Hey Buddy can you spare a DNA? New surveillance technologies and the growth of mandatory volunteerism in collecting personal information

Gary T. Marx
Professor Emeritus, Massachusetts Institute of Technology, Cambridge, MA, USA

Summary. The new social surveillance can be defined as scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts. Examples include: video cameras; computer matching, profiling and data mining; work, computer and electronic location monitoring; biometrics; DNA analysis; drug tests; brain scans for lie detection; various forms of imaging to reveal what is behind walls and enclosures. There are two problems with the new surveillance technologies. One is that they don't work and the other is that they work too well. If the first, they fail to prevent disasters, bring miscarriages of justice, and waste resources. If the second, they can further inequality and invidious social categorization; they chill liberty. These twin threats are part of the enduring paradox of democratic government that must be strong enough to maintain reasonable order, but not so strong as to become undemocratic.

Key words: soft surveillance, DNA, privacy, new technologies.

Riassunto *(Ehi amico, ti avanza del DNA? Le nuove tecnologie di sorveglianza e il crescere della partecipazione spontanea alla raccolta forzata di informazioni personali)*. Le nuove forme di sorveglianza sociale possono essere definite come forme di controllo attraverso l'uso di mezzi tecnici per estrarre o creare o raggruppare dati personali o di contesto. Videoregistrazioni, tecniche informatiche di *data mining* e di *profiling*, telelavoro, sistemi di localizzazione elettronici, biometria, analisi del DNA, test per la rilevazione dell'uso di droghe, tecniche di *brain imaging* usate come macchina della verità, varie forme di rilevazioni delle immagini al di là di muri e barriere, sono tutti possibili esempi di queste tecniche. Ci sono due problemi con le nuove tecniche di sorveglianza. Un problema è che esse possono non funzionare, l'altro è che possono funzionare troppo bene. Nel primo caso queste tecniche non riescono a prevenire disastri, portano ad errori giudiziari e a uno spreco di risorse. Nel secondo caso possono aumentare ineguaglianze e forme di malevola categorizzazione sociale, sospendere i diritti di libertà. Questa doppia minaccia fa parte del costante paradosso dei governi democratici che devono essere abbastanza forti per mantenere un ordine ragionevole ma non così forti da diventare non democratici.

Parole chiave: sorveglianza, DNA, privacy, nuove tecnologie.

INTRODUCTION

The new social surveillance can be defined as scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts. Examples include: video cameras; computer matching, profiling and data mining; work, computer and electronic location monitoring; biometrics; DNA analysis; drug tests; brain scans for lie detection; various forms of imaging to reveal what is behind walls and enclosures. The use of "technical means" to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Much new surveillance involves an automated process and extends the senses and cognitive abilities through using material artefacts or software. Traditional surveillance often implied a non-cooperative relationship and a clear distinction between the object of surveillance and the person carrying it out. In an age of servants listening behind closed doors, binoculars and telegraph interceptions, that separation made sense. It was easy to distinguish the watcher from the person watched. Yet for the new surveillance with its expanded forms of self-surveillance and cooperative

Indirizzo per la corrispondenza (Address for correspondence): Gary T. Marx, Professor Emeritus, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, USA. E-mail: gtmarx@garymarx.net.

surveillance, the easy distinction between agent and subject of surveillance can be blurred.

THE TRURO CASE

In Truro, Mass. at the end of 2004, police politely asked all male residents to provide a DNA sample to match with DNA material found at the scene of an unsolved murder. Residents were approached in a non-threatening manner and asked to help solve the crime. This tactic of rounding up all the usual suspects (and then some) is still rare in the United States for historical, legal, and logistical reasons, but it is becoming more common. In a criminal justice context the dragnet method illustrates some classic issues such as the tension between a standard of reasonable suspicion or probable cause and the need to solve high profile crimes, between a presumption of innocence and of guilt, and whether the government can be trusted when it promises to destroy the DNA collected, rather than to save it in a database. There is also the pragmatic question of whether or not it works and under what conditions and to what degree and for what purposes. For example for varied outcomes such as the identification and location of the guilty for a given crime and for an unrelated crime, false positives and negatives, and finding nothing at all, it would be useful to contrast situations involving acquiescence to, or rejection of, voluntary requests, unsolicited volunteers, information provided as a result of a warrant, and situations in which individuals provide information under the mistaken belief that they have no choice.

