Fast Capitalism
Volume 2 • Issue 1 • 2006

ISSN 1930-014X
doi:10.32855/fcapital.200601.004

Soft Surveillance: A Growth of Mandatory Volunteerism in Collecting Personal Information — "Hey Buddy Can You Spare a DNA?"

G.T. Marx

"Never underestimate the willingness of the American public to tell you about itself."
—Direct Marketing Executive

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 nonthreatening manner (even as their license plate numbers were recorded) 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. The Truro case illustrates expanding trends in surveillance and social control [1].

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 in the dragnet they cast, 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 in seeking involuntary compliance. They may also involve a crossing of intimate personal borders, as with a strip or body cavity search done by another. In principle such means are exclusive in being 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 and practice 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; the trading of personal information for rewards and convenience; 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. Taxicabs in some cities beyond transmitting video images, also invite police to stop and search them without cause—presumably such searches extend to passengers as well who see the notice and choose to enter the cab.

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, if 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 form involves disingenuous communication that seeks to create the impression that one is volunteering when that really isn't the case.

- 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."

The New York subway system has supplemented the random searches of officers with automated searching by sensing machines. Potential riders need not submit, but then they may not use the subway.

Private Sector Parallels

The soft surveillance trend involves corporations more than government. Note the implicit bargain seen 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")[2]. It is "naturally" folded into routine activities such as driving a car or using a credit card, computer or telephone. Such information is then used in profiling, social sorting and risk assessment (Lyons 2002).

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. (Walker 2004). 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 intensively competitive industries but a new morally ambiguous form of tattling. Regardless of whether they are materially or status compensated, the providers of information to marketing research, are also volunteering information on those who share their characteristics and experiences [3]. 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 for analysis, also simultaneously offers information on family members who have not agreed to this [4]. We lack an adequate conceptual, ethical and legal framework for considering this spillover effect from voluntary to involuntary disclosure involving third parties.

Beyond differences between those who volunteer only on themselves or on themselves and others, we see those who only offer information on others. Another prominent form of volunteerism involves citizens watching each other as adjuncts to law enforcement. Beyond the traditional Neighborhood Watch programs, we can note new post9/11 forms such as a police sponsored C.A.T. EYES (Community Anti-Terrorism Training Initiative) [5]. Additionally, other programs encouraging truckers, utility workers, taxi drivers and delivery persons report suspicious activity.

It is easier to agree to the offering of personal information when the data collection process is automatic and hassle-free. Let us further consider the role of technology in potentially bypassing the need even to ask for consent or to offer rewards.

If You Don't Have to Undress Are You Still Naked? Searching Made Easy

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 drug tests 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. This may also be the case for human odor. The recent development of nonelectrical sensors now make it possible to detect molecules at minute levels in saliva (New York Times, April 19, 2005).

Saliva testing is likely to offer a wonderful illustration of the creeping (or better galloping) expansion of personal data collection increasingly made possible by new (or less) non-invasive means [6]. Surveillance creep (Marx 2005) 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 easily and endlessly taken, and the changes charted 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, resistance to urine drug tests and avoiding liability for the illnesses of those who work around hazardous chemicals [7] would also have a strong interest in diagnostic spitting as a condition of employment. Public decorum authorities concerned with identifying those who spit when not requested to can also use the technology [8].

In many of these cases citizens are at least informed of what is going on, even if the meaning of their consent is often open to question. More troubling is the development of tactics that need not rely on the subject consenting, or even being informed, let alone receiving carrots or avoiding sticks in agreeing to cooperate. New hidden or low visibility technologies increasingly offer the tempting possibility of bypassing awareness, and thus any need for direct consent or other oversight, altogether.

New technologies 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. There is no need for an observer to enter the space. NSA's satellites engage in warrantless remote monitoring of electronic communication to, or from the United States.

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 eliminating the need for a warrant or asking the sniffed for permission to invade their olfactory space or "see" through their clothes and luggage. Research is also being done with the goal of using human odor to identify specific persons, illness (both mental and physical) and even early pregnancy [9].

