology drives itself and follows an internal logic that must unfold. It's as if the technology resulted from an immaculate conception apart from human will or interests. The proponent of this fallacy ignores variation in outcomes and the role of values, design and interests, assuming that people and social forces are irrelevant to technological wizardry. Further, the assumption of an invisible, unstoppable, progressive (in both a technical and social sense) logic of technological determinism obscures responsibility. To paraphrase a traditional bumper sticker, "Relax, technology is in control."[6]

Even many persons who are less welcoming of technology have a fatalistic sense that there is no escape. The etching is on the silicon chip. This can result in a self-defeating prophecy in which, believing that something undesirable can't be stopped, individuals take no action and by default encourage it.

The development of surveillance technologies is hardly self-evident. The statement "you can't stop progress" cries out for social and cultural analysis of the

meanings of progress. Technology involves both social and physical processes. It is hardly external to its settings.

There are no natural laws that require particular technical developments and applications, nor can a technology's characteristics fully capture its social meanings and impacts (Pinch and Bijker 1984, Bijker et al 1987, Graham and Marvin 1986, Leman-Langlois 2008).[7]

The police leader who said, "if the technology is available, why not use it?" should first ask questions such as, "what are the likely consequences of using this technology, and how does its use compare to that of other technologies and to the consequences of doing nothing?" We live after all in a democracy, not a technocracy. The fact that a technological potential exists, or even a technology, can never be sufficient justification for it, nor can it tell us with certainty the way(s) it will be used.

2. THE FALLACY OF NEUTRALITY[8]

When asked, "isn't the technology neutral?" George Orwell reportedly replied, "so is the jungle." The neutrality argument can conceal the hidden hands and unequal social terrain often lurking in the background. It masks power relations and draws attention from social and ethical questions.[9] Those backstage are protected from the ordinary reciprocity found with face-to-face interaction. This invisibility[?] may complicate efforts at accountability, and in extreme cases make it easier to take inhumane actions. Tom Lehrer's parody of Werner Von Braun’s rockets applies: "where they go up and what they do when they come down depends on the technology, not me."

The neutrality fallacy denies the political character of much surveillance. If questions are merely technical, and if surveillance is neutral in its impact, then there is no need for discussion or negotiation, and the structural roots of the problem that is presumed to be addressed by the technology go unresolved.[10] This fallacy also ignores the market-driven quality of much surveillance--for example, the claims by credit reporting bureaus hired by industry that they are neutral overlooks the fact that they are paid by the lenders. Would credit reports ask the same questions and operate in the same fashion if they were instead hired by consumers?

The distancing of the technology from its creators and its automatic (rather than direct human) application do not mean that the technology has equal impacts across society or that moral responsibility has been eliminated. The neutrality fallacy thus leads to a related fallacy of equality of development, access and application.

A technology can fail to be neutral in several ways. First, as suggested above, inequality in power and resources determines what groups are best positioned to sponsor the *development* of new technologies. If surveillance technologies were developed to serve the interests of the poor, workers, children, consumers, or developing countries, would we see the same technologies as we do when the technologies are developed and applied to serve the interests of the military, business, industry and the most developed societies?

Regardless of who develops the technology, it is rarely *equally available or useful* across society. In some ways modern means of communication and surveillance, from the printing press through to the Internet, tilt toward greater equality and

participation. But the individual who can access the Internet in the same way as large organizations can is not therefore made equal to them. To the extent that access is restricted by proprietary codes or cost, the ease or difficulty of using the tool is irrelevant. Furthermore, while the cost along with the skill required to use much of the technology has steadily lessened, the skill required to understand and fix it has in general steadily increased, enhancing dependence on, and trust in, specialists (for example, with reliance on computer diagnostics, note the disappearance of home auto repairs).

One must heartily agree with Mr. Bottoms that the technology is indeed neutral in what it captures, just as a weapon can be neutral in the damage it can inflict, regardless of the social characteristics of the target. Yes, the technology will respond to whomever appropriately enters the command or pushes the buttons, and it can offer data on whomever is sensed or identified. However, organizations relative to individuals and more privileged persons relative to less have greater resources to take advantage of new technologies. This permits them to go further in crossing the information borders of others and to better protect their own borders.

In the absence of categorical application (e.g., requiring all who fly to go through a metal detector), the egalitarian potential is undercut because the social contexts in which the technologies are applied are often far from neutral.[11] The rich have little need to shoplift or to sleep behind malls, let alone under bridges. Nor are the "equal opportunity" monitoring tools such as video-cameras and phone and computer monitoring that are applied to workers likely to be used for executives.

Finally, in highly differentiated societies, the technological advantages are unlikely to be equally distributed. Equality is likely to be greater in societies with a high degree of consensus and homogeneity and in settings where goals are shared, universal criteria determine the allocation of surveillance resources and where norms of, reciprocity are present.

3. THE FALLACY OF QUANTIFICATION[12]

Before automatically going by the numbers, it is necessary to understand the process by which they were created. What will be measured, how will it be measured, who will measure it, who will it be applied to, where will interpretive lines be drawn, and how competent is the system for interpreting the findings? How strong and consistent is the evidence? Are there procedures for questioning the evidence?

Measurement and interpretation have strong social components and are hardly of divine birth. The seeming objectivity of numbers should not prevent us from seeing that they reflect choices (for example, which means will be used for drug testing, what drugs will be tested for, where threshold levels will be set and how results will be used). Even when measures are valid, the tilt toward numerical measurement may mean giving lower priority to values that are hard to assess with numbers.[13]

A related problem is that in emphasizing numerical measures, the quantity of data may indeed increase but at a cost to the quality, and goals may shift. In a finding well known to organizational researchers, the emphasis may be placed on what is measured rather than the broader goal the measure is presumed to indicate.[14]

There is a danger of being captive of one's method. Consider the story about a drunk who lost his wallet in the middle of a dark street, but who looked for it on the corner, where there was a street light. When a friend asked him why he was looking there, he said, "because the light is better." While precision may generally be preferred to imprecision, we should not equate our sense of "reality" and the grounds for decision-making with, or reduce them to, what we can most easily and reliably access and measure.

4. THE FALLACY THAT THE FACTS SPEAK FOR THEMSELVES

Data are not knowledge. Seeing should not automatically be equated with believing. The facts do not speak for themselves. They are inert artifacts. We need always look for the ventriloquist in the wings. Surveillance facts are socially defined and interpreted. Any human knowledge, no matter how powerful, valid and useful is always abstracted out and partial. It represents only a fraction of what might be attended to, and it might be intended to deceive. Whitehead noted that, "there is a danger in clarity, the danger of overlooking the subtleties of truth." We need, as he also suggested, to seek simplicity but to meet it with skepticism.

Alternative information or a fuller picture could suggest a different meaning. As the fallacy of acontextuality (32) indicates, to adequately interpret we need to know what is specific to the setting and example.