The Truro case illustrates expanding trends in surveillance and social control. There is increased reliance on "soft" means for collecting personal information. In criminal justice contexts these means involve some or all of the following: persuasion to gain voluntary compliance, universality or at least increased inclusiveness, and emphasis on the needs of the community relative to the rights of the individual. As with other new forms of surveillance and detection, the process of gathering the DNA information is quick and painless, involving a mouth swab, and is generally not felt to be invasive. This makes such requests seem harmless relative to the experience of having blood drawn, having an observer watch while a urine drug sample is produced, or being patted down or undergoing a more probing physical search. In contrast, more traditional police methods such as an arrest, a custodial interrogation, a search, a subpoena or traffic stop are "hard." They involve coercion and threat to gain involuntary compliance. They may also involve a crossing of intimate personal borders, as with a strip or body cavity search. In principle such means are restricted by law and policy to persons there are reasons to suspect, thus implicitly recognizing the liberty of the individual relative to the needs of the community.

Yet the culture of social control is changing. While hard forms of control are hardly receding, the soft forms are expanding in a variety of ways. I note several forms of this – requesting volunteers based on appeals to good citizenship or patriotism, using disingenuous communication, profiling based on life style and consumption, and utilizing hidden or low visibility information collection techniques.

The theme of volunteering as good citizenship or patriotism can increasingly be seen in other contexts. Consider a Justice Department "Watch Your Car" program found in many states. Decals which car owners place on their vehicles serve as an invitation to police anywhere in the United States to stop the car if driven late at night.

A related form of volunteerism involves using citizens as adjuncts to law enforcement by watching others. Beyond the traditional Neighborhood Watch, we can note new post-9/11 programs, such as a police sponsored CAT EYES (Community Anti-Terrorism Training Initiative) and efforts to encourage truckers, utility workers, taxi drivers, and delivery persons to report suspicious activity.

There also appears to be an increase in Federal prosecutors asking corporations under investigation to waive their attorney/client privilege. This can provide information that is not otherwise available at a cost of indicting only lower level personnel. Plea bargaining shares a similar logic of coercive "volunteering", often hidden under a judicially sanctified and sanitized veneer of disguised coercion.

Another "soft" method involves disingenuous communication that seeks to create the impression that one is volunteering when that isn't the case. Consider:

- the ubiquitous building signs, "In entering here you have agreed to be searched";
- a message from the Social Security Administration to potential recipients: "While it is voluntary for you to furnish this information, we may not be able to pay benefits to your spouse unless you give us the information";
- a Canadian airport announcement: "Notice: Security measures are being taken to observe and inspect persons. No passengers are obliged to submit to a search of persons or goods if they choose not to board our aircraft."

A related form of soft surveillance involves corporations more than government. Note the implicit bargain with respect to technologies of consumption in which the collection of personally identifiable (and often subsequently marketed) information is built into the very activity. We gladly, if often barely consciously, give up this information in return for the ease of buying and communicating and the seductions of frequent flyer and other reward programs. Information collection is unseen and automated (in a favored engineering goal, "the human is out of the loop"), generating the appearance of actions that are neutral and objective and ignoring the choices inherent in the design of the system. Data gathering is "naturally" folded into routine activities such as driving a car, watching television, or using a credit card, computer, or telephone.