A vacuum like device is also available that can draw the breath away from a person suspected of drunk driving without the need to ask permission.

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 measuring brain wave patterns offer windows into feelings and truth telling [10].

The face still remains a tool for protecting inner feelings and thoughts, but for how long? Different issues are raised by recent improvements in the technology of face transplanting.

Individuals need not be informed that their communication devices, vehicles, wallet cards and consumer items increasingly will have RFID (Radio Frequency Identification) chips embedded in them. These can be designed to be passively read from up to 30 feet away by unseen sensors [11].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, entering a shopping mall and by failing to hide their faces, wear gloves and encrypt their communication, 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 from them. Someone gave it away and now it's out there for us to use."

Yes, But…

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 [12]. Such efforts draw on the higher civic traditions of democratic participation, self-help, and community. They may also deter. Yet there is 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 a 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, 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 [13].

If the case for categorical information is strong, then the rules ought to require it [14]. without need of the verbal jujitsu of asking for volunteers, or implying that the subject is in fact taking voluntary action in the full meaning of the term, when failure to comply has serious consequences, such as being denied a job, a benefit or appearing suspect in other's eyes.

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 legitimately hide, or more properly to selectively reveal, 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 in giving up anonymity in public places (absent cause) are hardly driven by an interest to aid the guilty. Sealing juvenile criminal records does not reflect a perverse strategy for infiltrating miscreants into adult life, but rather 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, inappropriate social sorting and theft that can flow from combining bits of personal information which are innocuous by themselves.

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, less invasive relative to the traditional forms of crossing personal and physical borders. We are 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 more defensible means of overcoming resistance.

Exchanges and less invasive searches are certainly preferable to data rip-offs and more invasive searches [15].

However, the nature of the means should not be determinative. The appropriateness of collecting the information is also important. 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 and non-embarrassing means, or of "volunteering" to avoid suspicion or opportunity denial.

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 and the possibility of offering resistance. What we don't know can hurt us as well.

One of the most troubling aspects of recent changes is that they so often occur beneath the radar of public

awareness and input. Consider technological designs thrust upon us by industrial fiat such as Caller-ID (initially offered with no blocking options).

Unhappy Underlaps

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 cavity searches and taking body fluids, and to a lesser degree, even fingerprinting) [16].

Limited resources, the unpleasantness of invasive searches (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, the seductiveness of consumption [17].

Also, the concurrent development of inexpensive, less invasive tools for broad searching. 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 is a partial legacy of the 1960s openness and transparency as it encounters the possibilities offered by the last decade's technologies. But it also speaks to some need of the modern person (and perhaps in particular the American) to see and to be seen and to know and to be known about through the ubiquitous camera and related means.

Here we see changes in a cultural strand 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 on themselves.

There can be psychological gratifications from revelation for both the voluntary revealer and the recipient of the information. This mutuality makes the topic interesting and complicated and works against a reductionist argument that knowledge always reflects the interests of those with the technology to discover.

With some revelation we see the truth in Janice Joplin's assertion that, "freedom's just another word for nothing left to lose." Voluntarily offered secret information may lose its value in the sunshine. Consider the freedom from the threat of blackmail that accompanies an individual going public with a secret, such as homosexuality and extra-marital affairs. One strand of feminism views exposure of the female body and the assertion of sexuality as willful acts that, in their naturalness, demystifies and turns the viewed person into an active agent, rather than the subject or object of the actions of others.

The prying and often inane TV talk and reality shows, web cam pages, web blogs, the goofy waving of fans at televised events and videotaping conception, birth 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.

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.

