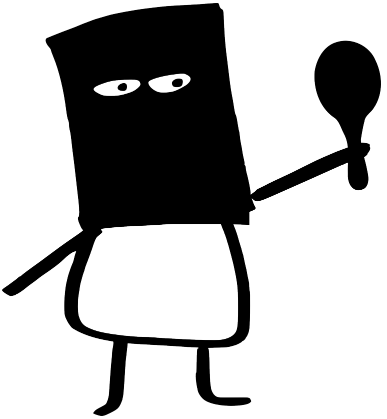
What's in a Name?

Some Reflections
on the Sociology of Anonymity



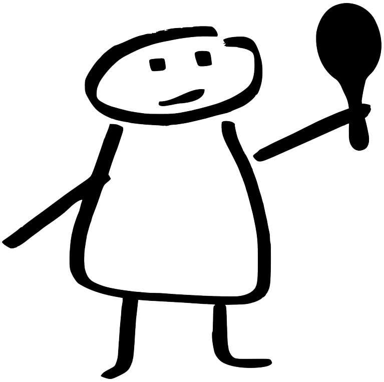
Gary T. Marx
Massachusetts Institute of Technology

"You ought to have some papers to show who you are." The police officer advised me.

"I do not need any paper. I know who I am,"
I said.

"Maybe so. Other people are also interested in knowing who you are."

B. Traven, The Death Ship



Content

What's this about?

A major consequence of new surveillance and communications technologies is the potential both to decrease and increase anonymity. Powerful surveillance technologies can inexpensively, efficiently and silently break through borders that have historically protected anonymity and other aspects of personal information. Anonymity may also be undermined by new biometric forms of identification such as DNA and retinal, voice and olfactory patterns. The ease of merging previously unrelated data and creating permanent records via audio and video recordings may also reduce the de facto anonymity which resulted from the absence of an observer, the failure of memory and weak means of data analysis. The "ocular proof" demanded by Othello of his wife's infidelity comes in an ever expanding variety of forms.

In contrast, new ways of communicating using encryption and through Internet services which offer the opportunity to use pseudonyms and forwarding services which strip all identifying marks, may increase some forms of anonymity. The personal identity of interlocutors is more difficult to ascertain absent other sensory cues or codes for authentication. The newness also means that neither formal nor informal norms have sufficiently developed.

The issue of anonymous communication on the net is part of a broader set of surveillance issues that includes the ubiquitous "cookies" question as well (cookies are remote programs that can monitor web page user's on-line behavior and can even invade their hard drive without their knowledge or consent). These in turn are part of the still larger issue of visibility and insulation in a society undergoing rapid technological change.

To paraphrase Mark Twain, reports of either the recent death or coming dominance of anonymity have been greatly exaggerated. We are as ill-served by sweeping statements about the end of privacy as we are about the appearance of a golden age of technologically protected communication. The systematic study of computers, privacy and anonymity is in its infancy. Conceptually the multiple dimensions involved here have not been specified, nor of course have they been measured in a systematic empirical fashion that would permit reaching broad conclusions. The situation is also dynamic --research documenting a clear problem (or its absence) can be a factor in subsequent developments.

This paper lays out some of the conceptual landscape surrounding anonymity and identifiability in contemporary society. The emphasis is on the cultural level --on normative expectations and justifications, more than on describing actual behavior. It is also on the anonymity of individuals rather than of groups or organizations (of course these may be linked as with infiltrators using pseudonyms working for false front intelligence agencies).

I offer some definitions and conceptual distinctions and identify seven dimensions of identity knowledge. I specify social settings where the opposing values of anonymity or identifiability are required by law, policy, or social expectations. I then suggest thirteen questions reflecting several ethical traditions to guide policy development and assessment in this area. While the tone of the paper is tentative in the face of the rapidity of change and the complexity of the issues, I conclude by offering one broad principle involving truth in the nature of naming that I think should apply to computer mediated personal communications.

Definitions and Concepts

Let us first define anonymity and relate it to privacy, confidentiality, and secrecy. Anonymity is one polar value of a broad dimension of identifiability vs. non-identifiability. To be fully anonymous means that a person can not be identified according to any of the seven dimensions of identity knowledge to be discussed below. This in turn is part of a broader variable involving the concealment and revelation of personal information and of information more generally.

Identity knowledge is an aspect of informational privacy. The latter involves the expectation that individuals should be able to control information about themselves. Privacy can be differentiated from confidentiality which involves a relationship of trust between two or more people in which personal information is known, but is not to be revealed to others, or is to be revealed only under restricted conditions. Secrecy refers to a broader category of information protection. It can refer to both withholding the fact that particular information exists (e.g., that a pseudonym is in use) and to its content.

Ironically anonymity is fundamentally social. Anonymity requires an audience of at least one person. One can not be anonymous on top of a mountain if there is no form of interaction with others and if no one is aware of the person. Compare the solitude of the Beach Boys' song "In My Room", a lonely, introspective, plaintive to unrequited love to Petula

Clark's desire to experience the freedom of being "Downtown" where "no one knows your name". While similar, only the latter is an example of anonymity.

