What's in a Name? Some Reflections on the Sociology of Anonymity

Gary T. Marx

Department of Sociology, University of Colorado, Boulder, Colorado, USA

To paraphrase Mark Twain, reports of either the recent death or coming dominance of anonymity have been greatly exaggerated. This article is a beginning effort to lay out some of the conceptual landscape needed to better understand anonymity and identifiability in contemporary life. I suggest seven 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.

Keywords anonymity, electronic communication, ethics, identification, privacy, pseudonymity, surveillance

Received 25 November 1997; accepted 30 August 1998.

Gary T. Marx was a fellow at the Woodrow Wilson International Center for Scholars, Washington, DC, to whom he is grateful for the wonderful environment in which this article 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, CA, American Association for the Advancement of Science, November 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.

Address correspondence to Gary T. Marx, 4615 New Sweden Avenue, Bainbridge Island, WA 98110, USA. E-mail: Gary.Marx@Colorado.edu. Web: http://socsci.colorado.edu/~marxg/garyhome.html

The Information Society, 15:99–112, 1999

0197-2243/99 $12.00 + .00

> "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*

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.[1] Anonymity may also be undermined by new biometric forms of identification such as DNA, 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 that 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 that 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 a web page user's on-line behavior and can even invade the user's hard drive without the user's 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.[2] 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 article 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.[3] 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 13 questions reflecting several ethical traditions to guide policy development and assessment in this area. While the tone of the article 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 versus nonidentifiability. To be fully anonymous means that a person cannot be identified according to any of the seven dimensions of identity knowledge to be discussed later.[4] This in turn is part of a broader variable involving the concealment and revelation of personal information and of information more generally.[5]

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 cannot 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, plaint 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.[6]

SEVEN TYPES OF IDENTITY KNOWLEDGE

Identity knowledge has multiple components and there are degrees of identifiability. At least seven 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 cannot 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),[7] (5) pattern knowledge, (6) social categorization, and (7) symbols of eligibility/noneligibility.

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

TABLE 1
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/noneligibility

issue that only a sociologist could love.[8] 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 "reachability," 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.[9] It answers a "where" rather than a "who" question.[10] 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 that 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).[11] Examples include the number given to 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 that cannot 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 that the person they are dealing with is using fraudulent identification—for example spies, undercover operatives, and con artists.[12]
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 others' 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 a.m.) 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 (Ferrell, 1996). 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 reoccurring crimes to a given individual even though they don't know the person's name (e.g., the Unabomber, the Son of Sam, the Red Light Bandit, Jack the Ripper). There are also prosocial examples, such as anonymous donors with a history of giving in predictable ways that 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, 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 way. This is categorical and identifies the 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, photocopy

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 (Table 2).

Rationales in Support of (Full or Partial) Anonymity.[13]

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.[14]
   - News media sources such as "Deep Throat" of Watergate ill fame.
   - Unsigned or pseudonymous political communications.[15]
   - The use of pen names and the nom de plume.[16]
   - 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.[17]
   - 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 "typecast" or having their reputations affected 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." Another example is 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).[18]
4. To encourage reporting, information seeking, communicating, sharing, and self help for conditions that are stigmatizing and/or that can put the person at a strategic disadvantage or are simply very personal. Some examples are:
   - 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 (Virnoche, 1997).

TABLE 2
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 judgments 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

- Posting personal information such as course grades in a public place using student ID numbers.[19]

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 are:
   - Anonymous gift giving to charitable organizations in which donors are protected from additional demands or advertising their wealth. The Judeo-Christian ethic, which makes virtue its own reward, supports this. The "secret Santa," in which persons bring anonymous gifts to be randomly distributed, is a variant.[20]
   - 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.[21]
   - 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 card, or frequent shopper card. When merchants can use fine-grained data-mining programs that correlate personal characteristics of the consumer, context of purchase, and barcoded sales, consumers may be more subject to manipulation. The gap here between being known only as "occupant" versus being a participant in a frequent shopper program is large (although for some persons this is compensated for by savings and individualized information about their consumption interests).
8. To protect one's time, space, and person from unwanted intrusions.[22] For example:
   - Unlisted phone numbers.
   - Opposition to caller-ID unless there is a blocking option.[23]
   - Women using a neutral or male name or an initial rather 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.[24]
   - Providing only minimal information on warranty cards.[25]
   - 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 cliché of wearing dark glasses.[26]
9. To increase the likelihood that judgments 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.[27]
   - The blind reviewing of articles for scholarly journals or grading student exams.
   - Reviewing college applications with names and gender deleted.[28]
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 (vs. face-to-face) interactions. 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).