Consider also those who agree to report their consumption behavior and attitudes in more detail as part of market research. A new variant goes beyond the traditional paid "volunteers" of the Nielsen ratings and other consumer research. Volunteers are given free samples and talking points. They seek to create "buzz" about new products without revealing their connection to the sponsoring business. Procter and Gamble for example has 240 000 volunteers in its teenage product propaganda/diffusion network. While many call, few are chosen (10-15%) for this highly coveted role [1]. These volunteer intelligence and marketing agents report on their own and others' responses to products, take surveys, and participate in focus groups. What is at stake here isn't merely improved advertising in intensely competitive industries but also a new and morally ambiguous form of tattling. Regardless of whether they are compensated, the providers of information to marketing research, are also volunteering information on those sharing their characteristics and experiences. Volunteer has two meanings here – first agreeing to act without external compulsion – a kind of free will or better, within cultural and resource limits, an independent willfulness with respect to action taken. This is often, but need not be, linked to a second meaning of acting without receiving material compensation. People who participate because they are paid of course may voluntarily agree to this, but their behavior is not voluntary in the way that those who participate without direct reward is. The volunteer marketers appear to "profit" from seeing themselves as insiders and as members of an elite consumer group being the first to know.

However no permission and no direct benefits flow to the mass of persons the sponsoring agency learns about. There are parallels to DNA analysis here: an individual who voluntarily offers his or her information also simultaneously offers information on family members who have not agreed to this. We lack an adequate conceptual, ethical, and legal framework for considering this spill over effect from voluntary to involuntary disclosure involving third parties.

We can also note changes in a related cultural area, involving the willing, even gleeful public exposure of private information – whether in dress styles, cell phone conversations, or the mass media. Many Americans are drawn to new communications technologies like nails to a magnet, unable to resist the prurient call to watch others, but also with a near Dostoyevskian compulsion to offer information about themselves. There can also be psychological gratifications from revelation for both the revealer and the recipient of the information.

The prying and often inane TV talk and reality shows, web cam pages, web blogs, the goofy waving of fans at televised events, and video taping of conceptions, births, and last wills and testaments suggest the extent to which we have become both a performance and a spectator society, literally from the beginning of life to the end.

SEARCHING MADE EASY

The new surveillance is more comprehensive, intensive and extensive. The ratio of what the individual knows about him or herself relative to what the surveilling organization knows is lower than in the past, even if objectively much more is known. Many forms of voluntarism are encouraged by techniques designed to be less directly invasive. Computers scan dispersed personal records for suspicious cases avoiding, at least initially, any direct review by a human. Similarly X-ray and scent machines "search" persons and goods for contraband without touching them. Inkless fingerprints can be taken without the stained thumb symbolic of the arrested person. Classified government programs are said to permit the remote reading of computers and their transmissions without the need to directly install a bugging device.

Beyond the ease of gathering DNA, consider the change from a urine drug test requiring an observer, to those that require a strand of hair, sweat, or saliva. Saliva is particularly interesting. Whatever can be revealed from the analysis of blood or urine is also potentially found (although in smaller quantities) in saliva, not only evidence of disease and DNA, but also of drugs taken and pregnancy. The recent development of non-electrical sensors now make it possible to detect molecules at minute levels in saliva. It is likely to offer a wonderful illustration of the creeping (or better galloping) nature of personal data collection that technical developments increasingly make possible. This involves both the displacement of traditional invasive means and the expansion to new areas and users. To take blood, the body's protective armor must be pierced. But expectorating occurs easily and frequently and is more "natural" than puncturing a vein. Nor does it involve the unwanted observation required for a urine drug sample. Saliva samples can be almost endlessly taken, and in charting changes make possible the early identification of problems. This may offer medical diagnostic advantages to individuals who can maintain control over the content of their spit. Yet employers concerned with rising health costs and resistance to urine drug tests – and eager to avoid liability for the illnesses of those who work around hazardous chemicals – would also have a strong interest in diagnostic spitting as a condition of employment. Invasive is a term easily thrown about in such discussions. Yet a variety of meanings can be unpacked. It can involve procedures in referring to degree of literal invasiveness via crossing a physical border of the person, here entries into natural body orifices such as ears contrast with breaking the skin to extract a bullet. It can refer to directionality, implanting in the body may have different connotations than extracting from it. It may refer to the nature of what is discovered (information on being left or right handed vs religious and political beliefs the definition may depend on the kind of relationship between the parties (*e.g.*, familial *vs* formal organizational). The *place* a search occurs, apart from what is searched or found

can also be a factor. The above factors are empirical and in a sense objective. Invasiveness can also be considered with respect to definitions involving perception and feelings, beyond anything observable in a behavioral sense. 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 input from others.