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 outlets for this are prone to induce a sense of pseudoauthenticity, 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 of the lessened control we have over information and models in distant computer systems. Data shadows or ghosts based on tangents of personal information (stripped of context) increasingly affect life chances. The subject often has little knowledge of the existence or consequences of these data bases and of how their identity is 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 the ability of science to predict and generalize. It is central to current ideas about economic competitiveness and risk management. The data analyst goes from known empirical cases to equivalent cases which 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 as ways of doing societal business increasingly clash with many of our basic Enlightenment ideas of individualism and dignity -ideas which were better articulated, and less contestable, in technologically simpler times.

In the face of grave risks and the blurring of lines between the foreign and domestic, today's security issues are more complicated, but still involve the question of where control agents should look (both morally and practically) to discover or prevent harm and how their behavior should be reviewed. A central idea in the Bill of Rights and in the general culture is that there be reasonable grounds on which to investigate, absent that individuals should be "let alone" as Warren and Brandeis (1890) argued. Of course just what being left alone means is contentious, especially when searches are done directly by machines rather than people.

Searches in the eighteenth century had a cruder physical quality and the object of a search was something material - whether contraband or printed material. Today, networks, electronic transactions and communication and behavior patterns that are more publicly accessible than papers hidden in a drawer, are of search interest. New data mining techniques (such as those proposed for the Total Information Awareness program, CAPPS2 for airline passengers or NSA's satellite screening of communications) depend on dragnets (both with respect to kinds of data and persons) of staggering breadth. There is an initial superficial troll in the hope of finding cases for more detailed investigation. The traditional standard is less easily applied to the initial automated search.

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.

Things that are "voluntarily" turned over to third parties such as garbage or dialed telephone numbers, along with what "a person knowingly exposes to the public, even in his own home or office" such as a voice sample, handwriting, fingerprint or facial appearance are generally beyond the search restrictions of the Fourth Amendment. Efforts to protect these (e.g., by shredding garbage or putting it in a sealed container), which clearly indicate an expectation of privacy, are not sufficient to legally guarantee it. Their exposure to "public" (defined as others, rather than as a particular place) brings the risk of revelation or discovery [18]. A central issue is of course what "exposure" means in an age of sense-enhancing (and often covertly and remotely applied) surveillance devices, which may, or may not, be widely known about or in common use. The two criteria of reasonablness offered by the landmark Katz case --the expectation of privacy as socially reasonable and the individual's expectations (which can be inferred from whether or not the individual takes actions to protect privacy, as well as from what the individual is aware of) are often at variance.

However my concern here is more with less visible 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). The Fourth Amendment is not what it was following the decisions of the Warren Court, particularly with respect to the exclusionary rule [19]. However it is still very far from what it was at the end of the eighteenth century. The overall pattern of the greater institutionalization of civil rights and civil liberties over the last century (whether involving race, gender, children, work, freedom of expression and association or searches and life styles) is unlikely to be reversed. Jagged cycles rather than clean linearity will continue to characterize this turbulent history. The maximally unconstitutional Alien and Sedition Acts have not returned. Wartime restrictions (whether Lincoln's suspending of habeas corpus or limits on speech during WW II) have been lifted as calmer times reappeared. To be sure the evidence of ebbs is undeniable, but relative to the period immediately after 9/11, there are some flows as well [20]. Power differentials can of course be enhanced by recent technical developments. However, for the questions considered in this article the centralizing power implications are more mixed [21]. Certainly the more privileged have greater say in what technologies are developed and greater access to them, as well to means to thwart them. Just because all persons radiate accessible data does not mean that data receptors are unaffected by social stratification. On balance, technical innovations are more likely to bolster, than to undermine, the established order. The developments I note can disguise a substratum of power, coercion and inequality.

Yet some counter points to an unqualifiedly hegemonic perspective can also be noted. These developments suggest a paradoxical view in which the technology's sponge-like absorbency is joined by its laser-like specificity -permitting both mass (nondifferentiated) and individual (highly differentiated) targeting. Data mining nicely illustrates this.

Universalistic or categorical (dragnet) requests for personal information have an egalitarian, rather than an individualizing and differentiating quality. The camera lens catches all within its province regardless of social characteristics (although the distribution of lens can hardly be said to be socially neutral).