11. To avoid persecution. For example:
    - Runaway slaves.
    - Jews, Romanies, leftists, and 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).[29]
    - 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 preceding items, 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 (Marx, 1994). While the revelation of name, address, or phone number is hardly an act of profound intimacy, it is nonetheless 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 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 from the preceding item 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 it could be associated with). 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.[30] 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 aid 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.[31] 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,[32] 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 (1963) 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 versus having it but pretending that one does not—granting a kind of pseudoanonymity. 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 oneself from the abundance of sensory stimuli offered by busy city environments.

Another environment where a degree of de facto 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.[33] 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 the small Western town where the fugitive in the novel *The Falcon and the Snowman* lived (Lindsey, 1985) and was eventually captured, in which there was a tradition of not asking who people were, or where they came from.

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 that 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.

TABLE 3
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

Thinking of society without personal identities is like a modern building without a foundation. The number of contexts where identity is expected and even required far exceeds those where its opposite is required or expected. Indeed, failure to identify oneself 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[34] (Table 3):

1. To aid in accountability.[35] 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 antimask laws of

some states (adopted as an anti-Ku Klux Klan 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 airline clerks and on the legitimacy-confirming badges of door-to-door solicitors.[36] 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 aid 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."[37] 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.[38] 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 overstuffed 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,[39] 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 names. 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 aid 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,[40] which are to be used only for that purpose) and the need 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 preceding examples 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 cannot live with each other, but neither can they live apart. The issue becomes, under what conditions do they coexist? 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 versus 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 versus 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 that 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 have cast a broad net 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 nonreciprocal, 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.[41]
7. Types 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.[42]

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) pseudoanonymous 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 CYBERSAPCE

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 preceding 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, 1963).

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.[43]

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 of access to relevant resources or of expertise and experience) and the person's legitimacy to perform a particular role. Legal name may be irrelevant, but verification is not. The crucial issue then becomes

authentication of the pseudonymity. 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) require 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 commnunications.[44]

In presenting this article, 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 site. Those contexts, however, are different from personal communications.

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

- Liberty and order.
- Accountability and privacy.
- Community and individualism.
- Freedom of expression and the right not to be defamed or harassed.
- Honesty in communications and civility/diplomacy.
- Creativity and experimentation versus exploitation and irresponsible behavior.
- Encouragement of whistle-blowing and due process.
- The right to know and the right to control personal information.
- The universalistic treatment due citizens and the efficiency of fine-honed personal differentiations.
- 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.

NOTES

1. A more developed statement of the new surveillance and its expression in the maximum security society is in Marx (1988, chap. 10). See also the discussions in Rule (1973), Foucault (1977), Laudon (1986), Clarke (1988), Gandy (1993), and Lyon (1994; Lyon & Zureik, 1996).

2. One point noted by neither the "Chicken Littles" nor the "Candides" is that in a free-market economy these move in tandem, if with lags. Caller-ID brings caller-ID blocks, anonymous forwarding services, and call forwarding (which means that the caller no longer knows where the person called really is, even though they have a number by which the person can be reached). The initial easy overhearing of cell and cordless radio phone transmissions was soon made more difficult by adding encryption.

3. The holding of cultural beliefs can of course be seen as a kind of behavior and the beliefs I describe are inferred from behavior. This article suggests the kinds of quantitative data that ought to be gathered on actual behavior.

4. It would be easier to just use "anonymity," but that can lead us to ignore the fact that there are continua with multiple dimensions and that our knowledge will be deeper if we contrast it to "identifiability". The term *identity knowledge* is intended to include both and is less cumbersome than "anonymity–identifiability." Identity data might also be used.