7 Types of Identity Knowledge

Identity knowledge has multiple components and there are degrees of identifiability. At least 7 broad types of identity knowledge can be specified. (table 1) These are 1) legal name 2) locatability 3) pseudonyms that can be linked to legal name and/or locatability --literally a form of pseudo-anonymity 4) pseudonyms that can not be linked to other forms of identity knowledge --the equivalent of "real" anonymity (except that the name chosen may hint at some aspects of "real" identity 5) pattern knowledge 6) social categorization 7) symbols of eligibility/non-eligibility.

1. identification may involve a person's legal name. Even though names such as John Smith may be widely shared, the assumption is made that there is only one John Smith born to particular parents at a given time and place. Name usually involves connection to a biological or social lineage and can be a key to a vast amount of other information. It tends to convey a literal meaning (e.g., the child of Joseph and Mary). This aspect of identification is usually the answer to the question "who are you?" The use of first names only, as was said to traditionally be the case for both providers and clients in houses of ill repute, can offer partial anonymity. The

question of whether full, last, first, or no name is expected in social settings may appear to be a trivial issue that only a sociologist could love. But it is in fact the kind of little detail in which big social meanings may reside.

2. identification can refer to a person's address. This involves location and "reach ability", whether in actual or cyberspace (a telephone number, a mail or E-mail address, an account number). This need not involve knowing the actual identity or even a pseudonym. But it does involve the ability to locate and take various forms of action such as blocking, granting access, delivering or picking up, charging, penalizing, rewarding or apprehending. It answers a "where" rather than a "who" question. This can be complicated by more than one person using the same address.

3. identification may involve alphabetic or numerical symbols such as a social security number or biometric patterns or pseudonyms which can be linked back to a person or an address under restricted conditions. A trusted intermediary and confidentiality are often involved here. These in effect create a buffer and are a compromise solution in which some protection is given to literal identity or location, while meeting needs for some degree of identification. As with name, the symbol is intended to refer to only one individual (but unlike a given name which can be shared, letters and numbers are sufficient as unique identifiers. Whereas when there

is more than one John Smith in question unique identity requires matching to other aspects of identity such as birth date and parents or address). Examples include the number given persons calling tip hot-lines for a reward, anonymous bank accounts, on-line services that permit the use of pseudonyms in chat rooms and on bulletin boards and representations of biometric patterns.

4. identification may involve symbols, names or pseudonyms which can not in the normal course of events be linked back to a person or an address by intermediaries. This may be because of a protective policy against collecting the information. For example in some states those tested for AIDS are given a number and receive results by calling in their number without ever giving their name or address. Or it may be because a duped audience does not know the person they are dealing with is using fraudulent identification, --for example spies, undercover operatives and con-artists.

5. identification may be made by reference to distinctive appearance or behavior patterns of persons whose actual identity or locatability is not known (whether because of the impersonal conditions of urban life or secrecy). Being unnamed is not necessarily the same as being unknown. Some information is always evident in face-to-face interaction because we are all ambulatory autobiographies continuously and unavoidably emitting data for other's senses and machines. The

uncontrollable leakage of some information is a condition of physical and social existence. This has been greatly expanded by new technologies. The patterned conditions of urban life mean that we identify many persons we don't "know" (that is we know neither their names, nor do we know them personally). In everyday encounters (say riding the subway each day at 8 am) we may come to "know" other riders in the sense of recognizing them. Skilled graffiti writers may become well known by their "tags" (signed nicknames) or just their distinctive style, even as their real identity is unknown to most persons[1]. Persons making anonymous postings to a computer bulletin board may come to be "known" by others because of the content, tone or style of their communications. Similarly detectives may attribute re-occurring crimes to a given individual even though they don't know the person's name (e.g., the Unibomber, the Son of Sam, the Red Light Bandit, Jack-the-Ripper). There are also pro-social examples such as anonymous donors with a history of giving in predictable ways which makes them "known" to charities. They are anonymous in the sense that their name and location is not known, but they are different from the anonymous donor who gives only once.

6. identification may involve social categorization. Many sources of identity are social and do not differentiate the individual from others sharing them (e.g., gender,

[1] Jeff Ferrell, Crimes of Style: Urban Graffiti and the Politics of Criminality (Boston: Northeastern University Press, 1996).

ethnicity, religion, age, class, education, region, sexual orientation, linguistic patterns, organizational memberships and classifications, health status, employment, leisure activities). Simply being at certain places at particular times can also be a key to presumed identity.

7. identification may involve certification in which the possession of knowledge (secret passwords, codes) or artifacts (tickets, badges, tattoos, uniforms) or skills (performances such as the ability to swim) labels one as a particular kind of person to be treated in a given away. This is categorical and identifies their possessor as an eligible or ineligible person with no necessary reference to anything more (although the codes and symbols can be highly differentiated with respect to categories of person and levels of eligibility). This is vital to contemporary discussions because it offers a way of balancing control of personal information with legitimate needs such as for reimbursement (e.g., toll roads, phones, photo-copy machines, subways) and excluding system abusers. Smart card technologies with encryption and segmentation make this form of increased importance.

