Negotiating the Digital Closet:

Online Pseudonymity and the Politics of Sexual Identity

David J. Phillips
Department of Radio-Television-Film
University of Texas at Austin
CMA6.118
Austin, Texas USA 78722
djp@mail.utexas.edu

Information, Communication, and Society 5 (3)

ABSTRACT

Online surveillance interferes with the individual's ability to control their expressive identity – to determine the scope of the social context in which their activities are to be seen and interpreted. Entrepreneurs have responded to these concerns by offering pseudonymizers, which employ cryptographic techniques to allow users to create several unlinkable personae and choose among them when engaging in various online interactions. This article investigates the tension between pseudonymity as a design paradigm for privacy technologies and as a lived practice for users. Because coming out – strategic revelation and the claiming of identity – has been at the core of the gay liberation movement, this article posits a politically and sexually active gay professional man as an ideal user of pseudonymity software, and places the design logic of pseudonymity within that particular set of social understandings. It reveals the conflicts, contradictions, and tradeoffs inherent in that use. Pseudonymity permits a very strong control of identity. It permits the user to segregate his public performances, and to engage in public debate without fear of bodily retribution. However, it is all but useless as a means of controlling social context of those performances. It requires that decisions about self-presentation in certain contexts be made in ignorance of who is sharing that context, and with what resources or purpose. While it promotes the production of multiple selves, those selves are not easily lent to practices of intimacy or community. Pseudonymity also facilitates profiling practices which define and reify classes of people, even as it protects the individual from some of the repercussions of being defined as part of that class. In short, pseudonymity software is informed by a politics of heroics rather than of community.

KEYWORDS

pseudonymity, privacy enhancing technology, gay and lesbian, sexual identity, identity management, personally identifiable information

INTRODUCTION

With increased public use of the Internet, privacy issues have gained social salience. Web site operators are able to profile each visitor's browsing activities (Bennett 2001). Regulations covering domain name registration require that registrant's name, address, and phone numbers be publicly available, and, in common practice, automatically searchable (Froomkin 2000: 25). Both in the U.S. and Europe, new laws permit simplified access for police agencies to ISPs' records of their clients online behavior (Electronic Frontier Foundation 2001). These developments interfere with the individual's ability to control their expressive identity – to determine the scope of the social context in which their activities are to be seen and interpreted (Rosen 2000). The ability to present the self, and to make moral claims about how one is to be perceived and acted upon, is a fundamental mechanism for structuring social relations and asserting social power (Goffman 1959).

Entrepreneurs have responded to these concerns by offering privacy enhancing technologies (PETs). These include infomediaries (which automatically release personal information to requesting parties only under certain conditions), cookie[1] management systems (which block web site operators from setting or accessing unique identifiers for each user), and anonymizers or pseudonymizers (which re-route web traffic in order to disguise its source or destination) (W3C 2001, Lumeria, Inc. undated, Cookie Central 2001, Anonymizer.com 2000, Burkert 1997). This article examines a specific PET – *Freedom*, a pseudonomyzer developed and marketed by Zero-Knowledge Systems – and asks how and to what effect, in practice, such a PET enables the user to control the context of self-disclosive activity. It further asks whether that control facilitates the ability to change specific social orderings or whether it only permits the re-enforcement

[1] Cookies are a mechanism by which web site operators can place a unique identifier on each user's machine, so that the site can compile a history of each user's activities across browser sessions. For a more complete description of cookies, see Cookie Central 2001).

and manageability of existing social orderings. It places the design logic of *Freedom* within the social understandings of a particular hypothetical user – a politically and sexually active gay professional man. The analysis is therefore rooted in a particular technology and referenced via a particular social position.

While this case is quite specific, and indeed involves a technical system which is no longer available[2], the attributes both of the technology and of the hypothetical user provide for an analysis which is potentially quite general. *Freedom* was recognized as the *ne plus ultra* of online privacy technologies, expertly incorporating the strongest cryptographic protections in a sophisticated interface (Norton 1999). It did what it did very well. Moreover, the underlying paradigm for privacy protection – digital pseudonymity – was quite sophisticated. This paradigm interpreted privacy as identity management. *Freedom* permitted users to create and assume any number of persistent but unlinkable personae, so that one could choose one's persona depending upon one's online social context. The analysis is intended to reveal characteristics of this underlying paradigm of privacy management itself, rather than vagaries of its particular instantiation.

The choice of the ideal user is theoretically informed, as well. For oppressed sexual minorities, in particular, strategic self-revelation, concealment, and context management is not merely personal, but fundamentally political. As will be discussed below, the gay rights movement has employed 'coming out' as its primary tactic and philosophy since at least the late 1960's. Therefore a socially active and politically aware gay man can be presumed to be conscious of both the practices of identity management and the political and personal repercussions of those practices. Positing a user who occupies an extreme and articulate position on the uses of social identity permits a nuanced general analysis of those uses.