As with the measurement fallacy above, we must ask how the measurement was created and how it is interpreted. The discretionary elements in the setting of standards for alcohol and drug testing offer a good example. The red light cameras for traffic

control are another. The number of red light runners apprehended is partly a function of how the equipment is set. Once the stop light has turned red, the grace period (before a traffic citation is issued) can be set at varying speeds –e.g., one second, three seconds etc. The shorter the duration, the greater the number of apprehended "violators." The "facts" as represented here by the number of violations are thus a function of how the tactic is calibrated.[15]

5. THE FALLACY THAT TECHNICAL DEVELOPMENTS MUST NECESSARILY MEAN LESS PRIVACY

Some surveillance advocates argue that given technical developments, privacy is finished and we should get over it.[16] The Supreme Court case of Katz v. United States is drawn on for justification. This case introduced the reasonable expectation of privacy standard. In this context, the meaning of "reasonable" is shaped by two factors –first what society is prepared to tolerate and second what the technology is capable of. With regard to the latter, some court decisions imply a steady whittling away of privacy rights as the technology becomes ever more powerful. In other words, unless one takes protective actions against surveillance, a reasonable person should not expect privacy, given what the technology can do. But the more important standard is clearly what society deems to be reasonable given democratic values, not reasonable in terms of what technology can do. What *could* be done given the capability of the technology is distinct from what we expect *should* be done given ethical standards. Powerful technologies that are invisible to subjects should be subject to regulation, whether out-right prohibitions, judicial warrants and other forms of regulation, or informed consent. Technologies can also be developed to protect personal information.

B. Fallacies of Scientific and Technical Perfection

In this group of fallacies, we see an overly optimistic, even utopian, faith in the efficacy of technology and its ability to solve problems without simultaneously creating new ones.

6. THE FALLACY OF THE 100% FAIL-SAFE SYSTEM

In complex environments rich in uncertainty, machines and those who run them are of course fallible. As the work of Perrow (1984) on Three Mile Island, Vaughan (1996) on the Challenger disaster, and Tenner (1996) on a broad range of technologies suggests, mistakes and unintended consequences adhere and inhere.

Claims such as, "but the computer says" or "it's in the computer" are offered as equivalent to a law of nature. But being "in" the computer guarantees neither accuracy nor appropriateness. Human agents have set the rules for collecting, entering and analyzing the data.

What may be very effective in a controlled laboratory setting may fail in the messiness of the real world. Consider some of the problems initially found with the use of electronic location-monitoring devices in which mylar in the walls gave false readings. Even where the measure is in principle valid and reliable (unlike with the least expensive drug test or the polygraph), it may be incompetently applied or neutralized.

7. THE FALLACY OF THE SURE-SHOT

Here we see a loose canon related to the fact that loose cannons may over- or under-shoot the target. Thus, this fallacy assumes that surveillance obtains its goal with

laser-like precision and has no impact on adjacent or unintended targets and broader surroundings. But in a complex world where much can go wrong, there are often second-order effects. Displacement can also occur. As research on video surveillance and crime suggests, a problem may simply be moved as security increases in one place but decreases in another. With respect to such displacement a prosecutor noted, "the bad pennies never get lost, they just move from one pocket to another."

8. THE FALLACY OF DELEGATING DECISION-MAKING AUTHORITY TO THE MACHINE

Given the limits of technology, there are obvious limitations in delegating decision-making authority to a machine, absent human review. As William James (1950) argued "the art of being wise is the art of knowing what to overlook." Discretion—a capacity that is central to wise actions--can be severely limited by the automatic quality of the machine. Because computer programs rely on selected categories of information, they are not equipped to deal with much of reality's richness the way a human can. This is particularly the situation for atypical cases and extenuating circumstances. The nightmare version of this is a war automatically generated in response to faulty data from sensors. Elephants, as well as soldiers (one’s own and adversaries), step on land mines.

9. THE FALLACY THAT TECHNICAL SOLUTIONS ARE ALWAYS TO BE PREFERRED

This is an error in both logic and definition. The solution chosen for a problem (if there is one) reflects assumptions and choices. Thus, with respect to surveillance issues, drug education or decriminalization are alternatives to drug testing. Paying workers well

and treating them with dignity will likely mean less need for intensive monitoring. The turn to a technology for surveillance should be based on analysis and a weighing of alternatives, rather than being the default position. For example, in intersections plagued by accidents from red-light running, the first step should be to analyze the broader causes—say, to see if altering road conditions can make a difference--before turning to cameras.

Rarely will complex problems existing within contexts of human liberty, conflict and creativity yield best (or only) to simple technical solutions, let alone explanations (see the related fallacy of reductionism). Even when all goes according to plan, at some point, the technology may malfunction--and given enough time or cases and complexity, at some point it is likely to. A society that can only maintain civil behavior by technical means is a society in trouble.

A related fallacy is that "technical problems must have technical solutions." For example, a common response to problems created by Caller-ID (e.g., revealing unlisted numbers) or eavesdropping devices is to come up with a counter technology that blocks or distorts. But such problems could also be addressed by regulating, prohibiting or limiting the technology and by education and manners.[17] This reflects the failure to see larger pictures and broader causes. [cartoon re knife and cause]

10. THE FALLACY OF THE FREE LUNCH OR PAINLESS DENTISTRY

Of course, this is nonsense. There are no free meals, and your teeth may hurt when the Novocain wears off. Those under the sway of this fallacy my conveniently ignore or fail to see collateral costs, especially when they involve powerless groups and

future costs. But the truth is that any format or structure both channels and excludes, generating trade-offs. In gaining one advantage we may lose another (e.g., breadth vs. depth, validity vs. low cost).[18]

If nothing else (and in a highly interdependent world with imperfect knowledge, there almost always is something else), a given use of resources involves forgone opportunity costs. Where might the resources go if the technological means are not used? For example, in the case of expensive screening for currently incurable diseases, the resources might instead be used to seek cures. Even where the case for using an intrusive technology is strong, we need to ask about the creation of unwanted precedents for other less justifiable uses and unwanted developments. These involve the next fallacy.

11. THE FALLACY THAT TECHNOLOGY WILL ALWAYS REMAIN THE SOLUTION RATHER THAN BECOME THE PROBLEM

We now know that today's solutions often become (or contribute to) tomorrow's problems. Contrary to Dr. Frankenstein's experience, this fallacy involves the belief that we can control the technology rather than the reverse. To counter this fallacy, the utopian imaginations of advocates need to be balanced by the dystopian imaginations of social critics and science fiction writers envisioning what might go wrong.

An aspect of this fallacy is failing to ask what kind of a precedent the adoption of the technology may create and what it opens the door to. A questionable means applied on behalf of an urgent goal is sometimes justified by the argument that "we can control it and will apply it only in this one narrow area." But given power differentials, there is a

tendency toward surveillance creep, as a once-restricted tactic spreads to new uses, users and targets.[19]

12. THE FALLACY THAT THE MEANS SHOULD DETERMINE THE END

As Albert Einstein observed, "perfection of means and confusion over ends seems to characterize our age." To a person with a can opener, the whole world looks like a can. Where there is a way, there is often a will.[20] A major critique of industrial society is that means too often determine ends; a related form involves the ritualistic danger of the means becoming the end.

It is vital for civilization (if not always for self- or organizational interests) that public policy starts with goals--asking what do we want to accomplish--instead of starting with a tool and asking how we can apply it. Problems should drive solutions rather than the reverse. The task should not be to find a job for the tool but rather to ask, "is this the job that ought to be done?" An alternative, more critical approach asks about goals and then a variety of means.

Goals may also change as a result of applying means without adequate discussion. Thus the installation of red light cameras may initially be for the obvious purpose, but once they are installed, the city may come to rely on the income and be more concerned with obtaining the fines than with stopping red light running. In a related example, some police departments have found that computers can greatly aide in the collection of revenue from parking violations. This is relatively clean work, and it creates impressive success in both statistics and revenue. However, in some jurisdictions traffic enforcement

has expanded at the expense of more traditional police goals with little official or public discussion.