Socially Sanctioned Contexts of Concealment and Revelation

What is the ecology or field of identity revelation/ concealment? How are these distributed in social space and time? What structures and processes can be identified? When and why does society require or expect (whether by laws, policies or manners) that various aspects of identity will not be revealed?

Under what conditions does the opposite apply --that is, when is the revelation of the various aspects of identity expected by law, policy or custom?

The lists that follow, while not exhaustive, hopefully cover the most common contexts in which anonymity and identifiability are viewed as socially desirable. I have classified these by their major justifications[2].

[2] I make these observations as a social observer and not as a moralist or empiricist (in the sense of subjecting claims to some kind of empirical standard). I argue neither that these justifications are necessarily good, nor that the claimed empirical consequences (and no unintended or other consequences) necessarily follow. To have a pony in those races requires analysis beyond the scope of this paper.

Here I simply take claimed justifications at face value and report them. This is a first step to empirically testing such claims. Three additional tasks involve a) trying to find a pattern in the attachment of moral evaluations to the various forms of behavior b) systematically relating the types of identity knowledge to the rationales c) as a citizen taking a moral position on what it is that the society has normatively offered up regarding identity knowledge.

Rationales in Support of (full or partial) Anonymity

1. to facilitate the flow of information and communication on public issues (this is the "if you kill the messenger you won't hear the bad news" rationale). Some examples:

- hot lines for reporting problems and violations, various communication channels for whistle blowers
- witnesses at Congressional hearings or in investigative media reports who are visible behind a screen and whose voice may be electronically distorted
- news media sources such as "deep throat" of Watergate illfame
- unsigned or pseudonymous political communications
- the use of pen names and the nom-de-plume
- groups investigating human rights and other abuses and those reporting to them (including mass media investigative reporters and social reform groups using stings and infiltration)

2. to obtain personal information for research in which persons are assumed not to want to give publicly attributable answers or data. For example:

- studies of sexual and criminal behavior and other social research
- informational audits
- medical research

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. For example:

- persons with a well known public reputation writing in a different area may want to avoid being "type cast", or having their reputations effected or not taken seriously (a professor who writes detective stories, a religious leader who writes about her doubts about religion). In the words of "Anonymous" the author of Primary Colors "I wanted the book to be reviewed, not the author."
- for dramatic reasons to fit cultural images of what a stage name should be or to enhance presumed marketability as with film stars changing ethnic minority names to short Anglicized names (Bernard Schwartz to Tony Curtis, Issur Danielovitch to Isidore Demsky to Kirk Douglas, or strippers with names such as Candy Barr, Blaze Star and Beverly Hills.

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. Some examples:

- self-help requests and discussion and support groups for alcohol, drug, and family abuse, sexual identity, mental and physical illness
- tests for AIDS and other socially transmitted sexual diseases, pregnancy

- sociability experiences among persons who are shy or uncomfortable in face-to-face interaction
- communicating about personal problems and issues with technologically distanced (and presumably safer) strangers[3].
- posting personal information such as course grades in a public place using student ID numbers

5. to obtain a resource or encourage a condition using means that involve illegality or are morally impugnable, but in which the goal sought is seen as the lesser evil. For example:

- amnesty programs for the return of contraband (guns, stolen goods) "no questions asked"
- needle exchange programs
- spies and undercover operatives (including on-line stings using pseudonyms)
- the Federal Witness Protection Program.

6. to protect donors of a resource or those taking action seen as necessary but unpopular from subsequent obligations, demands, labeling, entanglements or retribution. Some examples:

- anonymous gift giving to charitable organizations in which donors are protected from additional demands or advertising their wealth. The Judaeo-Christian ethic which makes virtue its own reward supports this. The

[3] See for example the discussion in Mary Virnoche "When A Stranger Calls: Strange Making Technologies and the Transformation of the Stranger"; paper delivered at the Pacific Sociological Association Meetings, 1997.

"secret Santa" in which persons bring anonymous gifts to be randomly distributed is one variant

- sperm and egg donors, birth parents giving a child up for adoption
- hiding the identity of judges of competitions and in courts to protect them from inappropriate influence (whether persuasion, coercion or bribes) and retribution
- hangmen in England wore hoods, in part to protect them from retaliation but perhaps also to enhance the drama
- identification numbers rather than names worn by police

7. to protect strategic economic interests, whether as a buyer or a seller. For example a developer may be quietly purchasing small parcels of land under an assumed name or names, in preparation for a coming development (a shopping mall, university expansion, transportation system) that has not been publicly announced. A company in financial difficulty may attempt to sell goods or services under another name to avoid letting customers know how desperate it is to sell. In silent (or loud) auctions bidders are identified by a number and in the latter case it may not be known who the person holding the number represents. The autonomy of individual consumers may be enhanced when they pay with cash or a money order, rather than an identity-revealing check, credit or frequent shopper card. When merchants can use fine-grained data mining

programs that correlate personal characteristics of the consumer, context of purchase and bar-coded sales, consumers may be more subject to manipulation. The gap here between being known only as "occupant" vs. being a participant in a frequent shopper program is large (although for some persons this is compensated for by savings and individualized information re their consumption interests)