Authorities concerned with identifying those who spit when not requested to, can also use the technology. The transit authority in Sheffield, England, as part of an anti-spitting campaign distributed 3000 DNA swab kits to transportation staff. Posters proclaim "Spit It's Out" and warn persons who spit that "…you can be traced and prosecuted. Even if we don't know what you look like. And your record will be on the national DNA data base. Forever". For those of another era, this is reminiscent of the grammar school teachers who threatened to add notes about misbehavior to "your permanent record".

The automated analysis of urine offers many of the advantages of saliva. A diagnostic test routinely used in some Japanese employment contexts requires that each time an employee enters the stall they be identified through their access card. This permits a comprehensive record of their flushed offerings over time. It is said to be of great benefit in the early diagnosis of health problems, it can also determine drug use, recent sexual activity and pregnancy.

In many of these cases citizens are at least informed of what is going on, even if the meaning of their consent is open to question. More troubling is the development of tactics that need not rely on the subject consenting or even being informed. New hidden or low visibility technologies increasingly offer the tempting possibility of by-passing awareness, and thus any need for direct consent, altogether. Consider technologies that overcome traditional barriers such as darkness or walls. Night vision technology illuminates what darkness traditionally protected (and the technology is itself protected unlike an illuminated spotlight). Thermal imaging technology applied from outside can offer a rough picture of a building's interior based on heat patterns, without the necessity of entering.

A person's DNA can be collected from a drinking glass or from discarded dental floss. Facial scanning technology only requires a tiny lens. Smart machines can "smell" contraband with no need for a warrant or asking subjects if it is permissible to invade their olfactory space or "see" through their clothes and luggage. Beyond the traditional reading of visual clues offered by facial expression, there are claims that the covert analysis of heat patterns around the eyes and of tremors in the voice, and the measurement of brain wave patterns, offer windows into feelings and truth telling. Reading brain wave patterns requires attaching sensors to the head and thus an informed subject. But should the remote reading of brain waves become possible and workable, science fiction would once again become science and another technological weakness that protected liberty would disappear.

The face still remains a tool for protecting inner feelings and thoughts, but for how long?

Individuals need not be informed that their communications devices, vehicles, wallet cards, and consumer items increasingly will have RFID (Radio Frequency Identification) chips embedded in them that can be designed to be passively read from up to 30 feet away by unseen sensors. The technology can require that the chip make physical contact with the sensor (*e.g.*, requiring the card to touch it) or chip can be read remotely. This nicely illustrates how technical design can have social causes and consequences.

When the chip must contact the reader the subject is of necessity aware, otherwise covert reading is possible by both the "official" reader and by an uninvited thief-lurker, although with current technology this is limited to about 30 feet. The greater the distance from the chip, the more power the reader needs and at some point this is great enough to fry the chip in the process of trying to read it. A rarely noted consequence of location technologies is their ability to identify social networks and patterns (*e.g.*, other co-present individuals whose chips are also read and an analysis of the timing of passages).

In the convoluted logic of those who justify covert (or non-informed) data collection and use, individuals "volunteer" their data by walking or driving on public streets or entering a shopping mall, by failing to hide their faces or wear gloves or encrypt their communications, or by choosing to use a phone, computer, or a credit card. The statement of a direct marketer nicely illustrates this: "Never ever underestimate the willingness of the American public to tell you about itself. That data belongs to us! ...it isn't out there because we stole it. Someone gave it away and now it's out there for us to use."