5. This topic is an important strand of the sociology of personal information, which is part of the broader subfield of the sociology of information, which nestles within the still wider field of the sociology of knowledge. Current developments in the area of personal identification are a droplet in the sea change of information collection, processing, and communication we are currently experiencing. Developments in biometric identification and smart card technology along with globalization bring these issues to the surface. The debate over national ID cards is one element of this (Bennett, 1997; Davies, 1995).

6. There may be a rough parallel here to the question, "Is there a sound if a tree falls in the forest and no one is there to hear it?" I don't know, but I do know that for anonymity to be present there must be a person aware of the presence of another, or of actions for whom the identity of the responsible agent is unknown. Sometimes, of course, it is not clear whether a human agent is responsible, as with some livestock killings. In rare contexts of intrigue and conspiracy, "finding the guy behind the guy" is like peeling an onion or nested Russian dolls in which there is infinite regress, and like soap bubbles they evaporate in your hand just as you think you have grasped them.

7. Undercover operatives, for example, are encouraged to take names close to their own. Gordon was originally an Anglo-Saxon name but it became so popular with Jewish name changers that it came to be seen by many persons as a Jewish name (Kaplan & Bernays, 1997).

8. Class and status issues apply here. For example, in 19th-century Britain some upper-class persons referred to their servants with generic names (thus butlers might be called Fred). Referring to Afro-Americans as "boy" or "girl" is related. This, like the uniforms of total institutions, dehumanizes in its massification and failure to uniquely identify and implicitly denies that there is anything worthy of unique note about the person. But in offering a kind of anonymity it also tilts toward privacy.

9. The anonymous Finnish remailing service of Johan Helsingius, for example, permitted recipients of anonymous communication to respond. The name of the anonymous sender was known but kept secret (at least until Helsingius responded to a police request for the name of a user posting information about the Church of Scientology). In contrast, a California call-forwarding service (an anti-caller-ID device) automatically erases the originating phone number. The need to bill clients may make masking identity more difficult.

10. The "where" question need not be linked with the "who" question. Thus the identity of fugitives is known but not how they can be reached. Even with both known they may be unreachable, as when there is no extradition treaty or they are otherwise protected. For example the United States knew that Robert Vesco was in Cuba but was unable to arrest him there.

11. In "Doin' My Time" Johnny Cash sings, "On this old rock pile, with a ball and chain, they call me by a number, not a name." While more precise and distinctive, the number may be experienced as dehumanizing in its failure to more directly convey meaning. It is quicker and easier to know people by their names than by a number. This may be part of a strategy of control, as in total institutions (Goffman, 1961). Yet unlike other tactics such as wearing uniforms or shaving heads, this remains a unique identifier even as its compulsory nature symbolically reflects power differences.

12. Marx (1990) considers the stimulus to fraudulent identification from recent developments in communications technology.

13. 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 article. 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 (1) trying to find a pattern in the attachment of moral evaluations to the various forms of behavior, (2) sytematically relating the types of identity knowledge in Table 1 to the rationales in Tables 2 and 3, and (3) as a citizen taking a moral position on what it is that the society has normatively offered up regarding identity knowledge.

14. Court testimony is an interesting contrasting case. In general, witnesses must be identified and one has the right to confront accusers. This is a response to the historic star-chamber, inquisition, and witch-hunt abuses. This contrasts with the grand jury, which does not offer anonymity but does offer confidentiality. Grants of immunity in some ways are functionally equivalent to guarantees of anonymity. British courts sometimes permit witnesses to testify behind a curtain.