The trade of personal information for consumer benefits better characterizes the more, rather than the less, privileged social groups. In addition, as with the Rodney King and related cases, widely available, low visibility techniques (e.g., video, audio and audit trails) can also be used against the more powerful.

Yet the cultural changes noted 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 [22].

A bad law can be challenged in court or repealed. A dangerous technology can be banned, regulated or challenged with a counter-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).

Is it Happening Here?

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 or the inability of 500,000 cameras in London to prevent the transit bombings; the failure of various airline passenger screening programs; wrongful convictions and the problems of some crime labs, the weakness of facial recognition technology in natural settings 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 and chill liberty. These twin threats are part of the enduring paradox of democratic government which 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 neoliberal ethos of the last decade. In what might be called the "only you" theory of social control, individuals are encouraged to protect themselves and those close to them, because government can't (or won't).

The individualized strategies seen with the offering of one's own information, and information on others, grows out of noble traditions of volunteerism and individual responsibility that are central to self and social control in a democracy. Yet private solutions for social, economic and political problems can be taken too far.

The idea of voluntary compliance and self-help valorizes increased individual choices, costs and risks. It simultaneously weakens many social protections and programs and pays less attention to the ways the social order may produce bad choices and collective problems. The consequences of these are then left to individual and private solutions [23].

This generates a suspicious society in which paranoia is entangled with reality. This emphasis can further social neglect and subsequent problems, leading to calls for more intensive and extensive surveillance, citizen cooperation and privatization in social control.

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 (or coerced or seduced) voluntarism and from open to secret data collection-these are points on continuums. We can differentiate information that is secret or unknown because an individual has discretionary control over revelation (e.g., regarding life styles, consumption, finances, religious and political beliefs) from that which is not revealed because a sense enhancing technology is lacking to reveal it (e.g., traditionally being unseen in the dark or from miles away).

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 call 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 some legitimate conflicting interests. Any practice is also likely to involve some conflict in values. Thus categorical pre-screening of everyone, as against only those there is a specific reason to screen is fair. Yet it can violate other cultural standards.

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 [24].

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 need to be strengthened, not weakened or ignored. Contemporary moral-panic efforts to erode these must to be strenuously resisted.

With respect to contemporary search questions those who would further unleash surveillance engage in high order mendacity when they attack critics for being against the goal of security, or against discovery behavior per se. Tough times may call for extreme measures. The real issue is one of procedure and accountability. The need for more invasive methods must be met with a corresponding increase in oversight and review. Today these too often are moving in opposite directions [25].

We need to better define the meaning of "search". Absent that we continue the drift toward blurring the lines between superficial and more probing searches and applying standards that may be appropriate for the former to the latter.

It would be foolish to elevate transparency and consent to absolutes, 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. Yet we need to rethink just what consent means when it is possible to so easily evade or manipulate it. What is an individual consenting to in "being" in public and in not shielding information that might be available to hidden technologies?

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 [26].

Consent obtained through deception, 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.

We need a principle of truth in volunteering: it is far better to say clearly that "as a condition of [entering here, working here, receiving this benefit…] 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 [27]?

We need to overcome the polite cultural 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 to inappropriate requests.

Finally, technology needs to be seen as an opportunity, rather than only as a problem. Technologies can be designed to do a better job of protecting personal information and notifying individuals when their information is being collected or has been compromised. Video monitoring systems can be designed to block out faces as their default position and X-ray and T-ray systems can be programmed to block anatomical details [28].

E-ZPass toll collection systems can be programmed to deduct payment, while protecting the anonymity of the driver. RFID technology can build notification in 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). 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.

From one perspective using technology to protect one's personal information may offer legal support for an expectation of privacy. In Kyllo v. United States, a case involving the legality of a search warrant based on evidence from thermal imaging technology, the dissenting judges argued that because the suspect did not take any actions to block the heat emissions that passed through his roof from his marijuana grow lights, he did not have an expectation of privacy. There thus is no Fourth Amendment issue and the police action should not require a warrant [29].