In considering means-ends connections, we must also attend to issues of proportionality and appropriateness found with the misbegotten cracking a nut with a sledge hammer.

C. Fallacies Involving Subjects

Here, we find questionable views regarding people as objects to be controlled rather than as citizens to be treated with dignity. With each of the fallacies in this category, the proponent communicates a symbolic message of objectification and manipulation of the human.

13. THE FALLACY THAT INDIVIDUALS ARE BEST CONTROLLED THROUGH FEAR

Nineteenth-century positivist theories of law and the presumed link between rationality and conformity gave great force to the belief that the more anxiety people felt over discovery, apprehension and sanctioning for normative violations, the better their behavior would be. This is related to several other "more" fallacies to be noted below.

In spite of surveillance developments, it is often impractical to watch everyone all the time. An efficiency measure inherent to Bentham's Panopticon was making subjects aware that they stood a chance of being seen, even if this often wasn’t the case. Given the uncertainty, the rational person is presumed not to want to take the chance that the video

camera is a fake, that (for a sales clerk) a difficult customer isn't a secret shopper, or that a random search or drug test won't be carried out.

The effort to engender fear and apprehension is an important part of some contemporary surveillance rhetoric. It may sell tools and elect politicians, but taken to an extreme, it is morally and empirically bankrupt in civil society. Things are usually much more complex than the messengers claim. Democratic principles require respect for the individual and tolerate a degree of disorder as a concomitant of a free society.

Certainly in many settings accountability increases proportionally with the visibility of compliance. But no such simple statement can be adequate for all complex human situations. Other factors being equal, good behavior is more likely to occur when individuals have participated in setting the standards, understand the reasons for them and feel respected by an organization. Adults are likely to resent being treated as children or as prisoners. When climates of fear and suspicion are created, innovation will be less likely and divisions between controllers and controlled will be deepened.

Even holding apart issues of effectiveness, means have a moral quality as well as ends. Policies to effect behavior out of fear, coercion (whether technical or social), and threat of punishment, while certainly needed, need not be unleashed or unreflectively favored over other approaches. The head of a large private security agency observes, "the best protection an employer can buy is not high-tech alarms or key card systems. It's employee trust and loyalty that will keep people from stealing or motivate them to turn in a colleague who is."[21]

14. THE FALLACY OF A PASSIVE, NON-REACTIVE ENVIRONMENT

Here we have the erroneous assumption that environments, especially those where there are conflicts of interest, are passive rather than reactive. But the tacks in the shoe that can function to thwart surveillance (neutralization effirts discussed in chapter 6) make it clear that isn't the case. Innovations in surveillance must be seen as variables in dynamic situations. There is a Social Heisenburg principle in which the act affects what is acted upon beyond its goal. This may be particularly noticeable over time, as the effectiveness of a solution lessens. New controls create new challenges and opportunities. Every lock has a key. As chapters 6 and 7 suggest, any solution that one group of smart people creates can be circumvented by another group, whether through technical or social means.

15. THE FALLACY OF IMPLIED CONSENT AND FREE CHOICE

Consent and choice are very difficult concepts to assess. Individual have cognitive limits on what they can know, and factors at many levels limit the amount of freedom in a "free" or willing choice. Certainly, one can protect one's privacy by not using a phone or computer or driving a car. But that is almost like saying if you breath polluted air or drink contaminated water, you consent to these environmental circumstances. The conditions of modern life are often such that one can hardly avoid choosing actions that are subject to surveillance. While the surveillance may be justified on other grounds, it is disingenuous to call it a free and informed choice.

16. THE FALLACY THAT PERSONAL INFORMATION IS JUST ANOTHER KIND OF PROPERTY TO BE BOUGHT AND SOLD

Personal information has a special quality, something that under some conditions seems sacred and inviolate. Yet it is not the same as raw materials or office furniture. Europe recognizes this to a greater extent than has the United States. Its concern to protect the dignity of the person (as broadly defined) restricts the sale of personal information.

Those in the data warehouse business often show inconsistency, if not maximally self-serving attitudes, toward property. On the one hand, in the collection phase, personal data is treated as a free public good, like air. It is just there waiting for whomever wants it. Yet once it is harvested, it becomes private property to be used as the possessor wishes, even including selling it back to those it pertains to (e.g., credit scores).

This contrasts with other free goods such as radio transmissions or a photo of a person taken in a public place. There, the gleaner is likely to be within his or her rights in gathering what is "freely" offered. Yet in principle it is a violation to sell this without permission. Why should it be any different when selling other kinds of personal information, such as credit card data? Greater consistency would be present if companies selling personal data paid the person whose data it “is” or at least “was.”[22]

Applied too broadly, the property-possession analogy for personal information fails at several points.[23] Simply because one may easily intercept personal data does not mean that it is appropriate to market the information. The strictures I refer to here are parallel to those in the Tom Voire case about not staring, or averting one's eyes to avoid embarrassing another person. Legal and professional codes protecting confidentiality also limit what can be done with personal data.

Even if viewing personal information as property is appropriate, there is likely a need for a safety net or equity principle guaranteeing a minimum threshold for withholding information, regardless of what the technology is capable of and what financial situation might propel some individuals to give up control over their personal information. There must be limits on the extent to which privacy is treated simply as a commodity, whether for those able to pay for more, those driven to sell what they have, or those with the resources to indiscriminately gather personal information.

An individual's privacy is linked to aspects of free choice. Current proposals to create privacy platforms for internet use in which individuals specify their preferred privacy level acknowledge this. Yet even an individual's choice to provide personal information may not be sufficient justification. The law and manners limit what we can voluntarily reveal. Note restrictions on public nudity and noise, restraining orders and confidentiality protections. There are little-noticed privacy thresholds that individuals are expected to adhere to. These are equivalent to other free choice limitations--e.g., against selling your kidneys or your self into slavery or prostitution.

But linking policy exclusively to preference and marketing criteria can be troubling. For example, during the Caller-ID conflict, marketing research found that West Coast customers in the United States were more concerned with privacy protection than were those who lived elsewhere. As a result they were offered ways to block Caller-ID not available to other customers. Marketing research ought not to override issues of principle.

17. THE FALLACY THAT IF CRITICS QUESTION THE MEANS, THEY MUST NECESSARILY BE INDIFFERENT OR OPPOSED TO THE ENDS

This is a classic smear tactic that permits shifting the debate away from the tactic to the presumed beliefs and motives of the critic, with the implication that he or she is soft on some problem like drugs, dishonest or unproductive workers, or national security and likely unpatriotic and unkempt as well.[24] The critic's interest in considering the moral status of means, or giving higher priority to other values, or voicing concern about effectiveness, costs and precedents is not acknowledged. Too often the critics concerns are dismissed based on cultural clichés and caricatures of Big Brother and Dr. Strangelove.

The parties often talk past each other from different assumptions and levels of abstraction. Advocates tend to be more concrete and focused on the immediate problem they see and the technical solution, while critics are more likely to raise broader and longer-term issues. Critics often fail (both strategically and humanely) to acknowledge the deeply felt concerns that can motivate surveillance application crusaders. While advocates do not see that the critic’s opposition can stem from trying to strengthen the system by questioning aspects seen to undermine it. Criticism can reflect loyalty rather than subversion. Those in dissent would often have greater impact if they can acknowledge the significance of a problem propose alternative means, urging caution and warning that the proposed cure may be worse than the illness. t

Whether proponents or opponents of a tactic, the quality of debate could be much improved if the parties refrained from trying to demonize the opposition and if they paid

greater attention to making their case based on logic and the empirical record (as limited as it is usually likely to be).

