日本財団
The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

“The IT Revolution and the Transformation of Society”

Tokyo

November 5-6, 2003

“Internet Anonymity as a Reflection of Broader Issues Involving Technology and Society”

By
Prof. Gary Marx
Professor Emeritus of Sociology
Massachusetts Institute of Technology

Internet Anonymity as a Reflection of Broader Issues Involving Technology and Society*

It's a remarkable piece of apparatus.

F. Kafka, "The Penal Colony"

Gary T. Marx, M.I.T.

I am honored to be at the Institute for International Policy Studies meeting and for the chance to share ideas with, and to learn from, a distinguished international group of colleagues about phenomena that have done, and are doing, so much to transform our societies. The hurricane of social change being wrought by information technology can be viewed as among the great transformations of civilization, along with the development of permanent agricultural communities, urbanization, and industrialization.

Yet it is also important to ask how social and cultural factors effect the forms and processes of information technology, especially across cultures and time periods. We must avoid the reductionist trap of technological determinism involving the failure to appreciate the extent to which human choices in turn effect technical forms and impacts.

I am a sociologist who for several decades has been studying the social impacts of information technology, particularly as these involve questions of privacy, anonymity, confidentiality, identity, civil liberties, surveillance, crime, deviance and social control. Much of this work is summarized in a web page: garymarx.net .

In this short period I will say a bit about anonymity and information technology. I will use this topic to illustrate some more general conclusions about why issues of information technology and society are so very complicated and do not lend themselves to easy solutions, nor support the rhetoric of technophiles who optimistically view information technology as the solution to societal problems, nor the technophobes who pessimistically view it as the source of societal problems.

The topic is complicated because 1) the elements or variables are multi-dimensional and contextual 2) there are enduring value/goal conflicts and often a lack of clarity with respect to what abstract values mean and how they should be prioritized and 3) there are ironic trends and counter-trends and unintended consequences. The field is fluid with new opportunities and problems ever emerging. Solving one problem may create another in an endless dialectical dynamic.

I will summarize 5 topics related to these questions from a much larger body of work.[1] The topics are 1*) some types and contexts* of anonymity 2) *some values* supporting and opposing anonymity in communication and some broader *value conflicts* within which these fit 3) *some trends and counter trends* involving information technology and society as this relates to personal information. 4) *some techno-fallacies* of the information age and 5) *some principles* to guide the setting of policy as this involves personal information and surveillance.

- *Remarks prepared for conference on "The IT Revolution and the Transformation of Society" Tokyo, Nov. 2003, Institute for International Policy Studies.*

A. Types and Contexts of Anonymity

First we can make problematic the question of anonymous with respect to *what*? [2]The dictionary defines anonymous as “not named or identified”. Thus the issue more broadly involves the availability or unavailability of a variety of kinds of information that may be known or identified about persons. Nine descriptive types of information about individuals which may be revealed or concealed can be noted. (Marx, forthcoming). These are:

1. Individual identification ***[the who question]***

2. Shared identification ***[the typification question]***

3.Geographical/Locational ***[the where, and beyond geography, how to reach question]***

4.Temporal ***[the when question]***

5. Networks and relationships ***[the who else question]***

6. Objects ***[the whose is it question]***

7. Behavioral ***[the what happened question]***

8. Beliefs, attitudes, emotions ***[the inner or backstage and presumed “real” person question]***

9. Measurement Characterizations (predictions, potentials) ***[the kind of person question, predict your future question]***

Table 1 offers examples of these concepts. Table 2 offers a different, more abstract approach in considering factors that may cut through these descriptive forms, uniting the seemingly dissimilar and separating the seemingly similar shown. With respect to these categories the absence of anonymity and the involuntary revelation of personal information becomes more problematic the more the values on the left side of the table are present.

I hypothesize that other factors being equal when anonymity or non-revelation are appropriate but not honored there is an additive effect and the more the values on the left side of the table are present, the greater the perceived wrong in the collection of personal information. The worst possible cases involve a core identity, a locatable person, and information that is personal, intimate, sensitive, stigmatizing, strategically valuable, extensive, biological, naturalistic and predictive and reveals deception, is attached to the person, and involves an enduring and unalterable documentary record.