From this sorely misguided perspective what can be routinely done determines appropriateness. Once a technology becomes widely available and is well known, responsibility for protection shifts legally (as well as practically) to the individual, not to those who would cross personal borders. In failing to act in response to changed technical circumstances beyond his or her control, the individual is seen to be making a choice and in a sense again volunteers to be searched and to accept whatever risks may be involved.

However, the goals and consequences of the technique need to be considered independently of any actions taken (or not taken) by the subject. Greater responsibility must be placed on those with the search tools as is the case in Europe. There the emphasis is on the general principle of respect for the dignity of the person as means of privacy protection. (Whitman 2004) [30]. This calls attention to the consequences of the actions of the search agent, rather than to the risks and rewards the subject is willing to accept. With respect to surveillance questions, market mechanisms involving choice, whatever their instrumental advantages, are less relied upon in much of Europe.

This also offers a general protective principle regardless of what new technologies are developed. As a result the appearance of new snooping technologies is generally less controversial in Europe, where they are in a sense still-born with restrictions. In the United States new technologies tend to be born enabled and any restrictive policies must be sought anew for each technique (e.g., caller-Id, drug-tests, video cameras).

In the United States a "blame the victim" caveat subjectus logic cries out for a cartoon entitled, "where will it end?" Beyond the paper shredder which has become routine in many homes [31]. The cartoon would show a citizen driven to protect privacy by always wearing gloves, a mask and perfume; and [32] having a closely shaved head; talking in code and encrypting all communications; insulating home, office and packages in thermal image resistant tin foil and only using restrooms certified to be monitoring free.

One way to think about the topic is to note that many of the kinds of surveillance once found only in high security military and prison settings are seeping into the society at large. Are we moving toward becoming a maximum security society where ever more of our behavior is known and subject to control?

Some features of the maximum security society are: 1) a "sensed" (and perhaps censored) society based on ubiquitous and ambient sensors softly, invisibly, effortlessly and continually gathering behavioral, locational, communication and physiological data 2) a transparent society, in which the boundaries of time, distance, darkness, and physical barriers that traditionally protected information are weakened and pierced 3) a dossier society in which computerized records play a major role 4) a networked society in which diverse kinds of previously unavailable (or if available, disaggregated) personal data are woven together in an ever finer mesh 5) an actuarial and risk-adverse society in which decisions are increasingly made using such data for predictions about future behavior as a result of membership in, and comparisons to, aggregate statistical categories 6) a suspicious society in which every one is assumed to be a possible subject of interest 7) a self-monitored society, in which auto-surveillance under the constant uncertainty of discovery plays a prominent role 8) an engineered society in which choices are increasingly limited and determined by manipulating physical and social environments.

In hopefully writing an imprescient novel, Sinclair Lewis in 1935 suggested It Can't Happen Here. But of course it can, and in some ways it has. In a book on undercover police practices I considered the softening of social control in other forms beyond those discussed here [33].

In concluding that book two decades ago I wrote,

> 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 and deceptive and shrouded in benign justifications, this is clearly the more difficult task (Marx 1988).

In 2006 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.

*Expanded version of article in Dissent Winter 2005. A related version will appear in T. Monahan, (ed.) Surveillance and Security: Technological Politics and Power in Everyday Life, forthcoming. I am grateful to Peter Andreas, Pat Gillham, Jackie Ross, Richard Leo, John Leudsdorf, Torin Monahan, Clive Norris, Zick Rubin, Jay Wachtel and Jim Rule for critical suggestions.

Endnotes

1. 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.

A review of 20 recent instances found that in the overwhelming majority of cases DNA dragnets did not lead to success. In seven of the cases traditional investigation methods did. (Grand 2002; Chapin 2005; Electronic Privacy Information Center 2005; see also Walker 2005).