---

[2] As of 22 October 2001, *Freedom* is defunct. Zero-Knowledge Systems has taken the service off line, focusing instead on a consumer security suite and business-to-business information management services.

The analysis of an idealized use of a sophisticated privacy software suite, especially the conflicts, contradictions, and tradeoffs inherent in that use, brings to light tensions between the ideal notions of privacy and lived practices of revelation and concealment. It brings to consciousness the tensions between ideology and action. It therefore suggests new ways to think about the ideas of privacy and identity, and the regulation of surveillance practice in law, policy, and technology design.

The following section reviews the theories and practice of the politics of sexual identity, including the relative risks and benefits of tactics of revelation and concealment. A further section presents a brief overview of techniques of online pseudonymity and an idealized account of the adoption of those techniques in everyday practice. Then that account is analyzed and critiqued to reveal the conflicts and negotiations involved in the translation of identity management from offline to online contexts. This critique particularly highlights issues of self-awareness, intimacy, community, and representation, and problemetizes pseudonymity as ideology and strategy. Finally, avenues for the development of concepts, laws, and technologies for the management of online identity are suggested.

THE POLITICS SEXUAL IDENTITY AND EVERYDAY IDENTITY MANAGEMENT

As a social ideal, privacy is of ambiguous value in identity politics, particularly in the modern gay liberation movement. Instead, issues and tactics of visibility and representation are at the core of the struggle. 'Coming out', the public claiming and embracing of a gay identity, has been the primary strategy and philosophy of the modern gay rights movement. Within this political strategy, there has been little purpose in calling upon privacy as a social ideal. Indeed, the strategy explicitly rejects the notions that sexuality is a private affair and that the domestic realm, populated by the nuclear family, is the bedrock and font-spring of moral value. Instead, privacy is seen, at least in

part, as an ideology of oppression and invisibility – depriving certain populations and issues of social standing and public debate. The domestic realm is understood as the domain of privatized, but legally sanctioned, patriarchal and heterosexist power relations. The power and deprivations of the private realm are gendered. Sexuality and gender roles are the repressed issues, women and sexual minorities are the repressed populations (Pateman 1983).

Feminists and gay activists have turned from privacy to democratic and economic participation as their normative claim to rights. In doing so, they have sought to articulate the ways in which the public and private realms are in fact mutually constitutive – the ways in which, in fact, the personal is the political.

'Coming out' – self-identifying as gay and presenting that identity to the larger world – serves at least three political functions. Firstly, it enables the individual to acknowledge, engage, and counteract the fear and shame of social stigma. Secondly, it enables the formation of a community within which to create a social identity, a culture, and a political power base. Finally, by coming out gay men and lesbians are able to present publicly, interpret, and argue for the social value of a gay identity, offering an alternative to the received hegemony of the heterosexual, patriarchal ideal (Boling 1996: 132-6).

'Coming out' is then an act both of personal liberation and of political claim-staking. It is a tactic, and a tactic that always occurs in a context of power. It involves risk – the risks of loss of income, of personal assault, of social stigma. These risks vary according to the circumstances of the actor. Popular chanteuses face a very different cost benefit analysis in coming out than do tenured professors or truck stop waitresses. The risks and benefits of coming out are also historically specific. In certain moments it may be politically and personally expedient to proclaim one's sexuality at a public rally but not at work. In other moments, the opposite might be true – anonymous declaration in a

crowd would be meaningless, whereas coming out in the workplace would catalyze powerful economic and political forces. Finally, each individual will maintain differing sexual identities depending on social context. One might be entirely 'out' to one's friends and co-workers but still maintain a formal indeterminacy at family re-unions. The ability to segregate these contexts is a measure of social power, and the inability to segregate them can be personally disastrous, as Arthur Sipple discovered when he saved Gerald Ford from an assassin's bullet. In knocking the gun from Sara Jane Moore's hand, he became a national celebrity. In San Francisco, Sipple had been a gay activist. This public, but local, identity was reported across the nation, particularly in his hometown, where his sexuality had remained hidden from his family. Unable to reconcile his various local identities, Sipple sank into a despair from which he never fully recovered, dying at the age of 47 (Morain 1989).

Being 'out' or closeted is not a binary condition, it is a negotiated and fluid identity status. It is not privacy *per se* that is essential in these political contests, it is the management of revelation in specific social contexts. Context management and identity management are essential to every instance of effective revelation and to the structuring of everyday power relations. Erving Goffman has studied in detail the methods that individuals use in face to face relations to manage revelation and concealment in specific arenas of public performance (Goffman 1959). In gay politics and the everyday praxis of gay men and lesbian women, we may see that these management activities are more acute, conscious, and theoretically informed.

At least since the late 1960s, sociologists have been aware that information technologies permit the collation of personal data across social contexts, and that that collation has significant implications for the distribution of social power (Rule 1974). These problems have only been exacerbated by the acceleration of online interactions. Recently, software developers have offered pseudonymity services as a solution to this

rampant distribution of personal data. On the face of it, unlinkable pseudonyms seem like ideal solution for empowering context management in online interactions. We therefore examine one such system in detail, to understand exactly how pseudonymity software mediates among practices of sexual identity management, online interaction, and data surveillance.