8. to protect one's time, space and person from unwanted intrusions. For example:

- unlisted phone numbers
- opposition to caller-ID unless there is a blocking option
- women using a neutral or male name or an initial rather than a first name in phone and other directories, or wearing a veil or clothes that conceal feminine distinctiveness
- post office box addresses identified only by number
- mail forward services
- providing only minimal information on warranty cards
- giving a fake name, or refusing to give one's name when seeking commercial information
- celebrities who don't want to be recognized using assumed names and the cliche of wearing dark glasses

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. For example:

- having musicians competing for orchestra positions perform behind a screen so that judges can not see them
- the blind reviewing of articles for scholarly journals or grading student exams
- reviewing college applications with names and gender deleted

10. to protect reputation and assets. The "theft of identity" and sending of inauthentic messages has emerged as a significant by-product of the expansion of electronically mediated (as against face-to-face) interactions[4]. For example:

- the free service set up by a Florida programmer "FAKEMAIL" in which thousands of bogus e-mail messages were sent out using names such as Bill Clinton
- the spreading of a variety of violations associated with the theft of identity or the creation of fictitious identities (Marx, 1990, Cavoukian 1996)

[4] See for example Gary T. Marx, “Fraudulent Identification and Biography” in D. Altheide, et al, editor. New Directions in the Study of Law, Social Control (New York: Plenum, 1990) and Ann Cavoukian, The Theft of Identity (Ontario, Canada: Office of the Privacy Commissioner, Ontario, Canada, 1996).

11. to avoid persecution. For example

- runaway slaves
- Jews, Romanies, leftists, homosexuals during the Nazi period
- those subject to human rights violations by repressive regimes

12. to enhance rituals, games, play and celebrations. Letting loose, pretending and playing new roles are seen as factors in mental and social health. Part of the fun and suspense of the game is not knowing who. For example:

- Halloween masks, masked balls, costume parties, role reversal rituals in traditional societies reflect this. Mardi Gras celebrations that involve masks and cross-dressing are an example.
- the preparations around surprise parties and some of the actual guests (though in this case there may be a move from anonymity or a deceptive ID to actual identification at the gathering)
- some board and computer games involve lack of clarity as to identity (either or both the real identity of the players and hidden identity in the game), on line role-playing and fantasy in which service providers offer a limited number of pseudonyms

13. to encourage experimentation and risk taking without facing large consequences, risk of failure or embarrassment since one's identity is protected. This is a kind of cost-free test drive of alternative identities, behavior and reading

material (the anti-chill justification). For example:

- pretending to be of a different gender, ethnicity, sexual preference, political persuasion etc. in on-line communication
- commercial invitations to try a product or service free for a limited period of time (although of course there is likely to be at least some identity trail here)

14. to protect personhood or "it's none of your business". What is central here is not some instrumental goal as with most of the above, but simply the autonomy of the person. This can be an aspect of manners and involves an expectation of anonymity as part of respect for the dignity of the person and recognition of the fact that the revelation of personal information is tied to intimacy[5]. While the revelation of name, address or phone number is hardly an act of profound intimacy, it is none-the-less personal. In many contexts, particularly those in public involving secondary or formal relations, the decision to reveal these is up to the individual and can be viewed as a kind of currency exchange, (along with other personal information) as trust in a relationship evolves. One shows respect for the other by not asking and the other is permitted the symbolic and instrumental option of being able to volunteer it.

The United States has particularly strong expectations here as seen in the limited conditions under which police can require that persons identify themselves (although the

[5] Gary T. Marx, "New Telecommunication Technologies Require New Manners," Telecommunications Policy 18 (1994): 538-552.

California inspired pseudo-gemeineschaft of "hi I'm Bill your waiter" might seem to contradict that). Behavior as a consumer also fits here. Beyond not wanting to reveal identity information that can be used in marketing, many persons feel that the kinds of liquor, birth control, medicines, magazines, or electronic products they purchase should be revealed at their discretion and not electronically taken from them.

15. traditional expectations. This is a bit different than the above because the custom that is honored does not appear to have emerged from a reasoned policy decision, but rather is an artifact of the way a technology developed or the way group life evolved. This then becomes associated with expectations about what is normal or natural, and hence expected and preferred.
The telephone is a good example. When caller-ID was announced there was significant public resistance because people were accustomed to being able to make a phone call without having to reveal their phone number (and all that could be associated with it.) Caller-ID as it was first offered without blocking changed that. Those who argued against this were often unaware of the historical recency of their ability to phone anonymously. In an earlier time period when all calls went through a local operator, this was not possible. The move to automatic switching was not undertaken to enhance privacy, but because it was more efficient. One's "right" to mail a first class letter anonymously emerged simply because at the time the relevant postal regulations were established the issue of

> accountability of the sender was not seen as relevant. A return address was recommended but that was only as an aide for undeliverable letters (and perhaps as an incentive for recipients who until 1855 had to pay the cost of the letters they received). A postmark has always been required but that appears to be more as a means of holding postal authorities accountable.