18. THE FALLACY THAT ONLY THE GUILTY HAVE TO FEAR THE DEVELOPMENT OF INTRUSIVE TECHNOLOGY (OR IF YOU'VE DONE NOTHING WRONG, YOU HAVE NOTHING TO HIDE)

This ignores a major social function of personal information borders and the principle that means, as well as ends, have a moral component. Privacy is valued not because of a desire to protect wrongdoing, but because the control of personal information is central to the person's sense of self and autonomy. All persons have things they do not wish to be compelled to reveal. The ability to control informational boundaries is also necessary for autonomous groups within civil society.

This fallacy also connects to #33 regarding representativeness and generalizing from one's own experience and attitudes. That Rocky Bottoms may not care who knows what kind of cat food he buys is not sufficient grounds for a general public policy. The "I don't care who knows" statement is frequently heard. Certainly within limits, the norms around privacy (in contrast to those around secrecy) permit an individual to reveal information. But that hardly justifies a public policy of mandatory revelation.

A person taking AIDS medication may care a great deal about having that known. But even in the cat food example, the speaker does not realize that he may have good reasons for protecting non-stigmatizing or non-discrediting information. This is because bits of data can be combined into a mosaic greater than the sum of the individual pieces, potentially undermining consumer and other forms of autonomy. The likelihood of

manipulation or wrongful discrimination increases as constraints on the collection of personal information decrease.

Borders have functions as well as dysfunctions, and both must be acknowledged. Surveillance advocates for example note only the negative side of compartmentalizing personal information. While any given strand of behavior or identity may be innocuous, the collage from combining many strands brings a qualitative change. The ability to be unnoticed, or rather noticed when one wills it, is an important element of liberty. It creates space for both social maneuvering and solitude.

D. Fallacies of Questionable Legitimation

Justifications are a central part of any worldview. These involve values and assertions about outcomes. The fallacies below involve dubious justifications and more directly reflect ethical assumptions than the other fallacies.[25] The problem is not so much with the value itself, but the lack of nuance; it is too literally expressed, and its fails to acknowledge or weigh other interpretations, competing values and contexts, and alternative outcomes.

19. THE FALLACY OF APPLYING A WAR MENTALITY TO DOMESTIC SURVEILLANCE

A misplaced war imagery with its rhetoric of subjects as enemies and permanent victory dominates many contexts of domestic surveillance. Yet most of those subject to domestic surveillance are not enemies in a war. They are citizens, employees, customers and children with rights and expectations of respectful treatment. This fallacy denies

legitimate conflicts of interest and the view that rather than final victories to be won, we usually have enduring problems to be managed.[26]

As the material throughout the book suggests, human inventiveness in a free-market economy with civil liberties protections, legitimate value conflicts, and changing contexts means that the interaction of those in conflict is in general ongoing, rather than ending with a clear victor. The symbolism associated with using war imagery can lessen inhibitions on means-ends relationships and result in a demonization of those with opposing views, who become not only wrong, but evil. Even in the case of contemporary external wars, we face questions about whether they can be finally won rather than managed, and if victory is possible, at what short and long run costs?

20. THE FALLACY OF FAILING TO VALUE CIVIL SOCIETY

In noting how social borders and restrictions on information collection may indeed make the job of government and commercial organizations more difficult, advocates fail to acknowledge that that is exactly the point and a central facet of modern democracy and limited government.[27]

To protect liberty, government, organizations and individuals are restrained. The deep involvement of government in an ever-increasing number of areas of individual choice traditionally considered private--whether the family, leisure or commerce--must give us pause, even as we recognize the increased interdependence and complexity of modern society and the need for new forms of accountable regulation. That also holds for the increased blurring of the lines between government and the private sector.

21. THE FALLACY OF EXPLICIT AGENDAS

Beyond a lack of well thought out goals, surveillance advocates may deceive subjects and the broader public with respect to the reasons they give for use of a tactic. The fallacy is to assume that the technology is applied only for the manifest rather than for unstated reasons, that what you see is what you get, and "we know where we are going." Yet policies may reflect efforts at symbolic communication and internal organizational conflicts beyond their stated goals. For example, drug testing or the questions asked in a job interview may have as their goal enforcing a particular morality unrelated to job performance per se. Video surveillance ostensibly undertaken to counter theft has been used as a cover for gathering information during unionization drives.[28]

In addition to asking what the agenda is, we must ask, whose agenda? With the blurring of lines between the public and the private, ostensibly public goals may be undercut by commercial goals. Thus, in delegating enforcement of red light violations to private contractors, cities such as San Diego and Washington D.C. ran the risk of confounding the ostensible goal of public safety and justice with the business goal of profit maximization. The city, too, while talking about traffic rules (whether for speeding or parking) may have as a more basic goal maximizing revenue. The mixing or obfuscation of goals with such delegation can also insulate and distance government from accountability.

22. THE LEGALISTIC FALLACY THAT JUST BECAUSE YOU HAVE A LEGAL RIGHT TO DO SOMETHING, IT IS THE RIGHT THING TO DO

Certainly we must start with the law, but not stop with it. The fact that a practice is legal does not mean that it is wise or just, or that it will not at some point become

illegal. In many cases new tactics are permitted simply because problems have not yet been realized or the political will to control them is absent. As noted in ch. 13, there is often a lag. The absence of rules to prohibit is not equivalent to a legislative affirmation of a right to apply a tactic.

In many states, as long as one party agrees, it is still legal to secretly videotape or audiotape others. In other cases, the public may perceive the need for legislation, but a powerful lobby is able to prevent it (e.g., an industry coalition against a work-monitoring bill that would guarantee workers the minimal right to be informed of monitoring). Judged in a broad moral and social context, law offers us a minimum standard, and its spirit as well as its letter matter.

23. THE FALLACY OF RELATIVISM, OR THE LEAST BAD ALTERNATIVE

Just because an approach is less undesirable than other approaches does not automatically make it acceptable. When dealing with competing wrongs, the less onerous is certainly to be preferred, but the choice is not a happy one. The state of being a lesser evil (or, for some of the tradeoffs, simply less desirable) is not equivalent to being a good. This background belief shows more humility than most of the others in acknowledging costs, but there are times when doing nothing in the face of limited choices is preferable.

24. THE FALLACY OF SINGLE-VALUE PRIMACY

A given value is assumed to *a priori* overrule other values with no need to make the case for why. For example, pragmatism and/or efficiency are seen to automatically

overrule other values such as fairness, equity, external costs imposed on third parties, and symbolic meanings.

Certainly given a concern for justice, scarce resources, a scientific ethos and common sense, we must ask, "does it work?" (holding apart the issues around defining and measuring this). But an affirmative answer shouldn't lead to the automatic unleashing of the technology, absent consideration of other values, in particular those that are difficult to measure, or that transcend the moment.

More than instrumentality must be considered. Our culture attaches morality to means as well as ends. Of course if you "hang them all," you will certainly get the guilty. Yet there is more to collective life than pragmatism; attention to collateral consequences and a sense of proportion are required.