"IF YOU HANG THEM ALL, YOU WILL CERTAINLY GET THE GUILTY"

In an environment of intense concern about crime and terrorism and a legal framework generated in a far simpler time, the developments discussed above are hardly surprising. Democratic governments need to be reasonably effective and to maintain their legitimacy (even as research on the complex relationships between effectiveness and legitimacy is needed). Working together and sacrificing a bit of oneself for the common good, particularly in times of crisis, is hardly controversial. Relative to traditional authoritarian settings, many of the above examples show respect for the person in offering notice and some degree of choice and in minimizing invasiveness. Such efforts draw on the higher civic traditions of democratic participation, self-help, and community. They may also deter. Yet there is also something troubling about them.

The accompanying rhetoric is often dishonest and even insulting to one's intelligence. Consider a phone company executive who, in defense of unblockable Caller-Id, said, "When you choose to make a phone call you are choosing to release your telephone number." In the same World Cup League of Disingenuity is the statement of a personnel manager in a one-industry town, "We don't require anyone to take a drug test, only those who choose to work here."

To be meaningful, choice should imply genuine alternatives and refusal costs that are not wildly exorbitant. Absent that, we have trickery, double-talk, and the frequently spoiled fruit of inequitable relationships. When we are told that for the good of the community we must voluntarily submit to searches or provide information, there is a danger of the tyranny of the communal and of turning presumptions of innocence upside down. If only the guilty need worry, why bother with a Bill of Rights and other limits on authority? There also comes a point beyond which social pressure seems unreasonable. If the case for categorical information is strong, then the law ought to require it without need of the verbal jujitsu of asking for volunteers or arguing that subjects are in fact taking voluntary action in the full meaning of the term, when they aren't. There also needs to be limitations on secondary use. DNA collected for law enforcement purposes is interesting in that regard. It was initially claimed that the DNA collected could only be used for identification purposes. Subsequent technical developments then made it possible to read much more of the DNA from the small sample taken, offering a broad window into the individual's genetic makeup, a factor far transcending simple identification.

Those who fail to volunteer can be viewed as having something to hide, or as being bad citizens and uncooperative team players. The positive reasons for rejecting such requests are ignored. Yet we all have things to hide, or more properly to reveal only selectively, depending on the relationship and context. The general social value we place on sealed first class letters, window blinds, and bathroom doors, and our opposition to indiscriminant wiretapping, bugging, and informing, or to giving up anonymity in public places (absent cause), are hardly driven by an interest in aiding the guilty. Sealing juvenile criminal records does not reflect a perverse strategy for infiltrating miscreants into adult life, but rather an understanding of, and some compassion for, the mistakes of youth.

We value privacy not to protect wrongdoing, but because an appropriate degree of control over personal and social information is central to our sense of self, autonomy, and material well being – as well as being necessary for independent group actions. A healthy, if necessarily qualified, suspicion of authority is also a factor in restricting information sought by the more powerful. As consumers and citizens we have an interest in avoiding the manipulation, discrimination, and theft that can flow from combining bits of personal information that are innocuous when standing alone.

Many of the new controls may seem more acceptable (or at least are less likely to be challenged) because they are hidden or built-in and less invasive relative to the traditional forms of crossing personal and physical borders. We are also often complicit in their application, whether out of fear, convenience, or for frequent shopper awards.

Converting privacy to a commodity in which the seller receives something in return to compensate for the invasion is a clever and defensible means of overcoming resistance.

Exchanges and less invasive searches are certainly preferable to data rip-offs and more invasive searches. However the nature of the means should not be determinative.

What matters most is the appropriateness of collecting the information and only secondarily the way that it is collected. A search is still a search regardless of how it is carried out. The issue of searches and the crossing of traditional borders between the civil and state sectors, or the self and others, involves much more than painless, quick, inexpensive (or positively rewarding), and non-embarrassing means. Here I imply the ideal situation in which individuals fully understand not only what they will be receiving, but what they are giving away, how it will be used and protected, potential risks and what secondary uses there might be. In suggesting that less invasive means of searching are preferable, we need to be mindful that these come with the threat of vastly expanding the pool of those who are searched (and of course as the Texas judge reportedly said, "if you hang them all, you will certainly get the guilty"). Expanded nets and thinned meshes are a function of perceived threats and degrees of risk, as well as ease of application. The seemingly ever greater ease and efficiency offered by technological means are on a collision course with traditional liberty protecting ideas of reasonable suspicion and minimization and impracticality. Certainly other factors being equal, soft ways are to be preferred to hard, even if the control/instrumental goals of those applying the surveillance remain the same. Yet coercion at least has the virtue (if that's what it is) of letting the subject (or object) know what is happening. What we don't know can hurt us as well.