One Size Does Not Fit All

Beyond the above types and dimensions, regarding personal information, judgements will vary depending on:

1. ***types of communicator/recipient*** (children and other dependents, responsible and irresponsible adults, law enforcers, persons vulnerable to retribution for reporting wrong-doing, those seeking information vs. those from whom information is sought, sending information/communication vs. receiving it)
2. ***the structure of communication*** (one-on-one, one-to-many, many-to-one and reciprocal or non-reciprocal, real or stale time, moderated and unmoderated groups)
3. ***types of activity*** (browsing, requesting information, posting bulletin boards, E-mail, discussion groups)
4. ***content/goals*** (games, self-help groups, hot lines, commerce, politics, science, protecting the sender of a communication or the recipient)
5. ***the national and cultural borders*** that communication invisibly crosses and types of response (prohibit, require, optional but favor or disfavor, laws, policies, manners). Even if one could agree on a policy regarding computer related anonymity, there is no central world net authority to implement it and technically doing this would be difficult.

B. Rationales For and Against Anonymity

The public policy questions raised by technologies for collecting personal information are more controversial than many other issues such as ending poverty and disease. In those cases the conflict involves asking "how" rather than "why". The questions raised by the concealment and revelation of personal information are like some relationships in which persons can not live with each other, but neither can they live apart. The issue becomes under what conditions do they co-exist? So it is with anonymity and identifiability. There are existential dilemmas and in many cases we are sentenced to a life of trade-offs.

I often ask my students what society would be like if there was absolute transparency and no individual control over personal information --if everything that could be known about a person was available to anyone who wanted to know. Conversely what would society be like if there was absolute opaqueness such that nothing could be known about anyone except what they chose to reveal. The absolute anonymity vs. absolute identifiability is a strand of this. Both of course would be impossible and equally unlivable, but for different reasons. To have to choose between repression and anarchy is hardly a choice between a pillow and a soft place.

The hopeful Enlightenment notion that with knowledge problems will be solved holds more clearly for certain classes of physical and natural science questions than for many social questions. Certainly those who live by the pursuit of truth dare not rain on that parade. Yet there is a difference between knowledge as providing answers, as against wisdom. Current debates over anonymity and identifiability in electronic communications would greatly benefit if better data were available, but the issue would not disappear because the value conflicts and varied social and psychological pressures remain.

A cartoon image nicely captures this -- we see a tanker truck with a sign on the back which says, "the scientific community is divided about this stuff. Some think it is hazardous. Some don't." So it is with this issue. The divisions do not reflect ignorance, stupidity, ill-will and evil on one side and empirical truth, wisdom, benevolence and righteousness on the other. Rather they reflect varying degrees of empirical truth on both sides and differing value priorities. Being able to disentangle these is vital for our understanding and for developing policy. Let us consider the values and goals question.

Among the most common justifications for full or partial anonymity:

1. to facilitate the flow of information and communication on public issues.
2. to obtain personal information for research in which persons are assumed not to want to give publicly attributable answers or data.
3. to encourage attention to the content of a message or behavior, rather than to the nominal characteristics of the messenger which may detract from that.
4. to encourage reporting, information seeking, communicating, sharing and self-help for conditions that are stigmatizing and/or which can put the person at a strategic disadvantage or are simply very personal.
5. to obtain a resource or encourage a condition using means that involve illegality or are morally questionable, but in which the goal sought is seen as the lesser evil.
6. to protect donors of a resource, or those taking action seen as necessary but unpopular from subsequent obligations, demands, labeling, entanglements or retribution.
7. to protect strategic economic interests, whether as a buyer or a seller.
8. to protect one's time, space and person from unwanted intrusions.
9. to increase the likelihood that judgements and decision-making will be carried out according to designated standards and not personal characteristics deemed to be irrelevant. A well known cartoon of two computer literate dogs captures this, as one says to the other, “on the internet no one knows you’re a dog.”
10. to protect reputation and assets.
11. to avoid persecution.
12. to enhance rituals, games, play and celebrations.
13. to encourage experimentation and risk taking without facing large consequences, risk of failure or embarrassment.
14. to protect personhood or "it's none of your business".
15. traditional expectations.

A consideration of contexts and rationales where anonymity is permitted or required must be balanced by a consideration of the opposite. The rationales here seem simpler, clearer and less disputed. While there are buffers and degrees of identification, the majority of interactions of any significance or duration tilt toward identification of at least some form.

Central to many of the contexts where some form of identifiability is required we find the following rationales:

1. to aide in accountability.
2. to judge reputation.