Applying a technology conveys social and historical meanings regarding values and how individuals are viewed. Symbolic meanings also need to be considered. The use of informers and hidden devices can communicate distrust and dystopia. Fingerprinting is a relatively reliable method.[29] Yet because of its historical association with criminals, it has a symbolic meaning that is independent of its usefulness and appropriateness in particular contexts (Murray, 2000).

25. THE FALLACY OF LOWEST COMMON DENOMINATOR MORALITY

According to this fallacy, if others push moral limits, it is acceptable to push back. But a bad precedent hardly justifies further bad behavior. For example during the Caller-ID wars, local phone companies justified the service by saying that since commercial toll-free carriers automatically had it, they should be entitled to it as well.

Folk morality suggests that two wrongs do not make a right. The fallacy of the lowest common denominator morality assumes that if your side doesn't use the technology, your opponents will, thus giving them an advantage. This rationale is often heard in justifying intrusive work monitoring, given the practices of competitors in a global economy. This sounds plausible until one learns that neither Japan, nor Europe, make as extensive use of new surveillance practices as does the U.S.

Taking the moral high ground may be its own reward. Maintaining a positive reputation and treating subjects with respect and dignity can be powerful competitive resources as well.

26. THE FALLACY THAT THE EXPERTS ALWAYS KNOW BEST

The problem of automatic deference and delegation to (often unseen) technical experts is a central concern in the critical analyses of technology. It depoliticizes issues that should be discussed and negotiated. Moreover, the secrecy and incomprehensibility of experts can mask bad behavior and mistakes.

Professionalization and specialization—with its "trust us; it's for your own good" message—can conflict with democracy, citizen participation, self-help and breadth of perspective. As Edward Shils, observes, "a society ruled by experts, specialized in their own fields and ignorant and indifferent to the rest, would be a poor way to continue as a free society" (1956 P.156).

The justification embedded in this fallacy overlaps the absolute faith in technology that runs through many of the fallacies. "Will they believe it?" a hacker in the film "Sleepless in Seattle" asks her friends after changing data in a computer, and the

friend replies, "if it's in the computer, they'll believe anything." Given the issues noted above, the aura of legitimacy that may automatically be granted technical answers is troubling.

A key question one could ask in response to this fallacious claim is, which experts? As numerous controversies make clear (e.g., nuclear power or global warming), scientists often disagree. Even if scientific experts can agree about causes and consequences, there is usually still a large leap to answering normative questions about what should or should not be done. One standard must be, would the expert unreservedly submit to the surveillance practice in question as the subject?

27. THE FALLACY OF THE VELVET GLOVE

However attractive, the tendency toward softer means can be beguiling. It is hard to say "no" if you are unaware of what is going on and/or are not inconvenienced. Just because personal data can be collected relatively silently and non-invasively, does not justify doing it apart from the goals. Judge Brandeis noted that vigilance was most needed when purposes were benign.[30] The same might be said for the softer, non-invasive means. Their seemingly non-problematic nature may take attention away from other aspects.

28. THE FALLACY THAT IF IT IS NEW, IT IS BETTER

The modern tendency to exalt in the new for its own sake must be carefully analyzed. Stressing that something is new may be good for marketing, but it is not necessarily good for public policy. New technologies with invasive potential must be subject to a broad range of empirical and ethical questions and not unreflectively

accepted as good simply because they are novel. Traditional means rooted in social conditions and developed through trial and error may reflect the wisdom of experience.

This fallacy of novelty is related to a "fallacy of intuitive appeal or surface plausibility." That is, "it sure seems as if it would work" combined with commonsense and a dash of wish-fulfillment can deter us from seeking evidence that the technology actually does work, doesn't involve undesirable side-effects, or is better than what it replaces.

Since many problems endure or re-appear, there is a constant search for better ways and a hope that "maybe this will work." Here we often see a "vanguard (or osmosis) fallacy," which assumes that "if the big guys are doing it, it must be good." Innovations often move from the major to minor players and to smaller or less prestigious organizations. The symbolism of wanting to appear up-to-date and of making progress through technology can be important forces, independent of the performance of the means or appropriateness for the context.

Many surveillance innovations have a fad-like quality involving broad media attention; quick, widespread adoption; diversification of the product; and then a rapid decline in use as limitations are realized.[31] The initial enthusiasm is encouraged by a "fallacy of ignoring the past." Contemporary receptiveness to surveillance innovations needs to be located within a broader framework of fads and fashions and cycles of reform.

29. THE FALLACY OF EQUIVALENCE, OR FAILING TO NOTE WHAT IS NEW

Ideologies strain toward consistency, yet they also almost always contain contradictory elements, whether out of self-interest, sloppiness or the difficulty of containing the world's complexity within a limited number of words. Bottoms, for example, argues that we live in revolutionary times and that the newness of the technology makes it desirable. Yet he also seeks to legitimate the techniques, by arguing that there is nothing really new and that each of the tactics has an accepted traditional counterpart. This is convenient, since, if his second point is correct, or if changes are merely incremental, there is no need for additional law or policy to permit or restrict use of the tactic. As noted in chapters 1 and 2, however, an enormous amount is new and in need of control, despite the continuities.

30. THE FALLACY THAT BECAUSE PRIVACY RIGHTS ARE RECENT AND NOT WORLD-WIDE THEY CAN'T BE VERY IMPORTANT

It is correct that privacy as it appeared in Western democratic mass societies is a historically recent phenomenon, not experienced, or perhaps even valued in many forms, by much of the world's population, or for most of human history. But what does that imply? Our assessments of good and bad ought not to be exclusively defined by individual preferences, majority rule, experts, or unquestioned reverence for standards applicable to other time periods and societies. Standards such as those in the United Nations' Universal Declaration of Human Rights offer a useful corrective to the undue glorification of local historical traditions that deny basic rights, even when these traditions are unchallenged.

E. Fallacies of Logical or Empirical Analysis

The preceding beliefs to some degree involve empirical and logical assumptions, but such assumptions are particularly important for those below.

31. THE FALLACY OF THE LEGITIMATION VIA TRANSFERENCE

A quote from a famous person or source is offered as sufficient justification for a position taken. This transference is well known in celebrity endorsements of products and politics.

32. THE FALLACY OF ACONTEXTUALITY

This is also the fallacy of literalism and universalism, in which one categorically asserts a normative principle or empirical finding, making no allowance for shadings, contingencies, mitigating circumstances, discretion or context. This envelops many of the inference errors noted in ch. 5.

33. THE FALLACY OF ASSUMED REPRESENTATIVNESS

A single illustrative case (often a personal example or one from the news) is believed to apply categorically, with no acknowledgment of potential variation or typicality or uniqueness of the case.

34. THE FALLACY OF REDUCTIONISM

A given cause or level of analysis is presented as sufficient for explaining and/or offering a simple (often unitary) solution.[32] However, almost every problem has a multiplicity of causes at different levels, and the causes may show varied interactions. With all these possibilities, one may also commit the fallacy of focusing on the wrong cause.

35. THE FALLACY OF A BYGONE GOLDEN AGE OF PRIVACY

This fallacy reflects a broad romanticized nostalgia for a time that never was. Rural areas and small towns may by default have offered some privacy from direct observation as a result of lower density. But the size of the community was often associated with intense curiosity about neighbors, gossip, and intolerance of non-conformity. Such communities offered far less formal protection of personal information, whether in the family, at work, in the marketplace or from government than does today's world.