DIALOGUE AND EDUCATION

Traditionally (if accidentally) there was a happy overlap between three factors that limited searches and protected personal information. The first was logistical. It was not cost-or time-effective to search everyone. The second was law. More invasive searches were prohibited or inadmissible, absent cause and a warrant. The third reflected the effrontery experienced in our culture when certain personal borders were involuntarily crossed (*e.g.*, strip and body cav-

ity searches and taking body fluids, and to a lesser degree, even fingerprints. Limited resources, the unpleasantness of invasive searchers (for both the searched and the searcher) and the ethos of a democratic society historically restricted searches.

These supports are being undermined by the mass media's encouragement of fear and perceptions of crises [2, 3] and by the seductiveness of consumption, together with the development of inexpensive, less invasive broad searching tools. Under these conditions one does not need a meteorologist to describe wind patterns.

The willingness to offer personal information and the fascination with the private aspects of other's lives partly ties to the 1960s legacy of openness and transparency as it encounters the new technological possibilities. But it also speaks to some need of the modern person (and perhaps in particular the American) to see and be seen and to know and be known about through the ubiquitous camera and related means.

Volunteering one's data and being digitally recorded and tracked is coming to be taken for granted as a means of asserting selfhood. This willful blurring of some of the lines between the public and private self and the ready availability of technologies to transmit and receive personal data give new meaning to David Riesman's concern with "other direction" [4].

Of course our sense of self and social participation have always depended on validation from others – on seeing ourselves in, and through, their eyes. But contemporary forms of validation induce a sense of pseudo-authenticity, an unbecoming narcissism, and a suspicious spy culture. The social functions of reticence and embarrassment, and the role of withheld personal information as a currency of trust, friendship and intimacy, are greatly weakened.

The abundance of new opportunities for self-expression offered by contemporary technologies must be considered alongside the lessened control we have of information in distant computer systems. Data shadows or ghosts based on tangents of personal information (stripped of context) increasingly effect our life chances. The subject often has little knowledge of the existence or consequences of these data bases and of how they are constructed or might be challenged.

This complicated issue of reducing the richness of personal and social contexts to a limited number of variables is at the core of science's ability to predict; it is central to current ideas about economic competitiveness. The data analyst goes from known empirical cases to equivalent cases that are not directly known. Because a given case can be classified relative to a statistical model as involving a high or low risk, it is presumed to be understood and thus controllable (at least on a statistical or "probabilistic" bases). This may work fine for business or medical decisions, but civil liberties and civil rights are not based on statistical categories. They are presumed to be universally applicable absent cause to deny them. So rationality and efficiency increasingly clash with many of our basic enlightenment ideas of individualism and dignity – ideas that were better articulated and less contestable, in technologically simpler times.

There is a chilling and endless regress quality in our drift into a society where you have to provide ever more personal information in order to prove that you are the kind of person who does not merit even more intensive scrutiny. Here we confront the insatiable information appetite generated by scientific knowledge in a risk-adverse society. In such a society knowing more may only serve to increase doubt and the need for more information.

My concern is more with cultural and behavioral developments than with the law. Certainly we do not lack for contemporary examples of constricted or trampled legal rights (*e.g.*, American citizens held at Guantanamo without trial or the unwelcome elements of the Patriot Act). Still, the growing institutionalization of civil rights and civil liberties over the last century (involving race, gender, children, work, freedom of expression and association, searches, and life styles) is unlikely to be reversed. Jagged cycles rather than clean linearity will continue to characterize this turbulent history. Wartime restrictions (whether Lincoln's suspending of *habeas corpus* or limits on speech during the Second World War) have been lifted as calmer times returned. To be sure the evidence of ebbs is undeniable, but even in the shadow of 9/11 there are some flows as well, particularly at the state and local level.