15. In *McIntyre, executor of Estate of McIntyre, Deceased v. Ohio Elections Commission*, 19 April 1995, the Supreme Court held that the First Amendment protects the anonymity of political documents and that individuals can not be compelled to reveal their name on such documents. Justice Black in *Talley v. California* 362, U.S. 60,64 (1960) claimed that "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." The *Federalist Papers* are an often cited example. In contrast, Justice Scalia is "sure" that "a person who is required to put his name to a document is much less likely to lie than one who can lie anonymously." To be identified as the author of a document "promot[es] a civil and dignified level of . . . debate" while anonymity "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of anonymity" (*McIntyre* ibid.) It would be useful to submit such claims to systematic empirical test. Both are likely correct, but until the limiting conditions are specified we are left at the level of argument by assertion. A vital distinction is between putting one's name on a document and whether or not that is confidential. It is difficult to argue that one who puts his or her name on a letter of recommendation that will not be treated confidentially "is much less likely to lie."

16. As with political communication, this partly comes under the protection of the First Amendment. The hiding of an author's identity may of course serve other purposes, such as marketing or avoiding prohibitions on writing, as with the black-listed Hollywood writers, or female authors in the 19th century (e.g., George Sands).

17. Protection of human subjects legislation mandates confidentiality, regardless of whether federal funds are involved. This means identity is anonymous for public audiences, even if it may be initially known by the researchers. This example also illustrates how anonymity is a socially determined property of relationships rather than something inherent.

18. A related category is persons who legally change their name. For example, the boyfriend who arranged to have injury done to skater Tonya Harding's rival changed his name after his prison sentence. This becomes the functional equivalent of a pseudonym for persons encountering him who are unaware of the name change. His action led to a lawsuit by a person with the same name as his new one.

19. Here the pseudonym works as a kind of secret code. But when a social security number is used, as it often is, this creates the possibility of theft of ID.

20. Here, however, the goal seems to be more to protect the feelings of those not able to afford expensive gifts than to protect the most privileged. John Marshall's effort to have judges wear black robes as a means of fighting against class distinctions is a related deindividualizing move (Smith, 1996). An interesting contrast is with donors to political campaigns, who must be identified, and the maneuvering around defining what are obviously political groups as nonprofits exempt from taxes and regulation.

21. This is a classic example of the trade-offs with this complicated issue. These advantages may be purchased at a cost of accountability on the judge's part. Note the recent revelations (and retrenchment)

in Peru with respect to "faceless courts" concerned with terrorism in which judges wore hoods or sat behind one-way mirrors. Claims that innocent persons were convicted and unduly severe sentences given out are now being considered by an appeals commission (*New York Times*, 15 October 1997).

22. Of course, for most of these there are also illegitimate reasons for wanting anonymity. But my emphasis here is on socially valued forms of anonymity. Caller-ID is a nice example of the complexity. Certainly abused partners in safe houses should be permitted to have a caller-ID block, while those who have abused them (if under juridical supervision) should be prohibited from having it.

23. The strength of popular sentiment here surprised the phone companies, which initially offered the service with no blocking option.

24. Recent developments such as e-mail and call forwarding are interesting in that although one may be able to "locate" another for communication, that need not imply knowing where they are in a geographic sense. Traditionally with a phone number, area codes and prefixes gave a clue to location, but with call forwarding they no longer do. In the same way, most e-mail systems permit those with an address to use any symbols, whether a name or numbers, as a header, and e-mail may be forwarded without the sender's knowledge. It is interesting that very rarely do individuals use other than their name. That is likely to change as knowledge of how to misuse personal information via computers spreads.

25. I recently purchased an electric razor, which came with a warranty card and 24 marketing research questions to answer. Nowhere does it say that answering the questions is independent of the warranty. In the best democratic tradition, it informs me that "returning this card ensures that your voice will be heard," since "to deliver products that meet your changing needs, we must understand the types of people who buy [our] products." But in much smaller print, which I had to use a magnifying glass to read, "your answers will . . . allow you to receive important mailings and special offers from a number of fine companies whose products and services relate directly to the specific interests, hobbies and other information indicated above." However, there is a chance to "opt out": "Please check here if for some reason you would prefer *not* [their italics] to participate in this opportunity." While I favor democracy, I am not sure my needs are changing, and it is unclear how receiving information from "fine companies" will help with my shaving needs (even if they were changing), nor that in turning down an offer to receive more junk mail I have opted not "to participate in [an] opportunity." The oblique recognition of privacy interests ("if for some reason"), however sugar-coated and adspeak, does acknowledge the possibility of saying "no" to the collection of personal information in irrelevant contexts.