36. THE FALLACY THAT CORRELATION MUST EQUAL CAUSALITY

This is a common failing of those in the persuasion business, as well as of some social scientists who should know better. Given dynamic conflict settings and their large number of variables, it is often difficult to say with the certainty that tactics work as well as advocates claim, nor that they fail as badly as critics claim.

Even when the desired outcome is present, inferences of causality are difficult to draw. The perennial problem of proving cause and effect is reflected in a story about a young man who each evening played the flugelhorn in the town square. He refused any tips. When asked why he came each night to play, he responded, "to keep the elephants away." He was told, "there are no elephants here." To which he replied, "you see."

37. THE FALLACY OF THE SHORT RUN

A focus on success in the present may mean a failure to consider longer-range negative consequences, including undesirable precedents and creeping encroachments

upon liberty. Consider the story about the person falling from the top of a 200-floor building. As the 150th floor is passed, a friend asks, "how are you doing?" The reply, "so far, so good." A story about a farmer who was having a hard time making ends meet is also illustrative. Someone advised him to feed his animals less, so he cut down their feed by 25%. It worked, and he saved a lot of money. He then said, "this is great, I'm going to cut their feed in half," and he saved even more money. And of course he kept on reducing their feed.[33]

38. THE FALLACY THAT GREATER EXPENDITURES AND MORE POWERFUL AND FASTER TECHNOLOGY WILL CONTINUALLY YIELD BENEFITS IN A LINEAR FASHION

As this is the American-inspired ideal that bigger is better, it might be termed a techno-phallicsy as well. With respect to opening up the coffers and ratcheting up the technology, we face issues of appropriateness of the technology, proportionality, threshold and time frame. There's nothing inherently good or bad about the increased power of a technology. Our judgments must flow from analysis, not from the ability to increase the dosage. As Simmel (Coser 1964) noted in situations of conflict, more may simply result in escalation, as opponents turn to equivalent means and discover ways of neutralization.

Greater speed ironically offers advantages of currency and prevention but in tandem with enhanced speed there is less time for careful deliberation and consideration of the long run (see fallacy 37). Surveillance agents may tilt toward the kind of data that can be immediately gathered and processed, which may not be the kind of data that are

most important. With respect to linearity, as with medicine, one usually reaches a point where increases in dosage do not have equivalent therapeutic effects (e.g., some aspirin will help, but if you take the entire bottle, you may die). This aspect is central to the next fallacy.

39. THE FALLACY THAT IF SOME INFORMATION IS GOOD, MORE IS BETTER

A children's poster shows 11 hippos stacked pyramid style in a canoe and a 12th jumping down onto it with the implication that the boat would capsize. It is captioned "more is not always better." This issue is treated at length in chapter 5 on social dynamics, where issues of converting data to knowledge, data overkill, information glut, and drowning in data are considered. [34]

The quality not the quantity of information is what matters, and personal information can often be compressed and protected in ways that organizations can use for verification without full access to personal details –as with assigning pseudonymous identities.

Of course, the enlightenment heritage of asking questions and valuing knowledge is fundamental, but that doesn't mean that all forms of personal information must always be widely available, or that all knowledge is good. Openness can have negative consequences in some contexts (e.g., certain forms of diplomacy or political decision making, strategic endeavors, manners). At times, it is morally, strategically and practically better not to know, and at other times, “it’s none of your business." At times, also, since nothing can be done about a problem, it may be better not to know and resources might be better used elsewhere.

40. THE FALLACY OF MEETING RATHER THAN CREATING CONSUMER NEEDS

This fallacy overlaps the notion of free choice and implies that consumption "needs," including perceptions of an appropriate level of security, rise up spontaneously within the individual rather than being generated by entrepreneurs. Of course there is always a mixture, but advocates seek to soften the harsher edges of manipulation by claiming that they are simply giving the public what it wants. Here, they deny the role played by propaganda and marketing strategies.

41. THE FALLACY OF THE DOUBLE STANDARD

The voices in the narratives strongly advocate the necessity and right to cross the information borders of others while calling for strong protections against others crossing their borders.[35] As noted in the next chapter, the legitimacy of crossing informational borders increases when parties are reciprocally able to do this.

42. THE FALLACY THAT BECAUSE IT IS POSSIBLE TO SKATE ON THIN ICE, IT IS WISE TO DO SO.

to When critics of technology point out possible negative consequences, a standard response is, "that's never happened" or "that couldn't happen." Yet foresight remains better than hindsight. It is unwise to wait until the damn breaks to decide to re-enforce or move it. There was a time when the nuclear accident at Three Mile Island and the Exxon oil spill in Alaska had not happened as well. It is not enough to show that a tactic has thus far been without disastrous consequences. In considering risks and worse-case scenarios, we must ask about the probability and cost of catastrophic failures.

Issues of scale may also apply. Thus, one person skating on thin ice may often be relatively safe, but not 100 persons.[36]

43. THE FALLACY OF RE-ARRANGING THE DECK CHAIRS ON THE TITANIC INSTEAD OF LOOKING FOR ICEBERGS

A cartoon shows a seated man with a knife stuck in his back. A doctor leaning over him says, "this will have to come out, but of course it doesn't address the deeper problem." And so it is with many quick-fix technical solutions to organizational or social problems; they are sometimes no more than Band-Aids on a hemorrhaging wound (e.g., removing benches from public areas as a response to homelessness).[37]

The emphasis may be on the wrong problem as a result of bad analysis or political factors. Technical solutions are often sold as cleaner, quicker and less expensive—as something that can be done—relative to the messy business of dealing with people and trying to understand the complex cultural and organizational reasons for many problems. And the mindset may in turn lead to the distorted view that "if you can't fix the real problem, fix whatever the technology permits you to fix." In such cases Thoreau's observation in Walden holds:

"But lo! Men have become the tools of their tools.
Our inventions are wont to be pretty toys
which distract our attention from serious things".

Attention to deeper causes and bigger pictures (with the implication that broad changes in a system may be required) do not play very well in the short run with a focus on the bottom line. Deeper analysis might even lead to the pessimistic conclusion that there are

no realistic solutions, or none that do not bring other problems. But if that is the case, it doesn't mean that the analysis was unworthy, that it might not shed some light eventually, or that the quick-fix is never an appropriate response.

To be sure, symptoms must often be treated as well as broader causes (if a bathtub is overflowing, one does need to mop the floor, as well as turn off the faucet). Yet too often the turn to a surveillance technology only deals superficially with the issues. Like an investigating committee, it can convey concern and give the illusion of action. An aspect of this is a shortened time frame.

44. THE FALLACY OF CONFUSING DATA WITH KNOWLEDGE AND TECHNIQUES WITH WISDOM

To varying degrees, all these fallacies reflect a broad, unquestioned faith in the efficacy of science and technology and the denial of tradeoffs. Technologies for extracting personal information are neither givens nor an automatic reflection of the natural world. As with the Wizard of Oz, the social hand behind the curtain and the levers of the machine need to be scoped out. Above all, technical mastery, or even knowledge, must never be equated with wisdom.

One Person's Fallacies Can Be Another's Truths

A necessary condition of wisdom is identifying and evaluating the web of tacit assumptions that are so intertwined with beliefs and action. The techno-fallacies discussed in this chapter and listed in the table differ in seriousness, and you will not hear any of them expressed universally, nor with equal intensity, by surveillance advocates,

who--as can be said of any group--have a diversity of positions. Moreover, the list is illustrative and not exhaustive.