3. To pay dues or receive just deserts.
4. to aide efficiency and improve service.
5. to determine bureaucratic eligibility --to vote, drive a car, fix the sink, cut hair, do surgery, work with children, collect benefits, enter or exit (whether national borders, bars or adult cinemas).
6. to guarantee interactions that are distanced or mediated by time and space.
7. to aide research (links to other types of personal data and longitudinal data).
8. to protect health and consumers.
9. to aid in relationship building.
10. to aid in social orientation.

The value conflicts involving anonymity and identifiability are nestled within a broader set of information and societal value conflicts.

Value Conflicts

There are enduring value conflicts and ironic, conflicting needs and consequences which make it difficult to take broad and consistent positions regarding the revelation or concealment of personal information as this involves information technology.

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 societies we want to be seen and to see, yet also to be left alone. Note the desire to reveal as seen in popular talk shows and celebrity tell-all books and public relations activities.

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 data. The expectation that one should be judged as an individual and in context may conflict with the greater rationality and predictive success believed to be found in responding to aggregates.

Many discussions between those who look optimistically at information technology as the solution and those who view it as the problem reflect Rudyard Kipling’s tale about blind persons and the elephant, in which each observer offers a plausible identification for one part of the elephant (e.g., the tail as rope). That is a legitimate goal or social trend is identified but others confounding ones are ignored or denied.

C. Some Trends and Counter Trends

Let me locate changes in anonymity alongside of a number of other social developments that suggest issues for social research and which make broad and unitary social and moral assessments challenging.

Central to these developments are the continuing very rapid changes in data collection, storage and analysis. Through 2003, processing speeds had doubled every 18 months and storage capacities had doubled every year. (Privacy in the Information Age, National Academy of Sciences, forthcoming)

Means of data analysis once restricted to governments and the largest organizations are available on a much wider scale to smaller organizations and individuals. Diverse kinds and sources of data are increasingly woven into a network. Computing is becoming ubiquitous and automated with sensors that passively read and send (with no action required on the part of the actor) remote signals to the internet and elsewhere, are increasingly found in objects (e.g., computing and communications devices, switches, groceries, cars, tools, weapons, clothes), persons and environments (roads, walls, doors). Through a "value-added" model the aggregation and analysis of data collected in varying formats and for varying purposes in turn creates new data and models. More information is also available for analysis because ever more is being kept rather than culled. It is now less expensive to store information than to discard it.

Given such changes, among trends that many see as worrisome and actually, or potentially, threatening traditional values of democratic societies:

1 ***the decline of anonymity***. The ability to be unnoticed has declined significantly, although this is not the same as being uniquely known.

2 ***making the meaningless meaningful***. Once noticed the ability to remain unidentified, whether by core identity, or some other specific measure has declined.

3 ***colonization of time, space and physical borders***. Whether voluntarily or involuntarily on the subject's part, the ability to discover and track the varied forms of individual information in real time across physical barriers, locations and over time has significantly increased.

4 ***increased validity (if still far from ideal for many purposes)***. When correctly applied, current core identification technologies show a high degree of validity relative to the cruder bodily measurement and eye witness techniques of the 19th century. Validity and understanding of current empirical events, competencies and experiences on the average is stronger than for those in the past and the latter in turn tend to have a greater validity than for future predictions. This factor has mixed consequences but the specter of unseen control is a concern.

5 ***category expansion***. There is a significant expansion of ways of measuring and classifying individuals and contexts and these are retrospective, as well as prospective. These abstract characterizations that symbolize personal characteristics involve behavior as well as presumed essence (whether physiological or moral). These often are, but need not necessarily be, attached to a core identity. These involve greater precision with respect to traditional measures, as well as composite measures that are increasingly removed from the "natural" relatively uncomplex factors which composed personal information prior to, and even during industrialization.

6 ***The merging of previously compartmentalized data***. The ability to be known

about as a result of combining indicators has significantly increased.

7 ***Apart from technical developments that permit involuntarily collecting personal information, there has been a major expansion of laws, policies and procedures mandating that individuals provide information.*** Whether related to effectiveness, crises, or fairness, access to participation in modern life (voting, government benefits, employment, building or gated community access etc.) increasingly requires some form of identity validation.

8 ***the integration of life activities with the generation of personal data***. We increasingly live in ways that automatically provide personal information as part of the activity –i.e., the use of credit cards, communication and driving.