Mention may also be made of some related contexts in which anonymity is present simply because the conditions of complex urban life permit it. For example (absent the new technologies), not being easily identified or having to identify oneself when in public is the default condition -- whether sitting on a park bench, walking on a crowded street or cheering in a stadium. Beyond there being no expectation that the individual must identify him or herself in public settings, a request from a stranger for such identification would be taken as unusual and off-putting, as would the stranger's offering of his or her personal identification information, other factors being equal (of course in the quasi-public setting of a singles bar that is not the case).

Here we encounter the interesting case of expectations of privacy in public (Nissenbaum, 1997). There is an irony in norms of privacy having particular cogency in public settings. While not codified, manners in public settings and in encounters with strangers limit what can be asked of the other and support what Erving Goffman terms disattending. One aspect of this is to help others avoid embarrassment and to help sustain a person's self-image and the image presented to others of being a particular kind of person, even when the facts suggest the opposite. Here we may distinguish between not having identity knowledge vs. having it, but pretending that one does not --granting a kind of pseudo-anonymity. This may be to avoid unwanted claims or to collude in helping others maintain a positive image of self. David Karp's (1973) study of the privacy sustaining behavior of patrons and employees in pornographic book stores is an example.

A related case is not taking advantage of available identity information. This factor was emphasized by Simmel (1964) in commenting on the urban dweller's tendency to screen out information and distance one'self from the abundance of sensory stimuli offered by busy city environments.

Another environment where a degree of defacto anonymity exists is in being away from home --whether as a tourist, traveler, or expatriate. Not only is one less likely to be personally known but many of the symbols (accent, dress, body language) that present clues to identity will go uninterpreted or simply serve to put one in the broad class of foreigner. Since the stranger may be seeking this anonymity, locals may have an economic or political interest in granting it. It would be interesting to study isolated areas and frontier towns in this regard. Note places such as the small western town where the fugitive in the novel Falcon and the Snowman[6] was living when he was captured, in which there is a tradition of not asking who people were, or where they came from.

[6] Robert Lindsey, Falcon and Snowman (New York: Simon and Schuster , 1985).

Rationales in Support of Identifiability

A consideration of contexts and rationales where anonymity is permitted or required must be balanced by a consideration of the opposite. When is identifiability required, expected or permitted?

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. As Scottish moral philosophers such as David Hume argued, human sentiments and social needs favor it. It is more difficult to do ill to others when we know who they are and must face the possibility of confronting them. Mutual revelation is a sign of good faith which makes it easier to trust (not unlike the handshake whose origin reportedly was to show that one was not carrying a weapon). It is a kind of sampling of one's inner-worth or an early showing of part of one's hand. It also makes possible reciprocity, perhaps the most significant of social processes. To paraphrase a line from the film "Love Story" --"being anonymous means you never have to say you are sorry" --and that of course is one of the problems.

Thinking of society without personal identities is like a modern building without a foundation. The number of contexts where it is expected and even required far exceeds those where its opposite is required or expected. Indeed failure to identify one's self often leads to suspicion rather than the reverse. As with the Lone Ranger we ask "who was that masked man?" Just try the simple experiment of wearing a hood or Halloween mask throughout the day and note how it will surface the usually tacit norms regarding identification and a variety of control responses.

Central to many of the contexts where some form of identifiability is required or at least expected we find:

1. to aide in accountability. Saints and those with strongly internalized moral codes respect the rules regardless of whether or not they are watched (or potentially locatable). But for others who can resist anything but temptation, especially if under cover of anonymity, this is less likely. Because individuals generally want others to think well of them and/or to avoid negative sanctions, normative behavior is more likely when people are identifiable. One extreme form is the anti-mask laws of some states (adopted as an anti-KKK strategy). The numbers on police badges are intended to hold police accountable while creating a buffer in their personal life from irate citizens. Contrast that with the names worn by airlines clerks and on the legitimacy-confirming badges of door-to-door solicitors. The current emphasis on identifying and tracking absent fathers with children supported by welfare is another example of accountability.

2. to judge reputation. In contrast to the small homogeneous group without strangers, mass

impersonal societies rely on name and the records and recommendations it can be associated with, to determine personal qualities. In small communities where membership itself is a form of vouching these are taken for granted.

3. to pay dues or receive just deserts. Reciprocity is among the most fundamental of social forms and it requires being able to locate those we interact with. An identity peg makes it possible to have guarantees (such as collateral for a loan), to extract payments (of whatever sort) and to distribute justice and rewards, although this need not always involve literal identity.