ONLINE PSEUDONYMITY[3]

Freedom is a software suite which employs cryptographic techniques to allow users to create several pseudonyms (or 'nyms') to use in online interactions (Goldberg and Shostack 1999). Before sending e-mail or browsing the web, the user starts *Freedom*, and then chooses which nym to assume during that net session. Once a nym is chosen, all packets to and from the user's machine are encrypted and sent through an anonymous remailer network. That is, each packet is encrypted in layers and forwarded through a sequence of servers. Each server decrypts one layer of the packet. This decryption reveals the identity of the next server in the chain, to which the packet is forwarded. Only the last server in the chain sees the final destination of the packet. No server is aware of the entire path, and so no server can know who is communicating with whom. No one can associate the nym with its owner. In addition to this route encryption, the contents of the packet are encrypted. No server, except perhaps the last in the chain, can monitor the contents of any message.

Although no message is traceable, nyms are persistent. Recipients of mail from a nym can respond to that nym. Websites visited by a nym can set cookies on the machine of the nym owner. The *Freedom* system will intercept and segregate these cookies, placing each in the 'cookie jar' of the nym that was operational when the cookie was received.

---

[3] Although *Freedom* is defunct, the description of its use and properties is written hereafter in the present tense for greater effect.

An idealized use of *Freedom* might go something like this[4]: Bob[5] is employed by the State of North Carolina, but he is often on the road and he often works from home. His employer endorses this situation, and to facilitate this arrangement they have provided him with a laptop. Bob is the only user of this machine, but it remains the property of the state. It is the only machine that Bob uses. He cannot really lug two laptops on his travels, one for business and one for personal use, and since it is a relatively high quality machine and quite adequate to his needs, he has decided not to buy a desktop computer for his home use. He has broadband Internet access at home, and uses a national dial-up ISP during his travels. The following example suggests a typical session when Bob is working at home.

When he turns on his computer, he enters a password to start *Freedom*. A dialogue box appears which permits him to chose from his 'True Identity' or any of his nyms. He chooses his 'True Identity' and downloads mail from his work account, bob@state.nc.us. When he replies to one of these messages, *Freedom* interjects a question: 'This message will appear to come from bob@state.nc.us - True Identity. Send Message / Block Message?' He chooses 'send' and conducts some professional e-mail correspondence. In the course of his work, he does some web-based internet research. Since he has not

---

[4] This is meant to be illustrative, not definitive. Of course, different users will have different routines. Different pseudonym management suites will have different features. The *Freedom* suite itself had many optional settings which permitted the user to shape the interaction to a great extent. Where these particularities make a significant difference to the quality of the experience, it will be noted.

[5] A bit of strategic revelation and concealment is in order here regarding the method of analysis. I, the author and researcher, am in fact a sexually and politically active gay man. The description and analysis is primarily informed by my use of *Freedom*. However, as I used *Freedom*, it became clear that certain issues would become more salient if I were in other circumstances – if I had another employer, perhaps, or another type of job, or if I lived in another state, or if I enjoyed other activities. I incorporated these other, imagined, circumstances into my analysis. So while I admit of a strong identification with my ideal user, and take full responsibility for the veracity of the following account, I claim the right plausibly to deny any inference from this account to my own behaviour.

chosen any nym, all of this web browsing will appear to originate from the IP address assigned to him by his ISP. All of the content will be sent in clear text and is susceptible to interception. Cookie management will be controlled by his browser.

Later, Bob wishes to do some personal communication – perhaps he is remodeling his kitchen and he wants to look at product reviews for major appliances and to exchange e-mail messages with his contractor. He is also involved in a local gay rights group and must arrange some business there. He is not closeted about any of these activities – his employer is aware of Bob's remodeling plans and Bob is purposely vocal regarding his political activity - but he does not want to present himself in these exchanges as a representative of North Carolina, so he chooses one of his *Freedom* nyms – 'bob' – and continues his research. Now, all e-mail that he sends seems to originate from 'bob@freedom.net'. This e-mail is now untraceable, in that it can be linked neither to the IP address he is currently using, nor to 'bob@state.nc.us'. It is also encrypted and, if intercepted, undecipherable.[6] In this instance, though, these attributes do not really matter to Bob – he does not consider any of the information particularly sensitive.

But Bob likes sex. He subscribes to a liberationist ideology of sexuality which holds that exploration of the connections among the libido, the mind, and the psyche can be powerfully instructive as well as just plain fun. He also subscribes to several chat rooms, mailing lists, and newsgroups which are explicitly and primarily erotic. These groups facilitate the exchange of narrative accounts, fantasies, and photos, as well as actual fleshly meetings. Bob is aware that this is a very different terrain of social activity than kitchen remodeling or relatively mainstream political activism. He does not mind claiming indiscriminately the identity of a sexually active gay man. In fact, he claims that identity

[6] This is not strictly true. The packets will be encrypted at Bob's computer and relayed through several servers before they reach their destination. The last server decrypts the packets entirely before sending them to the final destination. Any interception at this last stage of the transmission would yield clear text.

as an act of personal and political empowerment. Nevertheless, he chooses carefully those to whom he reveals the exact parameters of his desire. So he chooses another nym – 'seeker@freedom.net' – to continue his surfing.