9 ***the blurring of lines between public and private places makes personal information more available.*** Note the privatization of places traditionally seen as "public" such as shopping malls and industrial parks (with legal means of collecting personal information). Or consider the blurring of the lines between home and work and the merging of public and private data bases and the ability of technologies to reveal some aspects of what is within a private space without the need to literally enter it, e.g., thermal imaging or cameras in pubic places that aimed at private places. Other examples are the availability of web and related searches in finding and merging personal information that had been *de facto* private because of spatial and temporal separation and the presumed ability to learn about non-consenting individuals by generalizing from those sharing attributes who voluntarily provide the information (e.g., focus groups).

These trends suggest the familiar no where to run, tightening of the noose, decline of private space, privatization of public space, Leviathan all-knowing political, commercial and even interpersonal State of the dystopic imagination. Yet however powerful as an indicator of a social trend and as a raiser of consciousness, this view must be tempered by noting opposing developments.

The current situation is dynamic and rapidly changing. Some opposing trends involving the ironic vulnerabilities of any system of control, as well as broader historical trends can be seen. Among some counter trends:

1) ***increased freedom of choice***. Individuals in some ways are freer both morally and tactically to make or remake themselves than ever before. Some identities that historically tended to be largely inherited such as social status or religion can more easily be changed. Other identities have become culturally more legitimate, such as divorce and homosexuality, out of wedlock birth, adoption, with a subsequent decline in traditional stigmas and the need to be protective of certain kinds of information.[3] Even seemingly permanent physical attributes such as gender, height, body shape or facial appearance can be altered, whether by hormones or surgery or beauty parlors. The ultimate is the emerging technology of total face transplants.Television "make over" shows and self-altering products reflect related strands of this. These developments reflect the emergence of a more protean self and the self as a commodity and an object to be worked on, just as one would work on a plot of land or carve a block of wood. Identities in some

ways are becoming relatively less unitary, homogeneous, fixed and enduring, as the modernist idea of being able to choose who we are continues to expand, along with globalization processes. This is aided by the expansion of non-face-to-face interaction.[4]

2) ***new opportunity structures for exercising choice***. The distance mediated interaction of cyberspace which calls forth new means of authentication also opens up a vast potential for offering various forms of alternative or prevaricated individual information. Cyberspace as play (e.g., internet service providers offering on-line aliases and fantasy chat rooms) encourages this.
3) ***new functional alternatives to core identity***. The absolute number and relative importance of non-core forms of identity offering varying degrees of anonymity has increased. There is a significant expansion in the variety of pseudonymous certification mechanisms intended to mask or mediate between the individual's name and location, yet still convey needed information. As more and more actions are remotely tracked in cyberspace (e.g., phone communication, highway travel, consumer transactions) the pseudonym will become an increasingly common and accepted form of presenting the self for particular purposes (whether as a unique individual or as a member of a particular category). A cartoon showing a talking bird who speaks but only anonymously illustrates this.
4) ***enhanced chances for neutralization***. Beyond the expansion of life style/identity choices we see the ironic emergence of markets for counter-surveillance offering a vast array of methods to protect individual information, whether by blocking, distorting, deceiving or destroying the surveillance means. Much of this represents a righteous response to the creeping or galloping expropriation of personal information, yet some also represents new opportunity structures for violation. The ease of presenting fraudulent identities divorced from the traditional constraints of localism and place and time is central to crimes of identity theft.
5) ***significant improvements in technologies for protecting individual information***. With encryption there is the potential for a degree of confidentiality in communication, and enhanced accountability and data protection never before seen. Technologies and services for protecting personal information are increasingly available, from shredders to home security systems to various software and privacy protection services.
6) ***new normative protections and awareness***. There has been a significant expansion of laws, policies and manners that limit and regulate the collection of personal information and its subsequent treatment. There has been some growth in choice and opt-in systems. This ties to the broader 20th century expansions of civil liberties and civil rights, as well as to particular crises. Whether these go far enough, are effective, and how they compare across institutions and cultures are important research questions.

These opposing trends work against sweeping generalizations beyond this one against sweeping statements. Considered together some of the above developments are ironic and contradictory, I take this as a sign of reality's ability to overflow our either/or categories and the need to avoid simplistic theorizing, as well as the need for empirical research.