The cultural changes are worrisome because they are diffuse, subtle, and unseen – and they often reflect choices that, even if specious or manipulated, are difficult to challenge in a democratic society. The possibility of wrongful choice is an inherent risk of democracy. One's liberty can be used to smoke, eat rich foods, drive environmentally unfriendly cars, and watch unreality television, as well as to volunteer personal information – whether to government or the commercial sector. A bad law can be challenged in court or repealed. A dangerous technology can be banned, regulated, or countered with a different technology. But the only way to respond to liberty threatening choices of the kind discussed here is through dialogue and education (tools that are already disproportionately available to those supporting the current developments).

LIBERTY AND ORDER

Two broad opposed views of the new surveillance can be identified. One optimistically places great faith in the power of technology and welcomes ever more powerful surveillance as necessary in today's world where efficiency is so valued and where there are a multiplicity of dangers and risks. More pessimistic is the Frankensteinian/Luddite view that surveillance technology is inhuman, destructive of

liberty and untrustworthy. Clearly surveillance is a sword with multiple edges. The area is fascinating precisely because there are no easy scientific or moral answers.

There are value conflicts and ironic conflicting needs and consequences which make it difficult to take a broad and consistent position in favor of, or against, expanding or restricting surveillance. For example we value both the individual and the community.

We want both liberty and order. We seek privacy and often anonymity, but we also know that secrecy can hide dastardly deeds and that visibility can bring accountability. But too much visibility may inhibit experimentation, creativity and risk taking. In our media-saturated society we want to be seen and to see, yet also to be left alone. We value freedom of expression and a free press but do not wish to see individuals defamed or harassed. We desire honesty in communication and also civility and diplomacy. We value the right to know, but also the right to control personal information. The broad universalistic treatment citizens expect may conflict with the efficiency driven specific treatment made possible by fine-honed personal surveillance

Whatever action is taken there are likely costs, gains and trade-offs. At best we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point for decision making.

Contrary to the familiar Orwellian concerns about the all knowing eyes and ears of government, recent history suggests to some observers the reverse problem; blindness, deafness, and inefficiency (*e.g.*, the 9/11 danger known only in retrospect, the failure of various airline passenger screening programs, wrongful convictions and so on). In one sense, there are two problems with the new surveillance technologies. One is that they don't work and the other is that they work too well. If the first, they fail to prevent disasters, bring miscarriages of justice, and waste resources. If the second, they can further inequality and invidious social categorization; they chill liberty. These twin threats are part of the enduring paradox of democratic government that must be strong enough to maintain reasonable order, but not so strong as to become undemocratic.

The surveillance developments noted here are consistent with the strengthening of the neo-liberal ethos of the last decade. The idea of voluntary compliance valorizes increased individual choices, costs, and risks. It simultaneously weakens many social protections and pays less attention to the ways the social order produces bad choices and collective problems. The consequences of these are then left to individual and private solutions. This generates a suspicious society in which paranoia is entangled with reality.

There is no single answer to how the new personal information collection techniques ought to be viewed and what, if anything, should (or can) be done about them. From genuine to mandatory voluntarism and from open to secret data collection – these are points on continuums. There are important moral differences between what can be known through the unaided senses and what can only be known through technologically enhanced senses. The moral and practical issues around the initial collection of information are distinct from its subsequent uses and protections.

Diverse settings – national security, domestic law enforcement, public order maintenance, health and welfare, commerce, banking, insurance, public and private spaces and roles – do not allow for the rigid application of the same policies. The different roles of employer – employee, merchant-consumer, landlord-renter, police-suspect, and health provider – patient involve legitimate conflicts of interests. Any social practice is likely to involve conflict of values.