Using this nym, he visits a web-based newsgroup reader to view erotic photos and to post some that he took recently of a friend. He also visits some websites that are aimed at those who share his sexual tastes. Some of these sites have traveler's guides, and he tries to find information on clubs or activities in New Orleans, the city to which he has a business trip next week. He also visits a web-based chat room and chats with a few New Orleans locals, one of whom seems quite amiable and compatible. He gives this person his e-mail address, 'seeker@freedom.net', with the intent to follow up on this correspondence over the next few days, and maybe to meet when he reaches New Orleans. Because he has had a nym active during these exchanges, none of the content is interceptible, and none can be linked to his ISP, to his name, or to any of his other nyms or e-mail addresses.

He exits *Freedom* and logs off his computer.

ANALYSIS AND CRITIQUE

While the above account may seem a straightforward adoption of the prescribed use of a new technology, it in fact incorporates a host of explorations, negotiations and compromises. Before he could establish a routine for *Freedom* use, Bob had continually to ask himself how and why he wanted to be represented and identified in various online contexts. He had to answer those questions in the light of his personal situation and his experience of the histories and cultures of American gay life in the late twentieth century, and he had to come to terms with his feelings about his answers to those questions.

Segregation of nyms

These negotiations were necessitated by the design principles embedded in the product. The first and most fundamental of the principles upon which the security, and the freedom, of *Freedom* is founded is the absolute segregation of nyms, both from one another and from the fleshly user of the nyms. *Freedom*'s entire design is geared toward ensuring that no one can associate traffic from one nym with traffic from any other nym, or with traffic from the nym's owner. Most of *Freedom*'s design work was in removing or disguising identifying information in the IPs necessary for traffic routing. However, the designers were also aware that users themselves might reveal identifying information in the content of their messages. To ensure that a user does not inadvertently reveal her 'True Identity', *Freedom* includes a facility for checking the content of each packet for sensitive information before they are encrypted. Zero Knowledge suggests that users employ this facility to check that packets from one nym do not include the user's name, e-mail addresses, or other nyms.

This segregation is an all or nothing affair. It is much more strict than the management of personae and identities in offline contexts. In offline life, one might acknowledge the existence of another persona without revealing all of the details of that persona. That is, one might encounter co-workers in off-hours and outside the workplace. It might be mildly embarrassing to run into one's boss while filthy and unshaven, perhaps after a long weekend of kitchen renovation. Likewise it might be embarrassing to run into her while on one's way to a leather bar, dressed to signal precise sexual proclivities. However, none of these encounters do more than suggest a realm of activities; they do not reveal the activities themselves. Linkages between nyms are much more revelatory. For example, anyone who had just discovered that bob@state.nc.us is also bob@freedom.net could use a search engine to discover any web presence that bob@freedom.net might have. Professional profilers, such as DoubleClick, could

automatically and permanently merge the profiles of bob@nc and bob@freedom. That merger would provide them not only with the contents of both databases, it would also provide an extra bit of information, namely, that bob@nc would like to think of bob@freedom as a separate facet of his identity. This is a very interesting piece of psychographic data. For police agencies, or others with the interest and ability to track and document the history of a particular user's activities, a linkage between nyms would be a windfall. While it is by no means certain that one lapse would inevitably negate all of the benefits, past and future, of pseudonymity, nevertheless, the stakes are higher in the segregation of nyms than they are in the segregation of our everyday, offline personae. Indeed, as shall be discussed later, the very uncertainty of the consequences of a lapse, coupled with an awareness of the strength of the design features attempting to prevent such a lapse, is a significant source of ambivalence to the user.

Establishing an identity

This necessity of maintaining strict nym segregation results in a variety of negotiations and conflicts. The first arises when a user initially chooses a nym. For example, Bob had always been aware of the lack of privacy in his old surfing activity. He had assumed that anyone who wanted to badly enough could link his online persona to his name and address. He had, therefore, imagined the possibility of being confronted offline with some of his least temperate online exchanges. He had made an *ad hoc* calculation of the risks and benefits of these exchanges, and that awareness had circumscribed his internet activities. He had adopted *Freedom* in order to relax those constraints. But can he?

If someone links his new nym to his old online persona, then, within the context of that linkage, the nym will be only as secure as the old persona. And if 'seeker@aol.com' stops posting on the same day that 'seeker@freedom.net' starts posting, it is a reasonable inference that they are the same poster, especially if their styles, habitats, and self-

presentation are similar. So Bob must decide whether to surrender any named identity that he has already created in order to maintain the security of the new nym. He needs to make an *ad hoc* cost/benefit analysis of identity maintenance.