The major point of this chapter is not to argue in depth against statements I view as techno-fallacies, but to argue for the importance of critically examining what is said about any new (or old) surveillance practice. Such claims too often go unanalyzed.

The above are techno-fallacies of the technophile. The most extreme advocates favor maximum security and minimum risk. They do not appreciate the virtues of civil society and traditional borders, nor do they recognize the limits on human rationality and control, let alone on human perfectibility.

Contrary to the fears Rocky Bottoms expresses in his opening speech, I do not offer these techno-fallacies in a spirit of prohibiting new technology. I do so in a spirit of sensitizing conservatism, asking us to pause in the face of any proposed change and raise the kinds of questions suggested.

Consistent with this spirit is the need to examine all claimants, not only those who are dominant or on the other side of the argument. Technophobes with extreme libertarianism and/or prejudicial skepticism too often fail to appreciate the advantages of technology, the virtues of community, and the dangers of anarchy, thus holding their own fallacies, or sharing some with their opponents --for example, too cleanly separating the human and the machine.[38] Or by adding "never" or otherwise reversing many of the statements listed in this chapter, we have some mirror-image fallacies of the technophobic (e.g., the fallacy that technical solutions are never to be preferred).

A speech given by privacy advocates Angela Topps or Charles "Chicky" Little could contain some additional fallacies: the fallacy that the sky is falling or the apocalypse approaching; that if you can imagine bad things happening, they surely will; that the people always know what's best (the populist fallacy); that privacy is an unlimited good (or if some is good, more must be better); that privacy is primal (i.e., that it ought to take precedence over other values); that privacy is only an individual value rather than a social one; that privacy can only be taken from someone, rather than imposed upon the individual; that because something worked (or failed) in the past, it will in the future; that technology is always the problem and never the solution (the Luddite fallacy); and related to this, that technology can only be used to cross informational borders rather than to protect them.

Of course Karl Mannheim notwithstanding, the academic analyst who tries to stand above the fray and between supporters and opponents also has perspectives. The analyst sees and speaks from a particular social location with values and interests. Those on the front lines–whether those who want to unleash or stop a technology-- don't necessarily share the analyst's perspectives.[39] Thus, a fallacy list surfacing the tacit and debatable assumptions of the academic is also in order.

Such a list might start with these: the risk-free Monday-Morning Quarterbacking; the overly broad academic generalization; the dressing of common sense (or non-sense) in multi-syllabic jargon replete with esoteric references; the use of Ockham's razor to nit-pickingly slice the world into too many categories; the timid waffling in the face of complexity and always imperfect data; the failure to clearly enough differentiate value

statements from scientific statements; and the reverse of failing to specify how the empirical within the value might be assessed.

Besides understanding the claimant's assumptions and possible fallacies, to further dialogue, we also need to know what rules the claimant plays by. The worldview of those who start with advocacy rather than analysis is by definition self-serving. The rhetorical devices expected there differ from those of the academic analyst, who must start with questions not answers and question all claimants. The scholar of course serves his or her interests in the pursuit of truth. But especially because they are making truth claims, they must also strive for consistency and a stronger tilt toward logic and evidence.

An academic analyst should offer data, methods, concepts and theories in an open, civil, self-interrogating, and critical environment. This should be accompanied by healthy doses of qualification, caution and humility (given dynamic situations, measurement challenges, and the paradoxes of the sociology of knowledge) in the face of complex, interdependent problems.

Undue confidence can be a danger in science and technology. For complex issues of social policy limits must be acknowledged, but they must not immobilize. One can rarely wait until all the data are in and there is scientific consensus. Even then, the non-scientific aspects of values and goals remain.

With the above cautions, the analyst may nonetheless wish to give advice, particularly for topics of social import. In doing so, she or he must try to keep statements of fact distinct from statements of value, while acknowledging the tensions and

interconnections between them. The key is awareness and tentativeness (or at least continual openness to examining assumptions and alternatives).

The presence of values, however, is nothing to run from. Indeed, the failure to acknowledge values and to coat them in the camouflage of pseudo-scientific neutrality, necessity, certainty and precision is at the heart of many problems. The next chapter continues the consideration of values by offering a framework for judging surveillance practices.

---

[1] Within the broader culture, if not necessarily within the cheering squads of the surveillance professions, there is deep ambivalence and a counter to this view (Dr. Frankenstein stories). Note the fear and suspicion of technology and distrust of strong government and big organizations. The speech contrasts with the anti-surveillance themes noted in chapters 8 and 9 commonly found in the work of artists, cartoonists, novelists, film makers and university based social scientists. Their work also contrasts with the pro-surveillance perspective more commonly found in radio talk shows, advertisements, industry sponsored think tanks and public relations efforts.

[2] Of course intellectuals have social locations, interests and blind and obfuscatory spots as well. Believing in empiricism, logic and the higher aspects of western civilization reflect value commitments. But there are some central differences as well, such as adhering to an open, self-interrogating critical standard beyond

specific contexts and awareness of the paradoxical nature of the sociology of knowledge.

[3] The number of fallacies is already too long (and to honor # 39 more need not be better). Some additional ones: confusing the simulacra with the phenomenon, saying I'm sorry makes it ok, crooks and suspects have no rights, contemporary wars can be won with finality, if a democratically elected leader does it is not illegal, confusing what is possible with what is or is probable, good motives excuse bad outcomes, imputing competent, technique based intentionality to outcomes we like in the face of fortuity while imputing ill will, incompetence and conspiracy to outcomes we don't like, the rush to inherent trade-off talk before analysis.

[4] The elasticity and vagueness of symbols and concepts is also illustrated. Thus Bottoms supports his case by reference to John Lennon, Bruce Springsteen, liberty, and freedom of choice—resources also in the verbal arsenals of critics.

[5] See for example Lee and Lee (1939), Lowenthal (1949), Shils (1956), Hofstader (1965) regarding simplistic, manipulative, non-refutable, demagogic, sloppy, heated, energized, dark, conspiratorial, paranoid, apocalyptic, Manichean, true believer rhetoric and propaganda that find fertile ground in sectors of the United States.

[6] The original: "Relax, God is in control."

[7] In the case of criminal justice for example Manning (1992) shows how police practices and local political traditions conditioned and limited (from a stand point of system designers) police use of information technology. Chan ( ) found that police could not use much of the information available to them.

[8] Here I refer to neutrality in its North American rather than European sense. In Europe the idea refers to the assumption that for law and policy, it should not matter which technological means is involved, what matters is the broader value or privacy interest that is threatened.

The Napoleonic inspired civil law code contrasts with the Anglo common law system. For the latter, law appears when the court is presented with a problem. Rather than responding on the basis of broad principles (such as respect for human dignity or personality), in the United States the courts and law often respond on the bases of the particular technology or subject area involved. For example until recently video rental records had greater protection than health records and in general, audio recordings require a warrant, but video recordings do not.

[9] However widespread access to highly invasive technologies that lend themselves to stealth is not necessarily a virtue.

[10] In a related fashion Balzacq (2005) observes that a focus on the linguistic construction of securitization ignores the importance of context and the implications of power.

[11] Even then there are often complicating wrinkles. Consider the fast track for air travelers in which for paying a fee, pre-qualified travelers are whisked through security. While in principle anyone can apply for this, most travelers will choose not to spend the annual fee. Categorical application raises other issues, particularly

when done by the state (e.g., the requirement that there be some grounds for suspicion).