We need a situational or contextual perspective that acknowledges the richness of different contexts, as well as the multiplicity of conflicting values within and across them. In the face of the simplistic rhetoric of polarized ideologues in dangerous times, we need attention to trade offs and to the appropriate weighing of conflicting values. Given changing historical circumstances, there is no fixed golden balance point. However the procedures for accountability and oversight so central to the founding and endurance of the country must remain strong. Contemporary moral-panic efforts to erode these need to be strenuously resisted. It would be foolish to elevate consent to an absolute, but neither should we continue to slide into a world where meaningful consent is only of historical interest. At best we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point for decision making.

Appreciating complexity is surely a virtue, but being immobilized by it is not. The default position should be meaningful consent, absent strong grounds for avoiding it.

Consent involves participants who are fully appraised of the surveillance system's presence and potential risks, and of the conditions under which it operates. Consent obtained through deception or unreasonable or exploitative seduction or to avoid dire consequences is hardly consent. The smile that accompanies the statement, "an offer you can't refuse" reflects that understanding. A principle of truth in volunteering is needed: it is far better to say clearly that "as a condition of [entering here, working here, receiving this benefit, etc.] we require that you provide personal information". A golden rule principle ought also to apply: Would the information collector be comfortable in being the subject, rather than the agent of surveillance, if the situation were reversed? These are among 20 broad questions and related principles that I suggest be asked in any assessment of personal information collection [5].

Our culture needs to overcome the polite tendency to acquiesce when we are inappropriately asked for personal information. We need to just say "no";

when, after paying with a credit card, a cashier asks for a phone number, or when a web page or warranty form asks for irrelevant personal information, or a video store seeks a social security number. Offering disinformation may sometimes be appropriate. The junk mail I receive for Groucho and Karl offers a laugh, and a means of tracking the erroneous information I sometimes provide.

Finally, technology needs to be seen as an opportunity, rather than only as a problem. Technologies can be designed to protect personal information and notify individuals when their information is collected or has been compromised. Thus electronic silencers can inhibit third parties from overhearing cell phone and face-to face-conversations and computer privacy screens can block sneaky peeks by anyone not directly in front of the screen. E-Z Pass toll collection systems can be programmed to deduct payment, while protecting the anonymity of the driver. RFID technology can build in notification by requiring that the chip make physical contact with the sensor (*e.g.*, touching the card or item to the sensor), rather than permitting it to be read covertly at a distance. Cell phones cameras could be designed to emit a tell tale sound before a picture is taken, (this is required in Japan).

Sinclair Lewis hoped in 1935 that *It Can't Happen Here* [6]. But of course it can and in some ways it has. Twenty years ago in reflections on the year and book 1984, I wrote in these pages [7]*, the first task of a society that would have liberty and privacy is to guard against the misuse of physical coercion by the state and private parties. The second task is to guard against the softer forms of secret and manipulative control. Because these are often subtle, indirect, invisible, diffuse, deceptive, and shrouded in benign justifications, this is clearly the more difficult task*.

Two decades later the hot button cultural themes of threat, civil order, and security that Lewis emphasized are in greater ascendance and have been joined by the siren calls of consumption. If our traditional notions of liberty disappear, it will not be because of a sudden *coup d'etat*. Nor will the iron technologies of industrialization be the central means. Rather it will occur by accretion and with an appeal to traditional American values in a Teflon and sugar-coated technological context of low visibility, fear, and convenience.

Submitted on invitation.
Accepted on 4 October 2006.

References

1. Walker R. The corporate manufacture of word of mouth. *The New York Times Magazine* Dec. 5, 2004.
2. Altheide D. *Creating fear: news and the construction of crisis*. New York: Aldine de Gruyter; 2002.
3. Glassner B. *The culture of fear*. New York: Basic Books; 2000.
4. Riesman D, Glazer N, Denney R. *The lonely crowd*. New Haven: Yale University Press; 2001.
5. Marx G. Seeing hazily (but not darkly) through the lens: some recent empirical studies of surveillance technologies. *Law and Social Inquiry*. 2005;30:339-99.
6. Lewis S. *It can't happen here*. New York: Signet Classics; 1995.
7. Marx G. *Undercover: police surveillance in America*. Berkeley: University of California Press; 1988. p.76.