4. to aide efficiency and improve service. The modern ethos and competitive environments view knowledge as power and generate seemingly insatiable organizational appetites for personal information to serve organizational ends and in their words "to better serve the customer". The extent of this was brought home to me recently when I purchased some batteries at Radio Shack with cash and was asked for my phone number. Perhaps the case was stronger with the dry cleaners I next took my clothes to (although the numbered receipt had always been sufficient before). The clerk's matter-of-fact manner in asking for my name and phone number and cheery response "you are a new customer aren't you?" overwhelmed whatever hesitancy I might have had about giving out an unlisted number. But it did not begin to match my

surprise when a waiter looking down at his hand-held computer at a restaurant I had not been to for six months asked, "would you like the salmon you had last time"? The over-stuffed warranty cards we are asked to fill out offer another example.

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). Administrative needs in a complex division of labor require differentiation and complex norm enforcement, which in turn may depend on personal characteristics linked to name and place. a characteristic of modern society is ever increased differentiation and the proliferation of fine-grained categories for treating persons and of requirements for being able to perform various roles. This is believed to involve both efficiency and justice. These require unique identities, although not necessarily actual name. But the latter is seen to enhance validity beyond being an organizational peg. Compare for example the evolution of the contemporary wallet with its space for multiple cards, with the paucity of identification documents required in the 19th century and earlier, simpler carrying devices.

6. to guarantee interactions that are distanced or mediated by time and space. This is the case with ordering by credit card or paying with a check rather than cash (of course various types of impersonal

vouchers such as a postal mail order offer alternatives). However even in the latter case an address is frequently needed to deliver goods or to handle complaints and disputes. It used to be that one could simply call and make a restaurant reservation (often using as a nom-de-plume the name of a famous scholar or author). Then restaurants began asking for phone numbers and now some even require a credit card number to hold the place. Such identity becomes an alternative to the generalized trust more characteristic of small communities.

7. to aide research. Research may benefit from links to other types of personal data. Longitudinal research may require tracking unique individuals although identity can be masked with statistical techniques as a recent National Academy of Sciences (1995) study recommends.

8. to protect health and consumers. Health and consumer protection may require identifying individuals with particular predispositions or experiences such as exposure to a substance discovered to be toxic or purchasers of a product later found to have a safety defect. Concern over genetic predispositions to illness may be one reason why records are kept (if often confidential) of sperm and egg donors or birth parents giving a child up for adoption. The need to identify persons in death (as with the DNA samples required of those in the military) which are to be used only for that

purpose, or to obtain personal information helpful in a medical emergency are other examples.

9. to aid in relationship building. The currency of friendship and intimacy is a reciprocal, gradual revealing of personal information that starts with name and location. Here information is a resource like a down payment, but it also has a symbolic meaning beyond its specific content.

10. to aid in social orientation. It used to be said at baseball stadiums, "You can't tell the players without a program" (although we have seen a move from numbers to names on jerseys). More broadly social orientation to strangers and social regulation are aided by the clues about other aspects of identity presumed to be revealed by name and location (e.g., ethnicity, religion, life style).

But is it Good or Bad?

You've got to accentuate the positive
eliminate the negative
and look out for Mr. In-Between

1950s popular song

Easier sung than done. The key issue for ethics and public policy is under what conditions is it right or wrong to favor anonymity or identifiability? As the examples above suggest there are many contexts in which most persons would agree that some form of anonymity or identifiability is desirable. But there are others where we encounter a thicket of moral ambiguity and competing rationales and where a balancing act may be called for.

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 which 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 wonderful cartoon shows 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 empirical truths on both sides and differing value priorities. Being able to disentangle these is vital for our understanding and for developing policy.

One Size Does Not Fit All: Some Questions to Inform Policy Formation

I cast a broad net above in order to help locate networked communication within a wider social context. Apart from the value conflicts, one can hardly move directly to clarion guidelines from this for a number of reasons involving the great variety with respect to:

1. types and degrees of identity knowledge
2. 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)
3. 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)
4. types of activity (browsing, requesting information, posting on bulletin boards, E-mail, discussion groups)
5. content/goals (games, self-help groups, hot lines, commerce, politics, science, protecting the sender of a communication or the recipient)
6. the national and cultural borders that communication invisibly crosses andtypes of response (prohibit, require,

> optional but favor or disfavor, laws, policies, manners). Policies will vary and may change as conditions change. Even if one could agree on a computer policy regarding anonymity there is no central net authority to implement it and technically doing this would be difficult.

Laws to set outer limits with sanctions to aid compliance, policy criteria for more focused direction, technologies to protect and authenticate identification and markets to enhance choice all have a role to play, as do manners and custom.

While I don't want to suggest content for a prohibiting or unleashing policy (with one exception), I will remain true to the generalizing impulse by focusing on procedures and criteria for policy development. In that regard, the more one can answer "yes" to the following questions the better a policy regarding identity knowledge is likely to be:

These questions embody a variety of ethical rules. Questions 1-6 call for truth in the form of good science and logic. Questions 7-9 draw on utilitarianism in minimizing harm and maximizing benefits. The remaining questions (10-13) put forth ethical principles such as those involving the dignity and rights of the individual.

1. goals ---have the goals sought been clearly stated and weighted?