What does he lose by adopting a new name? Suppose that for years Bob had been known in his chat rooms as 'seeker@aol.com'. He had, in fact, built up a certain reputation as a quick-witted, responsible, and playful participant in these fora. Not only was his old persona a recognized and respected member of the community, but he likes his old name. It feels to him like himself. When he adopts *Freedom*, Bob must decide whether to retain that social capital and self-identity and adopt the nym 'seeker@freedom.net' or abandon it for a new label.

If he keeps it, he risks inviting an association of his new, protected, identity with his old, unprotected identity. What are the risks of this association? To answer this, he needs to know who, if anyone, is likely to make the link between his old and new identities. He needs to know what use is likely to be made of the link. Will that linkage only be made by people with whom he has personally interacted? In that case, the potential harm is negligible. Can the linkage be automated by a third party analyzing web traffic? If so, he considers the potential harm relatively high. But is it likely to be automated? Further, is the link provable, or could Bob plausibly deny the link? Under what circumstances might that denial be necessary or expedient? Is that deniability sufficient to his needs? What, in short, is he worried about?

Bob has, in fact, almost no way of knowing who is likely to notice the change in persona, or with what resources or to what end that change will be noted. Bob is again, as ever, negotiating the closet. This is always a personally and politically loaded activity, but now it is exacerbated by an uncertainty of the technical and social contexts in which the negotiation is taking place.

Inviting intimacy and building community

Pseudonym segregation must be negotiated again when the user wants to move interactions begun online into offline contexts. Strong pseudonymity software, such as *Freedom*, undeniably reduces the personal risks associated with the exploration of web content and e-mail. As long as the user has maintained strict segregation of nyms, he can be assured that no one can monitor his interactions or link those online interactions to his person.[7] This is significantly empowering as the user explores his own desires, and discovers the possibility of satisfying those desires. He may avail himself of chat rooms, historical archives, erotic imagery, and political organizations without leaving his home or risking his job or his social standing.

The solitary exploration described above will in all likelihood lead to the discovery of a community, or at least the discovery of other people with similar interests, feelings, and personal histories. Pseudonymity can mediate the risks of engaging this community, as long as that engagement takes place in the off-line world. This, again, can be significantly empowering. The history of the net is full of tales of enduring, cohesive, and supportive relations among people who never physically meet (Jones 2001, Phillips 1996). Likewise communities of anonymous or pseudonymous participants can be vital and enriching. Members of Alcoholics Anonymous (AA), an undeniably successful therapeutic program, create strong communities by explicitly bracketing their interactions within certain times, places, and identities (Arminen 1998).

In each of these cases, though, participants may choose to cross the boundaries of their initial social contexts. Newsgroups participants may meet in 'real life', and members of AA may establish strong interpersonal relations outside the meeting rooms. In every

[7] Actually, there is another instance in which the security of Bob's communications may be compromised. *Freedom* considers that it's job stops when messages reach the user's machine. All e-mail is stored there in plain text, as are browser bookmark and history files. Especially because he uses a machine owned by his employer, Bob must decide whether to use an auxiliary encryption program to protect this data. Again, he negotiates the closet.

case, there will be a negotiation of the new context, and a re-negotiation of the old one. It is this renegotiation of context which is particularly problematic with strong pseudonymity. Should a *Freedom* user wish to move interpersonal interaction to the physical world, or to allow a linkage between his online personae, troubling issues again arise regarding the risk and benefits of identity segregation.

The negotiation of social identity is not only about the construction and maintenance of boundaries, regions, and performances. It is also about negotiating the permeability of those boundaries - the wink, the grin, the appreciation of an 'in' joke which suggest that a new participant may be welcome in another region, another performance. It is about intimacy. Intimacy is less about sharing secrets than it is about revealing the inconsistencies and paradoxes of the constructed self. It is about granting access to many regions, many back stages. With *Freedom*, however, the invitation to intimacy is an all-or-nothing affair.

Pseudonym management requires, at least initially, vigilance regarding one's performance of identity. But too great an awareness of the performative aspects of one's life is debilitating. A certain 'through-line' of identity integrates our performative selves. In offline life, the performative aspects of self – choosing outfits and demeanours for professional meetings, family gatherings, or bar-hopping - may be experienced as quite pleasant and creative, and the segregation of those selves is easily maintained by managing one's physical presence. One simply does not show up at work in the demeanour and the costume that one assumes while watching television at home. Should an intruder from another social context happen into a protected region, negotiations are immediately undertaken to normalize the situation. This normalization might include the recognition of a mutual, but somewhat guilty, penchant for *Antiques Road Show*, and a happy intimacy might ensue.