Let me move from the above considerations which reflect my views as an empirical scientist to some ideas more explicitly reflecting both data and values to inform policy.

Scholars can endlessly debate these questions. But those setting policy must act. What can an academic analysis such as the above offer? Awareness and vigilance and self-reflection is one answer! We must be mindful of the cultural background assumptions (both empirical and normative) that like icebergs lurk beneath the surface of our taken-for-granted worlds. We can also offer ideas as buoys or channels to direct policy.

D. Some Information Age Techno-Fallacies

In listening to the rhetoric around information technology and society I often hear things that, given my knowledge and values, sound wrong, much as a musician hears notes that are off key. Table 3 identifies a number "information age techno-fallacies" .

Beliefs may be fallacious in different ways. Some are empirically false or illogical, and with appropriate evidence and argument, persons of good will holding diverse political perspectives and values can agree that they are fallacious. Others are normative statements and will be seen as fallacies only when there is disagreement about the values, or value priorities on which they are based.

However the reasons for a normative position often involve empirical assumptions, along with moralistic claims. For the social scientist in particular, it is important to identify and evaluate the former.

While it is possible to identify fallacies (as well as truths) unique to particular information extractive tools and privacy contexts, my emphasis here is on fallacies that cut across these. Related beliefs about technology can also be seen in other issues such as those involving the environment, energy and transportation. [5]

E. Principles to Inform Public Policy

Finally let me go beyond calling for increased awareness of these assumptions and a call for empirical research and logical thought regarding them, to state some value positions or principles which I, as both a scholar and a citizen, would like to see more clearly reflected in our policies concerned with the social aspects of information policy. Here I move from the role of the scholar and scientist to that of the partisan advocate.

An English expression holds that, “where you stand depends on where you sit.” Certainly this social analysis reflects my own personal and national experiences. Cross-cultural analysis of the social impacts of information technology is sorely lacking and very needed. My comments refer to the situation in the United States. Yet I would hypothesize that the values reflected in Table 3 and 4 speak to the highest ideals of contemporary democratic civilization and are consistent with the United Nations Declaration of Human Rights. In addition through globalization and international convergence we see increased commonalties in social forms and impacts across societies. The cross border and non-territorial aspects of cyber-space also add a universal element.

With respect to questions of ethics and policies for governing the collecting, storing, accessing, merging, analyzing and communicating personal information the principles in Table 4 are central.

Many of these were first expressed in the Code of Fair Information Practices developed in 1973 for the U.S. Department of Health, Education & Welfare. They are also now found in various European and Asian directives.

The 1973 Code offered a principle of informed consent in which the data collection is not to be done in secret, individuals are to be made aware of how it will be used, and where appropriate, consent to it; a principle of inspection and correction in which individuals are entitled to know what kind of information has been collected and to offer corrections and emendations; a principle of data security in which the information will be protected and precautions taken to prevent misuses of the data; a principle of validity and reliability in which organizations have a responsibility to insure the appropriateness of the means used and the accuracy of the data gathered and a principle of unitary usage in which information gathered for one purpose is not to be used for another without consent.

As new information technologies, uses, and problems have appeared, additional principles have emerged. These include a sanctity of the individual and dignity principle in which there are limits (even with consent) on the taking, volunteering and commodification of personal information; a golden rule principle in which those doing the surveillance would agree to be the subjects of information gathering under comparable circumstances; a principle of consistency such that broad ideals rather the specific characteristics of a technology should govern surveillance practices; a principle of morality in which the fact that a tactic is legal is not sufficient justification for using it apart from broader ethical considerations; principles of relevance and of minimization such that only information that is directly relevant and necessary for the task at hand is gathered (minimization refers to both the amount of information gathered and the intrusiveness/invasiveness of the means); a principle of joint ownership of transactional data such that both parties to a data creating transaction should agree to any subsequent use of the data, including the sharing of benefits if appropriate; broadening of the principle of informed consent to favoring opting-in over opting out and a principle of co-determiniation, or at least consultation regarding policies; a principle of restoration such that in a communications monopoly context those altering the privacy status quo should bear the cost of restoring it; a safety net or equity principle such that a minimum threshold of information protection should be available to all; a principle of equal treatment such that surveillance deemed to be invasive, but appropriate, is applied to all members of an organization not just the least powerful members; a reciprocity or equivalence of tactics principle in which in situations of legitimate conflict of interest all parties can use the same tactics; a principle of timeliness such that data are expected to be current and information which is no longer timely should be destroyed; a principle of the periodic review and evaluation of data collection policies as broadly defined; a principle of human review such that an automated decision is always subject to review by a person; a principle of redress such that those subject to inappropriate surveillance or unfairly hurt by it have adequate mechanisms for discovering and being compensated for the harm; a less worse alternative means principle in which means are compared to each other and a sometimes it is better to do nothing principle in which the consequences of inaction are compared to those of action.