[12] In a related vein Sorokin (1965) overshot the target in writing derisively of "quantoprhenia and numerology". What we need instead is humility and sophistication in the use of numbers.

[13] Consider for example positions on the death penalty based only on a "cost-benefit" analysis which find that it generally costs several times as much to put someone to death as to imprison them for life.

[14] Note the self-deluding body count system of the Viet Nam war. (Gibson 1986, Bell 1979) and in criminal justice (Wachtel 1985).

[15] A different standard would assess harm from the behavior. Thus a person who rapidly speeds up as the light turns is likely much more dangerous, yet would be less likely to be identified as a violator by the technology, because the speeder will be within the grace period.

[16] As the opening chapters suggest that is a silly statement given the multiple dimensions and kinds of privacy considered in chapters 1 and 2 and the dynamic qualities of the issue. The fact that it has been so widely reproduced in the media and so rarely questioned with respect to its factual basis reflects the poverty of much of the public dialogue on the issue.

One statement of the insensitive view, "You have zero privacy anyway –get over it," by the CEO of Sun Microsystems was apparently driven by a concern that if consumers didn't get over it, online growth would be hurt. Instead of uninformed

assertions that run the danger of becoming self-fulfilling, one alternative to lowered consumer expectations is of course enhanced technological protections for identity and gradations in the kind of consumer information that is required for transactions. www.securityfocus.com/news/11377 The former however bootlegs in another fallacy.

[17] In a different context President Reagan's "Star Wars" program was a continuation of the early response to atomic weapons which involved building bomb shelters and bigger bombs. An alternative was to define the problem as calling for understanding of mutual grievances, negotiation and disarmament.

[18] For example a good profile may increase arrests among the less competent but make it easier for skilled offenders knowledgeable about the system to avoid detection. The smaller the camera lens the easier it is to hide, but the more limited the range.

[19] In the area of criminal justice, a police supervisor notes, "tactics developed for use against killers and kidnappers come to be used against junkies and whores." This ties to the earlier discussion of surveillance creep.

[20] As noted in chapter 5 an interesting empirical issue is the link between development of a technology and its diffusion and how its availability and successful promotion may preclude, displace or bolster other solutions, as well as its implications for other goals.

[21] This raises another issue involving carrots and sticks and coercion and manipulation. The end result serving the interests of those in control may be the

same even as the means vary significantly. The velvet glove vs. the iron fist question (fallacy 27) is related. This also connects to the "good people and dirty work" (Hughes 1962).

Orwell, while hardly an advocate of the unaccountable use of either approach appreciated Kipling's poem "Tommy" quoted in the introduction. Orwell wrote that Kipling's "grasp of function, of who protects whom, is very sound. He sees clearly that men can only be highly civilized while other men, inevitably less civilized, are there to guard and feed them." *Critical essays* (1946) on web at http://gaslight.mtroyal.ab.ca/Orwell-B.htm . He of course differed markedly from Kipling in his assessment of colonialism, even as the characters in *Burma Days*, his novel based on is posting their as a police officer reflect Kipling as well.

[22] Laudon (1996) and Rule and Hunter (1996) suggest this as policy. This would be fairer than the current system but limitations would still likely be appropriate with respect to what an individual can sell. An example can be seen in some magazines which give subscribers a free month if they agree to the sharing of their data.

[23] A complicating factor here is co-generated data, whether a picture of a former lover or exchanges with merchants. Should rights in the data be shared –requiring permission from both parties and sharing of any benefits from sale? Or should the parties have independent rights to use as they wish?

[24] Sometimes this is not a fallacy. Thus the libertarian who views drug use as a matter of free choice will hardly be supportive of drug testing.

[25] Given the value component it is likely to be more difficult to reach agreement among those holding diverse views than is the case for the fallacies of logic or the empirical. In calling these fallacies I am speaking not only as a scholar reflecting my understanding of the values of American and western civilization, but also as a citizen reflecting my preferences on issues that can be only partly informed by logic and evidence.

[26] For a clear headed approach to managing, rather than wining, the war on drugs see and MacCoun and Reuter (2001)

[27] This gets at the endemic tensions between authority and society. As Lincoln so well put it government needs to control society, but to be controlled itself.

[28] Consider also the real goal of a company that advertised that it could help persons with bad credit records—the actual goal was to create lists to sell of persons with bad records. The reason some firms request phone numbers when a person pays with a credit card is not to insure the security of the transaction (it is guaranteed), but for marketing purposes. A failed drug test can be grounds for terminating a worker before he or she becomes eligible for a retirement system. Pre-employment medical tests may reveal that a woman is pregnant and prevent her from being hired.

[29] But on the limitations of fingerprints see Cole 2001. In another example, police dogs can be an efficient crowd control device. Yet if you were the police chief in Birmingham, Alabama, (where citizens hold vivid television memories of police dogs attacking civil rights demonstrators) would you use dogs for crowd control? Of

course this could also be questioned on pragmatic grounds. Thus if using dogs generated a backlash and disorders escalated, it would be harder to argue that the tactic "worked" beyond perhaps the immediate moment. The use of dogs and water pressure for crowd control appears to have lessened as a result of the development of rubber bullets and pepper spray. However there use as sniffers has increased. (Marks, 2009)

[30] "Experience should teach us to be most on our guard when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding."

[31] Given a conflict setting and the complexity and difficulty of intervention, social control efforts seem particularly prone to cycles of reform. The recent history of the community corrections movement offers a good example moving from pretrial diversion in the late 1960s, mandatory sentencing in the mid-1970s, and intensive probation supervision in the early 1980s. While corrections and police agencies are particularly prone to such cycles, schools and mental health not far behind. Where nothing works very well, or that much better than anything else, there may be greater receptivity to presumed reforms.

[32] H.L. Mencken's observation that, "for every complex problem, there is a solution that is simple, neat and wrong applies." Yet if applied too universally it illustrates its' own point.

[33] In another example, a Chinese story suggests that to cool the tea pot it is better to add more water than to put out the fire (the latter presumably being a problem when fires were harder to start). Both proportionality and temporality are found here.

[34] For example the East Germans were apparently able to tap most phone calls of West German and NATO officials, but do not appear to have been able to make very effective use of this.

[35] Survey research reflects this inconsistency (Margulis, *et al* 2010*).* There is strong support for protections from the privacy invasions of others, but much less support with respect to what the individual feels entitled to do to others. Attitudes toward Caller-Id reflect this, individuals like to know who is calling them, but often resort to blocking options to stop others from knowing who they are calling.

[36] Disagreements over the point at which issues of quantity shift to those of quality is another source. Note that while the woods may remain the same, hiking has a very different meaning for solitude when alone, as against being in a large group.

[37] Marx 2007, 2001, 1995 analyzes this.

[38] That distinction worked for much of human history. But with the increasing interdependence seen with cyborgs, advanced robots and people hooked up to machines, the lines are less clear now. As Deleuze (1995) and Haggerty and Ericson (2000) suggest, this interdependence and mélange of people and technology can be seen to involve a surveillant assemblage. This requires a different level analysis.

[39] Being criticized by those with opposed viewpoints can be one indicator of speaking unpleasant truths. Such critics often fail to appreciate the substantive and strategic contribution that objective analysis can bring and to reflect on the basis of their own strongly held views. Our National Research Council (2007) report on privacy was attacked by several activist colleagues because, "it had too many academics on board" and "there was too much waffling".