A sense of an integrated self facilitates these intimacies. That is, the more one is comfortable shifting among personae, employing *double entendre*, negotiating and utilizing the proprieties of each social situation, the more at home one may feel in one's self and in the world. One may be - quite comfortably, appropriately, and simultaneously - a shoe fetishist, a bizarrely over-educated leftist intellectual, a charming professional consultant, and a couch potato with a camp appreciation of television cooking shows. There is no need to negate any of these facets in order to present another. Yet that sort of negation of the connection among our myriad defining characteristics is at the heart of online pseudonym management. Strict pseudonymity is not about self-integration, it is not about letting people in, it is not about revelation. It compartmentalizes personae in a way that everyday, contextualized self-presentation does not.

That compartmentalization is both necessitated and made difficult by the user's ignorance of the online context in which he performs. One never knows who else is present and ready to catch the online wink. There is no ability to assess or manage the context of revelation.

Public representations of identity

Public argument over the social position of gay individuals, identities, and communities is the core of the modern gay rights movement. Not only is this argument publicly visible, it is also about public visibility. It simultaneously addresses and reconfigures the social consciousness of sexual minorities. Pseudonymity software mediates public visibility in several ways.

Effective participation in public discourse may be anonymous. Indeed, pseudonymous political writings have an honoured history in the U.S. (Hamilton *et al*. 1961). In some cases, political activists have a Constitutional right to anonymity.[8]

[8] Talley v. California, 362 US 60

Anonymous screeds, fictionalized biographies, interviews granted backlit or from behind a potted palm – all have been vehicles of gay liberation. With *Freedom*, online political presence can be extremely effective, extremely visible, and entirely pseudonymous, and for this it is an invaluable tool.

However, there are other, more problematic, aspects of pseudonymous public visibility. These involve the public fiction of the gay man as cultural icon. Arguments over the representation of gay men and lesbian women in the popular imagination have a long history in gay and lesbian politics. Activists have contested popular culture images where sexual minorities are depicted as sick, victimized, or criminal, and often all three simultaneously – essentially weak but still utterly dangerous (Russo 1980). Similar arguments over stereotyping have erupted as gay men, and to a lesser extent, lesbians, have been configured, represented, and analyzed as a market segment. It is not clear at all that the power of representation is diminished when it takes the form of demographic analysis rather than cultural myth. Indeed, these digital models may be more insidious than public representations, because the models and the algorithms which guide their use are privately owned and circulated, and so unavailable for public contestation (Gandy 1993).

Profiling usurps the subject's power of self-representation. The profiler, not the subject, determines which data points in which contexts are useful or meaningful, and so creates a persona which may be quite independent of the subject's intended self-presentation activities (Frohmann 1994). These profiles are used by their owners for their own purposes. The interests of the subject, or of the demographic group to which the subject is assigned, are considered only insofar as they align with the interests of the profiler. These interests may well be partially aligned. Public recognition of gay or lesbian markets – whether for Subaru cars or 'I can't even think straight' T-shirts – is certainly advantageous to some buyers and some sellers. But interests are often at odds,

and it is quite possible that one would *not* be offered ads for health insurance or particular vacation packages because of a private analysis of one's surfing habits (Li 1996). Moreover, it is not clear that the representation of and action toward the gay community as a market is a politically progressive development. In the rare instances when marketers have published their data, activists have argued that the data tend to represent the community as young, male, and possessed of disposable income. This representation, made for the purposes of the market, ignores, deflects, and denies real political concerns of poverty (especially among lesbians) and social oppression (Badgett 2001).

Increasingly, website operators support their operations and make a profit through advertising. They are able to charge more for ads if they can guarantee that the ads will be targeted to a particular population of web users. To do this, site operators employ third-party profilers to surveille users and serve ads. Profiling is the creation of a digital persona which represents an individual and is used as a management tool in fashioning interactions with the individual (Clarke 1994). Cookies are the primary mechanism for constructing and utilizing digital persona on the web.

True to the design paradigm of strong pseudonym segregation, *Freedom* includes a cookie management facility which contextualizes cookies within each nym. When a web surfer is using *Freedom*, visited sites may still set and refer to cookies, but those cookies are managed by *Freedom*, not by the surfer's browser. *Freedom* segregates cookies into a different 'cookie jar' for each nym. So, for example, if Bob visits the Yahoo! site under the nym 'bob', the Yahoo! site will reference its cookie in Bob's cookie jar. Later, when Bob selects the nym 'seeker' and revisits the site, the site will be unable to relate the cookie for 'seeker' to the cookie for 'bob'. Yahoo! and its affiliates will have separate, unlinkable profiles for bob and seeker.

Again, the primacy of segregation of nyms as a design criterion is evident in *Freedom*'s cookie management system. *Freedom* provides only the most rudimentary

facilities for managing cookies within each nym's cookie jar. Further, the cookie jars are not stand-alone files; they are incorporated into the *Freedom* software. It is difficult, if not impossible, to integrate them with auxiliary cookie management software. There are cumbersome workarounds, but by default *Freedom* facilitates profile building within nyms. It therefore provides an excellent case study of how pseudonymity of itself might articulate with common practices of personal data use.