2. can science save us? ---can a strong empirical and logical case be made that a given policy regarding identifiability will in fact have the broad consequences its' advocates claim?

3. reversibility- if subsequent evidence suggests that undesirable consequences outweigh the desirable can the policy be easily reversed?

4. technical system strength --can the system, whether hardware, software or humanware, in fact deliver on the policy (that is, guarantee anonymity or the authenticity of a communicator's identity)?

5. sanctioning and revelation --If anonymous or pseudo-anonymous users violate the rules are there clear standards and procedures for when they will be cut off and for when (and to whom) pseudo-anonymous identities will be revealed?

6. system tests --are there periodic efforts to test the system's vulnerability and effectiveness and to review the policy?

7. alternatives --if alternative solutions are available that would meet the same ends is this the least costly?

8. unintended consequences --has adequate consideration been given to likely/possible undesirable consequences?

9. third parties ---will innocent third parties not be hurt by the policy and if they will are there ways to mitigate the harm?

10. democratic policy development --have participants played some role in the development of the policy?

11. informed consent --are participants fully appraised of the rules regarding identity knowledge under which the system operates? If they don't like the rules can they find other equivalent places to communicate?

12. golden rule --would the sender of the message be comfortable receiving a message in the same form if the context was reversed?

13. equality --is use of the form of identification equally available to all parties to the communication? Can the recipient respond in kind to the message sender?

Honesty in Cyberspace

The complexities and varied situations should make us suspicious of sweeping imperatives. Policies must be crafted to specific contexts. In the context of one-to-one personal communications in cyberspace, I think a strong case can be made that there should be a truth in the nature of naming policy. Certainly as the above rationales suggest there are many contexts in which persons ought to be free to call themselves whomever they want (assuming they don't steal someone else's identity or use a fictitious identity for the purpose of harming or violating the rights of others). Legal name is not always the preferred form of identity. But if there is not to be honesty in identification, then there should at least be honesty in indicating that a pseudonym is used.

If one is anonymous or uses a name that is obviously not one's legal name ("Minnie Mouse" "the Red Baron", "Ernest Hemingway") or in which there is no pretense to genuine identity (e.g., initials or first names or 007) or is in a setting where all participants know the use of pseudonyms is accepted or even expected, this is not an issue. However in most other contexts of personal relations where regular sounding first and last names are used as pseudonyms, our culture has embedded "identity norms" about authenticity in personal interaction. (Goffman 1961)

Absent special conditions, people are expected to be who they claim to be. When a false name is used and discovered, as in the extreme case with con artists, the problem is not only material loss, but the sense of being duped and even betrayed. To pretend to be another is to deceive the actor and audience. It is unfair in introducing inequality into what should be an equal, reciprocal relationship (the deceiver knows your name and that he or she is deceiving you, but you don't know that, nor do you know the real name of the deceiver). I think respect for the person being communicated with and their expectation that they will not be deceived should outweigh any freedom and liberty claims of the secret user of a pseudonym.

The fact that cyberspace makes it so relatively easy to secretly use pseudonyms in personal communications is hardly a justification, even if it is a temptation. I do not argue against the use of pseudonyms or means of identification other than legal name in personal communication, but recipients of the communication should be informed when such is the case. Certainly in many contexts what matters is continuity of personhood and the validity of the claims the individual makes (whether of the ability to pay for something or their access to relevant resources or of their expertise and experience) and their legitimacy to perform a particular role. Legal name may be irrelevant but verification is not. The crucial issue then becomes authentication of the pseudonmity. Smart cards and new crypto protocols may make this easier.

Modern technology offers a variety of ways of uncoupling verification from unique identity. Validity, authenticity, and eligibility can be determined without having to know a person's name or location. Public policy debates will increasingly focus on when verification with anonymity is or is not appropriate and on various intermediary mechanisms that offer pseudonymous buffers but not full severance. Since the cognitive appetite is difficult to sate, organizations will push for more rather than less information on individuals although they will not necessarily want to share their information with each other.

But the availability of new technologies does not negate my argument against deception in those contexts where a realistic sounding name is offered in personal communication (of course one can also make problematic just when a communication is personal).

Knowing that a pseudonym is in use permits speculation as to whether or not this is appropriate and if it isn't, why the veil might be in place and discounting, or qualifying, the message. Such forewarning will often suggest the need for greater caution than when a person's actual name is used. In face-to-face interaction we have visual and auditory cues to assess strangers, even then common-sense advises caution. How much truer that is when we lack these in cyberspace and have even less grounds for knowing the identity of strangers and if they are who they claim to be. Good manners (and in some contexts the law) requires not deceiving those we interact with about our identity. If this holds for conventional interactions it should also hold for those mediated by technology. We are entitled to know when we are dealing with a pseudonymous identity in personal communications.

In presenting this paper the truth in the nature of naming argument has often been misunderstood. I am not saying that anonymous or pseudonymous communication on the net should be banned. I am saying that if the latter is present in personal communications, then the recipient has a right to be informed of it. This does not go as far as some computer networks such as the WELL which have a policy against any anonymous or pseudonymous communication. Certainly the latter can be a means of protecting one's privacy in interactions with organizations, or when one is seeking information from a web cite. Those contexts however are different from personal communications.