2. This is the techno-fallacy of autonomous technology in which the hand and the assumptions of the human designer are unacknowledged. In Marx (2003) I discuss 21 such fallacies associated with communication and surveillance technology.

3. 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. A distinction can be drawn between an individual offering data that permits other members of his or her group to be better manipulated ala an understanding of their demographics and attitudes, with offering data which stigmatize. Group stigmatization for example can apply to ethnic groups shown by DNA to have a proclivity for some illnesses (Alpert 2003).

4. The appropriate response is not to ban the subject's willful seeking of the information, but to rigidly control use of the information as it might be applied (e.g., by insurance companies) to other persons to whom it refers, but who have not sought it.

5. The program seeks to give "the average person terrorist indicators to watch for, not race or religion" (http://web.mit.edu/gtmarx/www/www.cateyesprogram.com).

6. 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). (Marx, forthcoming). 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. Thus in the Kyllo case the majority held that a search of the home was inherently invasive because of where it occurred. Whether the search discovered heat emissions or contraceptives was irrelevant. The "where," not the "how" or "what" defined it.

> 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.

7. In such contexts the identification of early stage pregnant employees is of particular interest.

> The automated analysis of urine offers the same potential. 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 earlier diagnosis of health problems. On the other hand ...

8. Consider for example the transit authority in Sheffield, England who, 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".

9. Here science may come to the defense of folk prejudices which hold that the "other" smells differently.

10. 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. Ray Bradbury's heroes in Fahrenheit 451 who resisted a book burning, totalitarian regime by memorizing destroyed books would need to find alternative means.

While there is some overlap, compare the passive, low-visibility reading of personal information (whether brain waves, smells, or from a chip) that is involuntarily transmitted with the widespread use of air-sniffing radiation-detection devices aimed at places rather than persons.

11. 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 copresent individuals whose chips are also read and an analysis of the timing of passages).

Technologies can be contrasted by whether their application requires the subject's awareness and active or passive cooperation (or at least involvement). Compare truth determination via the traditional polygraph attached to the individual with reading of facial signals, or the analysis of word patterns. The Enron case partly relied on finding lying through the analysis of word use patterns in e-mails. Of course in the latter cases subjects can be informed that low visibility techniques are being used and consent can be requested. Even when there is no formal request for permission-as with being starred at, awareness may offer the possibility of deterring, challenging or avoiding the unwanted data collection. Visibility can make reciprocity an option.

12. In a government context requests for voluntary searching is legal as long as police do not, "convey a message that compliance with their requests is required" and refusal to volunteer can not be used against the person. (Florida v. Bostick 1991) Yet apart from their words, the official status, badge, weapon and demeanor of an officer may convey an alternative message. Efforts to deceptively create the impression that information must be legally provided would seem to violate the 5th Amendment.

13. Consider, for example, the politicians who release their drug test records and sworn statements attesting to their marital fidelity and who challenge their opponents to do the same. Since the court in Chandler v. Miller, 117 S.Ct. 1295, 1303 (1997) overturned a Georgia ruling permitting drug testing of those currently holding or seeking public office, this can no longer be legally required. Social pressure and a strategic response to such a challenge is, however, another matter.

14. 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.

15. 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.

16. The issue with fingerprints, beyond the symbolism in their association with criminals and temporarily stained finger, is the absence of anonymity and the ability to link disparate records. As noted in a recent development the dirty finger smudge problem (and reminder) has been eliminated through an inkless system.

17. See for example recent studies by Glassner 2000.

Altheide 2002.

18. Major Supreme Court cases here are: trash-California v. Greenwood 1988 and United States v. Scott 1992; dialed telephone numbers-pen register data, Smith vs. Maryland 1979; voice sampling-United States v. Dinoisio 1973; handwriting sample-United States v. Mara 1973.