26. But of course there is ambivalence here, and this is time and place specific. Their essence also depends on their being recognized. There are parallels re revelation and concealment for those engaged in illegal activities who also need clients and yet need to be protected. Note both their need and contempt for the paparazzi.

27. Where the proof is in the consumption, as with listening to music or in a pie-eating or wine-tasting contest, this may be a good idea. For many complicated personnel decisions where reputation is a central factor beyond some immediate demonstration of dexterity, it is impossible.

28. A University of California Regent has proposed that these not be factors in admission.

29. The socially elapsed time periods are an interesting variable. Cases where there is an endpoint of revelation differ in important ways from those where the anonymity remains undiscovered or the person behind the mask remains undiscovered.

30. Certainly it is possible to find rationales against unrestricted caller-ID. But these came after the ability to make anonymous phone calls was taken away, rather than being factors that initially produced it.

31. This discussion is generally restricted to contexts of purposive anonymity where a justfication is present or appears after the fact to further justify practices that have been customary. In contrast, in an example of what might be called the unplanned conditions of complicated life, most of the enormous quantity of literary works attributed to "anonymous" are that way not out of an interest in hiding identity, but because the author's name was never recorded or has been lost.

32. This was not the case in the former East Germany, where the Stasi could collect samples of a person's smell by rubbing a park bench with a cloth and storing it for later identification by dogs, should it be necessary.

33. However, from a juridical standpoint, nonnatives (relative to citizens) may also be subject to greater needs to identify themselves at the hands of the state via passports, visas, and identity cards.

34. The list is far from exhaustive, and these may overlap, but I think it does touch the major categories.

35. One related factor noted by Simmel (1964) and documented by contemporary research is the size of the group. Latane and Darley (1970) and later researchers report more responsible bystander behavior with smaller size groups. Of course, the smaller the size, the less likely it is that the individual will be fully anonymous, but size appears to be an independent factor.

36. I have been unable to find a pattern in what telephone receptionists reveal—some will open with a full name, some with only a first name, some with operator 24, and some the company name. If you ask for their name as validation of your call and the information they offered, you may or may not be successful.

37. This contrast highlights another distinction: who offers the rationale, who seeks anonymity or identifiability. In this case an organization's rationale for wanting the information to better serve its ends may conflict with the ends of the individual, who may view this very insatiability as a reason for wanting anonymity. This suggests a fourfold typology involving agreement or disagreement between suppliers and consumers of the information with respect to the desirability of providing or not providing identity information.

38. I assume the request was primarily for record-keeping purposes and was better than asking for social security number. It certainly has no bearing on the quality of the dry cleaning. It may also have been for promotional and marketing research purposes, given the vast data sources accessible from name and phone number.

39. Compare the B. Traven quote at the start of the paper with another foreign traveler's encounter with police: "It's strange . . . how, ever since I discovered that my passport was gone, I've felt only half alive. But it's a very depressing thing in a place like this to have no proof of who you are, you know" (Bowles, 1978, p. 164). Here we see the eternal duality between identity residing in the reflections we obtain from others versus some primordial, presocial self. There is also the interesting case of the "Nansen" passport, which was an official document that said the holder was a person without an official passport.

40. Two marines who refused to provide this were court maritaled. They claimed their DNA was personal and should not be taken from them and doubted it would only be used for the stated purpose.

41. The relative looseness and tolerance of the United States is of note here and may mean higher rates of identity shielding and alteration and greater acceptance of these than is the case in most of the world. The United States makes it easy to hide and change identities relative to Europe and Asia. For example, we do not need to carry and produce a national ID card or register with the local police when we change addresses, we are not given a never-to-be-changed ID number at birth (although recent requirements for children to have social security numbers comes close), and it is legally rather easy to change one's name. The value of a fresh beginning, likely supported by the idea of coming to a new world and the frontier, also supports this. As a result, we may also go to greater lengths to find out who people really are—note greater U.S. reliance on private detectives, undercover operations, and wiretapping. Perhaps as a result, there is a greater appetite for gossip or curiosity about others in the United States than in Europe—note the attention to the sexual activities of celebrities and politicians, the talk-show revelations, and Hollywood-inspired publications such as *Confidential Magazine*. On the other hand, there are the British tabloids and the paparazzi.