These principles can be stated in the form of questions to be asked about policy development for a given area such as anonymity. In an earlier 1999 paper drawing on many of the above principles, I suggested the questions found in table 5.

Certainly these principles cannot be automatically transferred to situations such as those of public order and health, criminal investigations, national security and times of crisis. A central point of much sociological analysis is to call attention to the contextual nature behavior. Yet common sense and common decency argue for the consideration of these principles, absent compelling circumstances.

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.

This article opens with a tongue-in-cheek statement by the novelist Kafka that a new technology, "is a remarkable piece of apparatus." This is from his short story, "The Penal Colony" in which a correctional officer invents a very sophisticated machine for punishing inmates. The story ends with the officer being killed by the machine he created.[6] While it is premature, and perhaps even sacrilegious, to conclude that information technology will destroy, rather than save us, Frankensteinian outcomes are not always figments of the literary or psychoanalytic imagination. Research and vigilance however may work against this.

[1] In particular I draw from Marx, G. T., forthcoming, Windows Into the Soul: Surveillance and Society in an Age of High Technology. Chicago: University of Chicago Press; and "Varieties of Personal Information as Influences on Attitudes Toward Surveillance" forthcoming in R. Ericson and K. Haggerty (eds.) The New Politics of Surveillance and Visibility, University of Toronto Press and various articles at garymarx.net -- "What's New About the New Surveillance?: Classifying for Change and Continuity," Surveillance and Society. vol. 1, no. 1, 2002 (at www.surveillance-and-society.org./);"What's in a Name? Some Reflections on the Sociology of Anonymity," The Information Society, Vol. 15, No. 2, 1999; "An Ethics for the New Surveillance". The Information Society. Vol. 14, no. 3, 1998); "Murky Conceptual Waters: The Public and the Private", Ethics and Information Technology. Vol. 3, no. 3, 2001); "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", Journal of Social Issues, Vol. 59, no. 1, 2002).

[2] One important distinction is between anonymity with respect to core biological identity (e.g., an individual as unique because he or she is born at a particular place and time as a result of the biological uniting of two parents) as linked to a legal identity, as against various other pseudonymous forms of identity such as a national identification number. Pseudonyms may or may not be linked to a given name or location. Sometimes what matters is being able to locate an individual or authenticate some aspect of their identity, rather than literally knowing their core biological/legal identity. This may be for purposes of communication or to deny or grant some form of access or privilege.

[3] Increased freedom of choice can exist with increased volume and intensity of

surveillance. This is merely to suggest that the kinds of information individuals wish to keep private changes with social and cultural change, not that the overall amount we wish to conceal declines. That is an empirical question which must take into account the absolute amount there is to be known about a person, a factor that has markedly increased and continues to increase in recent centuries. New diagnostic means involving DNA and predictive profiles for at risk individuals may create new forms of stigma. The case for a relative increase in surveillance is dependent on the ratios of what there is to be known of interest, what the technology is capable of and the actual extent of its application.

[4] Sex change operations are at one extreme. But more common are the new identities created through the increased intermarriage of ethnically, racially, religiously and nationally distinct groups. An increase in children of mixed marriages, those holding duo-citizenship, immigration, tourism and communities in cyberspace illustrate this. New categories for marginal, hybrid and anomalous groups will appear. As just one example take the millions of Americans who, as products of a mixed marriage, consider themselves *both* Christian and Jewish, White and Black or Asian and Hispanic.

[5] See for example, on computers and society Wiener (1967) and Weizenbaum (1976) and for the environment some of the aphorisms offered by Mander (1992). Many can be seen in discussions of modernism in general (e.g., the analysis in Beninger 1986 and Scott 1998).

[6] Note also Nathaniel Hawthorne's story, "The Birthmark" in which an alchemist in seeking to successfully rid his wife of a small blemish accidentally kills her. The operation was a success but the patient expired.