The ability to segregate nyms and their cookies does offer an opportunity for gay men to influence the processes of profile production and targeted marketing. By using *Freedom*, one can establish multiple IDs and personae in DoubleClick's database, and cause DoubleClick to serve different ads depending upon which persona is being referenced. In this way, the user may be able to control or influence the context of his action and the response of the audience within that context. This is the central operational activity of Goffman's (1959) theory of self-presentation, and a fundamental process in the creation and maintenance of social orders.

For gay men and lesbians, however, it is not clear what the social and political implications of this contextualization are. It may well serve to further marginalize the sexual and erotic aspects of one's activities, supporting the definition of one's self as gay in one context and 'regular' in another. It may place sexuality (especially non-mainstream sexuality) once again firmly out of the public realm, and out of the political realm, out of acceptable public consciousness. It may re-enforce the zoning of our consciousnesses and activities into 'family' and "adult" regions. It may well reinforce existing structures and stigmas which relegate non-heterosexuality to the margins of society.

In summary, privacy technology operating under the paradigm of strong pseudonymity permits a very strong control of identity. It offers significant opportunities for a publicly sexual gay man to protect his interests. It allows him to

engage in some behaviour in a way that is quite hidden, to segregate his public performances, and to engage in public debate without fear of bodily retribution.

However, it is all but useless as a means of controlling social context of that identity. Online architectures are still, in a sense, panoptic. There is no way of knowing who is present, who is watching, whether and for what purpose data are being collected. At most one can choose to be watched multiply, to be several subjects of knowledge. This may be significantly empowering, and it certainly is grist for the mill of Foucauldian identity theorists. But it does not articulate well with the culture and politics of everyday self-presentation. While it promotes the production of multiple selves, those selves are not easily lent to practices of intimacy or community.

Pseudonymity management requires a consciousness of when and what to hide, how to construct barriers. It does not address the problems of when and what to share, how to connect. It requires decisions about self-presentation in certain contexts, and it requires that those decisions be made in ignorance of who is sharing that context, and with what resources or purpose. The practical process of establishing and maintaining this segregation of personae, often informed only by the user's own personal worst-case scenario, may awaken feelings of schizophrenia, powerlessness, and shame. In short, it may feel very much like a return to, or a re-inscription of, the closet.

Pseudonymity lends itself to profiling practices which define and reify classes of people, even as it protects the individual from some of the repercussions of being defined as part of that class. For example, by segregating his erotic activities, but still permitting the tracking and surveillance of those activities, the user facilitates the construction and imposition of norms of erotic behaviour. Because he contributed to that construction pseudonymously, those norms may not be immediately imposed back upon the user. Those norms may, however, be inimical to the interests of gay men as a group, especially

insofar as they position sexual behavior, and communities identified through sexuality, within a larger social order.

In short, pseudonymity software is informed by a politics of heroics rather than of community.

DIRECTIONS FOR FUTURE RESEARCH

When the salient social problem is identified as the collection and collation across contexts of individually identifiable information, then segregated pseudonyms seem to be a reasonable technical response. But this segregation of digital personae, though itself complex behaviour, does not begin to approach the complexity and nuances of everyday identity management. Nor does it directly address the underlying structures of interest and power from which issue the imperative for data collection. What is required of technical developers and policy makers is threefold. First, they must develop a more sophisticated understanding of identity management, especially the role of intimacy, trust, and community. This may involve development of technologies which permit of locality, rather than identity. That is, instead of inviolably separate personae, we should develop models for overlapping and permeable contexts of identity – circles of knowledge and degrees of trust. Some research in this area is promising. For example, Ellison (1997) has described identification systems which permit of local but interlinked naming structures. One might be able to prove, for example, that one is the entity known as *A* in context *X* as well as the entity known as *B* in context *Y*, but to limit the availability of that proof to, say, context *Z*. Brands' (2000) cryptographic protocols allow some control over when and how particular descriptive attributes are released and used, so that one might maintain a stable, central identity, but control connections among facets of that identity depending on the context of interaction.

Both of these techniques are theoretically and cryptographically complex. A great deal of research and development is necessary even to bring them to the stage of

prototype, and those prototypes will more than likely fail in practical use. But it is only through use that we can learn how these theoretical models will articulate with the complexities of everyday situated practice. Failure on a significant scale is likely to be a pre-requisite for eventual success. Further, personal data collection is one of the few dependable income streams in the current market model for the Internet, as well as a linchpin of developing models of intellectual property management. It is therefore unlikely that profit making corporations will be willing to undertake these research ventures. We must, instead, recognize network identity as a fundamental issue of citizenship and social power, and incorporate identity management into public and quasi-public research initiatives.

Our second task is to confront and interrogate current information surveillance practices. We must fashion policy which promotes individuals' ability to know who is monitoring their activities, which activities are being monitored, and how those data are being used. We must also engage in educational activities which will empower individuals to place these activities within an understanding of the global political economy of information. Without both particular knowledge of specific surveillance activities and the cognitive schemata to make sense of these activities, individual choice and consent are practically meaningless.