19. Dash (2004) offers a short history of the whittling down of the exclusionary rule.

20. Note pointed Congressional discussions on revising the Patriot Act, an explosion in state privacy laws, and the many local communities that passed resolutions in opposition to aspects of the Patriot Act. Of course in many ways the United States lags behind Europe, but the point is not only how far laws and policies are from the ideal, but that they are on the books and that they have a symbolic meaning and reaffirm values. In some of its actions (e.g., banking, fair credit reporting legislation, the 1986 Electronic Privacy Protection Act) the congress has implicitly legislated the ethos of the fourth amendment. Consider too, the consciousness raising aspects of recent legislation requiring companies that discover the electronic compromising of personal data to notify subjects and the "do not call lists".

21. Qualifications to the too easy linkage of power and surveillance are discussed in Marx (2005).

22. Of course there are limits such as on selling a kidney, selling one's self into slavery or waiving medical or legal liability. Recent HIPPA legislation does however permit waiving of a jury trial in the event a patient has a dispute with a medical provider.

23. Katz (2001) for example argues that the subjection of children to new surveillance tools (nanny and daycare cams, drug testing, electronic tracking and the like) is in response to the lack of adequate social provision for the needs of children and the creation of safer public environments.

24. There is also need to analyze what is meant by trade-offs, what the empirical evidence is for concluding trade-offs are in fact present and how focusing on one set of questions often means ignoring others (Monahan, forthcoming). We can also identify conditions under which privacy and security are supportive or at least congruent, for example appropriately applied, highly effective systems minimize false accusations and unnecessary searches and treating citizen's with respect can enhance legitimacy and cooperation with control agents.

25. Consider the monitoring of international communications of Americans by NSA without recourse (even on a delayed bases) to the warrant requirement of 1978 law and significant weakening of the Attorney Generals and local guidelines on intelligence gathering. N.Y. T. Dec.19, 2005. Notes also a decline from 200 million documents declassified in 1998 to 44 million in 2005 and a doubling to 15 million of the number of newly classified government documents. N.Y.T. Dec. 29, 2005.

26. The "opt-in" feature of some data base systems reflects this in using the information of persons who are informed and who consent.

27. These are related to 20 broad questions and related principles that I suggest (Marx 2005) be asked about any collection of personal information. These involve factors such as goal appropriateness, means-ends relationships, identifying and dealing with undesirable unintended consequences and reciprocity. In general the more the questions can be answered in a manner consistent with the underlying principles, the more legitimate the collection of personal information is.

> I prefer a contextual approach to the policy questions, rather than one that begins with a value that must always take precedence-whether this involves the rights of the individual or the needs of the community.

28. The latter would eliminate the need for same sex monitors with its assumptions of a homogeneity regarding the sexual orientation of the watched and the watcher.

29. In this reading such a search is legal according to the Supreme Court's test established in the 1967 Katz case. The majority of Justices however did not agree. On the other hand, the failure to take protective actions might also be seen to suggest that the individual expected the activity to remain private because he was unaware of high-tech means not yet widely used. He hence saw no need to take blocking actions. As with so much in the law, the line here is more like a cooked noodle rather than a re-bar.

30. The greater role of liberty as the most salient principle for protecting privacy in the United States (particularly from government) is also supportive of the citizen's right to volunteer personal information. It ironically also serves to legitimate the liberty claimed by private agents of surveillance, gun owners and purveyors of hate speech. A key issue is how liberty plays out for various kinds of actors.

31. Those not wanting to use a paper shredder might consider moving to Beverly Hills, California where it is illegal to rummage through other's garbage left on the street.

32. However research efforts are underway to overcome any distorting elements for human smell essence that perfume or eating garlic might disguise.

33. The means considered in this paper, along with other changes suggest a decline in the use of domestic coercion in many spheres. Thus consider the practical disappearance of whipping, flogging and public executions, lesser use of capital punishment, a decline in the homicide rate and of corporal punishment in

the home and schools and programs emphasizing antibullying and the development of discussion and negotiation skills. The development of nonlethal weapons might also fit here (but as with the softening of power more generally it may come with increased use and intervention-see note 15). Nonlethal weapons are sometimes lethal.