As the competing rationales discussed above suggest, there are value conflicts (and conflicting needs and consequences) here which make it difficult to take a broad and consistent position in favor of or against anonymity. To list only some of these:

1. liberty and order
2. accountability and privacy,
3. community and individualism,
4. freedom of expression and the right not to be defamed or harassed,

5. honesty in communications and civility/diplomacy,
6. creativity and experimentation vs. exploitation and irresponsible behavior,
7. encouragement of whistle-blowing and due process,
8. the right to know and the right to control personal information
9. the universalistic treatment due citizens and the efficiency of fine-honed personal differentiations,
10. the desire to be noticed and the need to be left alone.

Whatever action is taken there are likely costs and gains. At best we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point. Continued empirical research and policy and ethical analysis are central to this. The process of continual intellectual engagement with the issues is as important as the content of the solutions.

Tables

TABLE I - Types of Identity Knowledge

1. legal name
2. locatability
3. pseudonyms linked to name or location
4. pseudonyms that are not linked to name or location
    a. for policy reasons
    b. audience does not realize it's a pseudonym
5. pattern knowledge
6. social categorization
7. symbols of eligibility/non-eligibility

TABLE II - Rationales for Anonymity

1. to facilitate the flow of information
2. to obtain personal information for research
3. to encourage attention to the content of the message
4. to encourage reporting, information seeking and self-help
5. to obtain a resource or encourage action involving illegality
6. to protect donors or those taking controversial but socially useful action
7. to protect strategic economic interests
8. to protect one's time, space and person
9. to aid judgements based on specified criteria
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
14. to protect personhood
15. traditional expectations

TABLE III - Rationales for Identifiability

1. accountability
2. reputation
3. dues paying and just deserts
4. organizational appetites
5. bureaucratic eligibility
6. interaction mediated by space and time
7. longitudinal research
8. health and consumer protection
9. currency of friendship and intimacy
10. social orientation to strangers

TABLE IV - Questions to Aid Policy Development Regarding Identity Knowledge and Networked Communications

1. goals ---have the goals sought been clearly stated and weighed?

2. can science save us? ---can a strong empirical and logical case be made that a given policy regarding identifiability will in fact have the broad consequences its' advocates claim?

3. reversibility --if subsequent evidence suggests that undesirable consequences outweigh the desirable can the policy be easily reversed?

4. technical system strength --can the system (whether hardware, software or humanware) in fact deliver on the policy (that is guarantee anonymity or the authenticity of a communicator's identity)?

5. sanctioning and revelation --If anonymous or pseudo-anonymous users violate the rules are there clear standards and procedures for when they will be cut off and for when (and to whom) pseudo-anonymous identities will be revealed?

6. system tests --are there periodic efforts to test the system's vulnerability and effectiveness and to review the policy?

7. alternatives --if alternative solutions are available that would meet the same ends is this the least costly?

8. unintended consequences --has adequate consideration been given to likely/possible undesirable consequences?

9. third parties ---will innocent third parties not be hurt by the policy and if they will are there ways to mitigate the harm?

10. democratic party development --have participants played some role in the development of the policy?

11. informed consent --are participants fully appraised of the rules regarding identity knowledge under which the system operates? If they don't like the rules can they find other equivalent places to communicate?

12. golden rule --would the sender of the message be comfortable receiving a message in the same form if the context was reversed?

13. equality --is use of the form of identification equally available to all parties to the communication? Can the recipient respond in kind to the message sender?

Abstract

To paraphrase Mark Twain, reports of either the recent death or coming dominance of anonymity have been greatly exaggerated. This paper is a beginning effort to lay out some of the conceptual landscape needed to better understand anonymity and identifiability in contemporary life. I suggest 7 types of identity knowledge involving legal name, location, symbols linked and not linked back to these through intermediaries, distinctive appearance and behavior patterns, social categorization and certification via knowledge or artifacts. I identify a number of major rationales and contexts for anonymity (free flow of communication, protection, experimentation) and identifiability (e.g., accountability, reciprocity, eligibility) and suggest a principle of truth in the nature of naming which holds that those who use pseudonyms on the Internet in personal communications have an obligation to indicate they are doing so. I also suggest 13 procedural questions to guide the development and assessment of any internet policy regarding anonymity.

Gary T. Marx was a fellow at the Woodrow Wilson International Center for Scholars, Washington D.C. to whom he is grateful for the wonderful environment in which this paper was prepared. He is also grateful to Terry Bynum and Ann Wood for their extensive comments and to several "anonymous" reviewers for this journal.

Versions of this paper were delivered at a conference on Anonymous Communication on the Net, Irvine, California, American Association for the Advancement of Science, Nov. 1997 and at their annual meetings in Philadelphia. This draws from a forthcoming book Windows Into the Soul: Surveillance and Society in an Age of High Technology, based on the American Sociological Association-Duke University Jensen Lectures.