42. The discussion that follows is informed by Marx (1998).

43. The more personal and sustained the interaction, the stronger the expectation. Thus, to dress in drag on a public street is different from making social friends in a bar with a person unaware of the deception. To use a non-ethnic-sounding name to avoid employment discrimination is different from using a pseudonym with closefriends.

44. As Bok (1978) argues, honesty ought to be the default value. Where there are exceptions, as with law enforcement or less frequently investigative journalism, the case must be affirmatively made for why an exception is needed, and there must be appropriate reviews, oversight, and minimization of the degree of deception.

REFERENCES

Bennett, C. J. 1997. Pick a card: Surveillance, smart identification and the structure of advanced industrial states. Paper presented at the 1997 Canadian Political Science Association Annual Meetings, St. John's, Newfoundland.

Bok, S. 1978. *Lying: Moral choice in public and private life*. New York: Pantheon.

Bowles, P. 1978. *The sheltering sky*. New York: Ecco Press.

Cavoukian, A. 1996. *The theft of identity*. Office of Privacy Commissioner, Ontario, Canada.

Clarke, R. 1988. Information technology and dataveillance. *Communications of the ACM* 31:29–45.

Davies, S. 1995. *A case of mistaken identity: An international study of identity cards*. Toronto: Information and Privacy Commissioner of Ontario.

Ferrell, J. 1996. *Crimes of style: Urban graffiti and the politics of criminality*. Boston: Northeastern University Press.

Foucault, M. 1977. *Discipline and punish: The birth of the prison*. New York: Vintage.

Gandy, O. 1993. *The panoptic sort*. Boulder, CO: Westview Press.

Goffman, E. 1961. *Asylums: Essays on the social situation of the mental patient*. New York: Anchor.

Goffman, E. 1963. *Stigma: Notes on the management of spoiled identity*. Englewood Cliffs, NJ: Prentice Hall.

Kaplan, J., and Bernays, A. 1997. *The Laguage of Names*. New York: Simon and Schuster.

Karp, D. 1973. Hiding in pornographic bookstores. *Urban Life and Culture* January.

Latane, B., and J. Darley. 1970. *The unresponsive bystander: Why doesn't he help?* New York: Appleton-Century-Crofts.

Laudon, K. 1986. *The dossier society: Value choices in the design of national information systems*. New York: Columbia University Press.

Lindsey, R. 1985. *The falcon and the snowman*. New York: Simon and Schuster.

Lyon, D. 1994. *The electronic eye. The rise of surveillance society*. Cambridge, England: Polity Press.

Lyon, D., and E. Zureik, eds. 1996. *Computers, surveillance and privacy*. Minneapolis: University of Minnesota Press.

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

Marx, G. 1990. Fraudulent identification and biography. In School of Justice Studies, Arizona State University, *New directions in the study of law and social control*. New York: Plenum Press. pp. 143–165.

Marx, G. 1994. New telecommunication technologies require new manners. *Telecommunications Policy* 18:

Marx, G. 1998. An ethics for the new surveillance. *The Information Society* 14(3):171–185.

National Academy of Sciences. 1995. *Private lives and public policies. Confidentiality and access to information in a free society*. Washington, DC: National Academy of Sciences Report.

Nissenbaum, H. 1997. Toward an approach to privacy in public: Challenges of information technology. *Ethics and Behavior* 7(3):

Rule, J. 1973. *Private lives, public surveillance*. London: Allen-Lane.

Simmel, G. 1964. *The sociology of Georg Simmel*, ed. K. Wolff. New York: Free Press.

Smith, R. E. 1996. *John Marshall, definer of a nation*. New York: H. Holt.

Virnoche, M. 1997. When a stranger calls: Strange making technologies and the transformation of the stranger. Paper delivered at Pacific Sociological Association Meetings. San Francisco, CA.