Finally, we must recognize the social relations which precede and inform identity and surveillance. Pseudonymity is a modestly useful tool. But of itself it has no power to reconfigure relations of social power. The manipulation of Internet Protocols will not remove sodomy statutes from North Carolina's law books. It will not prevent employers from firing lesbian mothers at will. It will not prevent homicidal bashing of gay teens. To be truly liberatory, reactions to surveillance must include not only technologies and policies which address informational privacy, but more fundamental mobilizations against

the perception of personae, persons, and classes as targets either for murderous hostility or for market exploitation.

REFERENCES

Anonymizer.com. (2000) 'Anonymizer.com: privacy is your right', http://www.anonymizer.com/corporate/index.shtml

Arminen, I. (1998) 'Sharing experiences: doing therapy with the help of mutual references in the meetings of Alcoholics Anonymous', *The Sociological Quarterly* 39, p. 491-515.

Badgett, M (2001) *Money, Myths, and Change: The Economic Lives of Lesbians and Gay Men* Chicago, IL: University of Chicago Press.

Bennett, C. (2001) 'Cookies, web bugs, webcams and cue cats: patterns of surveillance on the world wide web', *Ethics and Information Technology*, 3*:* 197-210.

Boling, P. (1996) *Privacy and the Politics of Intimate Life* Ithaca, NY: Cornell University Press.

Brands, S. (2000) *Rethinking Public Key Infrastructures and Digital Certificates: Building In Privacy*. Cambridge, MA: MIT Press.

Burkert, H. (1997) 'Privacy-enhancing technologies: typology, critique, vision', in P. Agre and M. Rotenberg (eds.) *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, pp. 125-42.

Clarke, R. (1994) 'The digital persona and its application to data surveillance', *The Information Society*, 10: 77-92.

Cookie Central. (2001) 'PC software', http://www.cookiecentral.com/software.html

Electronic Frontier Foundation (2001) 'EFF analysis of the provisions of the USA Patriot Act', http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html; Accessed December 2, 2001.

Ellison, C. (1997) 'What do you need to know about the person with whom you are doing business?', House Science and Technology Subcommittee Hearing, 28 October 1997: *Signatures in a Digital Age*.

Frohmann, B. (1994) "Communication technologies and the politics of postmodern information science', *Canadian Journal of Information and Library Science* 19: 1-22.

Froomkin, A. M. (2000) 'Wrong turn in cyberspace: using ICANN to route around the APA and the constitution', *Duke Law Journal* 50: 17-184.

Gandy, O.(1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.

Goffman, E. (1959) *The Presentation of Self in Everyday Life*. New York, NY: Doubleday.

Goldberg, I. and Shostack, A. (1999) 'Freedom 1.0 architecture and protocols', http://www.freedom.net/info/freedompapers/Freedom_Architecture_protocols.pdf. Accessed 12 January 2000.

Hamilton, A., Madison, J. and Jay, J. (1961). *The Federalist Papers.* , ed. R. Fairfield, Garden City, NY: Anchor Books.

Jones, S. (2001) *CyberSociety 2.0.* Thousand Oaks, CA: Sage.

Li, K. Chi-Wen. (1996) 'The private insurance industry's tactics against suspected homosexuals: redlining based on occupation, residence and marital status', *American Journal of Law & Medicine* 22: 477-502.

Lumeria, Inc. (Undated) 'We are: an overview of Lumeria's "Sunshine" platform', http://www.lumeria.com/what1.shtml

Morain, D. (1989) '"Forever grateful" to ex-marine, Ford says', *Los Angeles Times*, March 8: part 5, p. 2, column 3.

Norton, P. (1999) 'Freedom 1.0', *PC Magazine*, December 23.

Pateman, C.. (1983) 'Feminist critiques of the public/private distinction', in S. Benn and G. Gaus (eds.) *Public and Private in Social Life,* London: Croom Helm.

Phillips, D. (1996) 'Defending the Boundaries: Identifying and Countering Threats in a Usenet Newsgroup' *The Information Society* 12 :39-62.

Rosen, J. (2000) *The Unwanted Gaze*, New York, NY: Random House.

Rule, James B. 1974. *Private Lives and Public Surveillance: Social Control in the Computer Age*, New York, NY: Schocken Books.

Russo, V. (1981) *The Celluloid Closet,* New York, NY: Harper and Row.

W3C. (2001) 'Platform for privacy preferences (P3P) project', http://www.w3.org/P3P/. Accessed 13 February 2001.

Warren, S. and Brandeis, L. (1890) 'The Right to Privacy', *Harvard Law Review* 4: 193-220.

Westin, A. (1967) *Privacy and Freedom*, New York: Atheneum.

Zero-Knowledge Systems. (Undated) 'Freedom - internet privacy and internet security: security software for your protection online'. http://www.freedom.net. Accessed January 17 2000.