Robert Nisbet (1975) considers the softening of power in broader historical perspective as does Foucault (1977) from a different critical perspective. Richard Leo (1992) offers a case study of the move from coercion to deception in police interrogations as the third degree largely disappeared. One can also make distinctions between hard and soft control problematic. They may share the logic of bribery, which when pushed, can blur the borders between them. Thus how should we conceptualize compliance gained by the threat, but not the application, of coercion? Certainly this is hard, yet the absence of punishment or cost becomes a sort of reward, or at least an inducement. The carrot lies in avoiding the stick.

In another example of blurred borders, consider the expanding number of fast track programs which offer individuals the chance to give up personal information in return for preferential treatment, such as at airports or on toll roads. Here the potential stick of "long waits" is avoided for the carrot of "no wait", by submission to another stick-that of "volunteering" personal information.

Court Cases

Bostick v. United States, 501 (1992)
Katz v. United States, 389 U.S. (1967).
Kyllo v. United States 99.8508 (2001).

References

Alpert, S. 2003. "Protecting Medical Privacy: Challenges in the Age of Genetic Information." Journal of Social Issues Vol. 59:2.

Altheide, D. 2002. Creating Fear: News and the Construction of Crisis. New York: Aldine de Gruyter.

Chapin, A. 2005. "Arresting DNA: Privacy Expectations of Free Citizens Versu Post-Convicted Persons and the Unconstitutionality of DNA Dragnets." Minnesota Law Review 89.

Dash, S. 2004. The Intruders. New Brunswick: Rutgers University Press.

Glassner, B. 2000. The Culture of Fear. Basic Books: New York.

Grand, J. 2002. "The Blooding of America: Privacy and the DNA Dragnet." Cardozo Law Review.

Foucault, M. 1977. Discipline and Punishment: The Birth of the Prison. New York: Vintage.

Katz, C. 2001. "The State Goes Home: Local Hyper-Vigilance of Children and the Global Retreat from Social Reproduction." Social Justice Vol. 28(3)...

Leo, R. "From Coercion to Deception: The Changing Nature of Police Interrogation in America." Crime,Law and Social Change Sept. 1992.

Lewis S. 1995. It Can't Happen Here. Signet Classics: New York.

Lyon D. 2002. Surveillance and Social Sorting. New York: Routledge.

Marx, G. 1988. Undercover: Police Surveillance in America. Berkeley: University of California Press.

------. 2003. "Some Information Age Technofallacies." Journal of Contingencies and Crisis Management. March 2003.

------. 2005. "Seeing Hazily (But Not Darkly) Through the Lens: Some Recent Empirical Studies of Surveillance Technologies." Law and Social Inquiry Spring.

------. Forthcoming. "Varieties of Personal Information as Influences on Attitudes Toward Surveillance." In the Politics of Surveillance and Visibility, edited by R. Ericson and K. Haggerty. Toronto: University of Toronto Pres..

Monahan, T. Forthcoming. "The Wrong Questions about Security and Surveillance."

Nisbet, R. 1975. The Twilight of Authority. New York: Oxford University Press.

Riesman, D. et al. 2001. The Lonely Crowd. Yale University Press: New Haven.

Electronic Privacy Information Center, 2005. Brief of Amicus Curiae. U.S. Court of Appeals for the Fifth Circuit. No. 05-30541. Case No. 3:03-cv-00857-JJB-CN

Walker, R. 2004. "The Corporate Manufacture of Word of Mouth." The New York Times Magazine, December 5, 2004.

Walker, S. 2004. "Police DNA 'Sweeps' Extremely Unproductive: A National Survey of Police DNA Sweeps." Department of Criminal Justice, University of Nebraska. Unpublished manuscript.

Warren S. and L. Brandeis. 1890. "The Right to Privacy." Harvard Law Review 4:193.

Whitman, J.Q. 2004. "The Two Western Cultures of Privacy: Dignity Versus Liberty." Yale Law April, Vol. 113(6).