

CONTEXTUALIZING ONLINE IDENTITY: PARADIGMS AND PROCESSES

David J. Phillips
Department of Radio/Television/Film
University of Texas at Austin
djp@mail.utexas.edu
512-471-6624

TELECOMMUNICATIONS POLICY
RESEARCH CONFERENCE

ALEXANDRIA, VA
SEPTEMBER 19-21, 2003

*15 September 2003
(Replaces preliminary draft dated
3 September 2003)*

IDENTITY, IDENTIFICATION AND CONTEXT

Social roles, social situations, and social relations are created in their performance. But these roles, situations, and relations are not created anew with each performance. The performances themselves occur within, and are structured by, institutionalized settings and culturally specific “common sense.” Yet these institutions do not exist apart from the performances within them. By our actions, we reconstitute and reconstitute the institutions and structures within which our actions occur, and with which our actions make sense. There is thus a recursive relation between performance in the here-and-now and enduring social structures. To paraphrase Giddens (1984), social structures are always the product of the activity they recursively organize.

Therefore the ability to knowingly act within particular contexts is also the ability to shape those contexts. The abilities to know where one is, to decide how to act, how to interact, how to perform, how to be seen and known in that place, are aspects of the power to create social places and social relations. Awareness of context, and the ability to adapt the performance of one’s identity to that context, are resources of social power. This paper addresses the institutionalized distribution of that power.

Identity, in the sense of social role, is inextricably linked to social context. The ability to manage transitions between social contexts, to focus our activities judiciously, to be known and responded toward appropriately by different persons, is a resource in the continual construction of appropriate places. This adaptation of identity to context is evident in the performance of everyday notions of propriety – dressing and speaking as

appropriate in various places (the office, the family kitchen, the bowling alley) and among various cohorts (one's supervisors, one's children, one's bridge club).

This adaptation of identity to context is socially useful in several ways. A member of an oppressed class - slaves, servants, those of stigmatized identity - quickly learn that she needs to be much more adept at reading the boss's mood, or the tenor of a crowd, than they are at reading hers. She learns to be invisible, to blend into an environment in which she don't truly belong, and to read subtle signs suggesting when she needs to disappear, for her life.

Knowledge of the milieu is also necessary in order to gain status within that milieu. As one is better able to utilize the accepted modes of behavior of a particular social context, one attains "belonging," status, and power. As Lady Utterword assures us in Shaw's *Heartbreak House*, "if you will only take the trouble always to do the perfectly correct thing, and say the perfectly correct thing, you can do just what you like." (Shaw 1964 [1919], p 83)

Finally, knowledge of social mores is useful for mirroring those mores ironically, using them facetiously in order to analyze, mock, or change them. (Butler 1998)

Our roles, our contexts are constantly changing. In everyday life we move from home to work to the gym, altering our disposition to meet the context. We try to segregate these contexts, and make an effort to affect the changes between them quickly, gracefully, and seamlessly. Moreover, identities and social contexts are not discrete; all of our relationships overlap and interweave among each other. We are, at one and the

same time, a hostess and a mother; we cruise for dates as we shop for dinner; we wonder how to manage the fact that one's brother-in-law is now one's employee.

All of this management of identity, of projection of self, of social roles within social contexts, occurs more or less effortlessly in everyday life. That degree of effortlessness depends on the availability of certain resources. These resources include understandings of:

- the attributes by which the subject is known, understood, and acted upon. The means by which one is recognized, and the type as which one is recognized, go far in determining how one is treated, how one is responded to, the likely effects of one's actions. Quoting Shaw again, but this time from the other end of the social ladder, "The difference between a lady and a flower girl is not how she behaves, but how she is treated" (Shaw 1951, p. 99). What defining factors are considered relevant in the cognitive or ontological model of the subject? What values are readily available for the instantiation of those factors? This is seen in the current political arguments over the ascription of race in the U.S. census. Will the institutional construction of the individual permit a mixed race identity, or a person of no race at all? As both Eliza and Lady Utterword are well aware, it is easier to demand to be treated as a lady if the concept of "lady" is well established.
- the context in which the subject known. Does a particular knowledge of an individual extend through various institutional settings, or is it limited, say, to the census bureau or to one's dry cleaners?

- the subject's awareness of the context in which she is acting. Are actors aware of who is sharing the space with them? Are actors aware of the social mores which regulate appropriate behavior in a space? After all, a flower girl in the ballroom is not blind, but she is nevertheless at a loss. She sees, but cannot make sense of, the cues suggesting how to act. Until she can interpret those codes, she cannot use the signs available in that milieu as tools.
- the possibilities that are afforded the subject to influence, or be influenced by, the social context. Is the actor able to act in a way which makes certain actions available only to certain others? Can an actor determine or influence the scope of the knowledge about her, or the contours of that knowledge?

In everyday life, many things structure the availability of these resources - walls, mirrors, upbringing, education, zoning laws, corporate policy. These structures are often invisible, but always they are available, in some way, for contestation. And in that contestation, our behaviors influence the structures which constrain and shape our behavior.

As social interaction moves toward information-rich environments and virtual interactions, it behooves us to translate this understanding of the interplay between identity, social context, and social power to the behavior and structures which constitute those environments and interactions. As individuals interact with each other and with institutions via digital media, technical and social mechanisms are being established to identify the participants in these interactions. As in offline interaction, the identification

process is used in the negotiation of a mutually agreed upon context for the interaction - to respond appropriately, to grant or deny access to information or other resources, to present a particular face.

This paper has two aims. The first is to present three paradigms for online identification, and to analyze them in terms of the resources they make available for the negotiation of identity and context. That is, each is evaluated in terms of the identity categories it facilitates, the degree to which it makes the environment of interaction visible, the degree to which it allows users to make sense of that environment, and the ways in which it facilitates strategic self-disclosure. The second aim is to understand the social forces that have been at work in structuring access to these differing paradigms. On the whole, the goal is to illuminate the activities which embed, challenge, or reinforce the ability of certain social actors to influence the enduring shape of social places, roles, and relations.

Analytically, this work owes much to Bechtold's (2003) taxonomy of namespace administrations. In that work, he classifies name spaces such as PKI and Microsoft's .Net Passport along several axes - whether they are flat, hierarchical, or decentralized; heavily controlled or loosely coordinated; multi-purpose or single-purpose; controlled technically or contractually; whether they are administered publicly or privately (p 1244). This article extends that work in two ways. First, it extends the analysis of the social import of these systems beyond the legal and policy realms to include social theoretical issues such as presence and cultural identity. Second, it examines more closely the social processes shaping these systems. Bechtold recognizes the recursive nature of technology and social

structures, but looks more at how technical systems embed and structure social relations. I want to focus also on the social activities that can influence the shaping of the technical systems. I add an emphasis on what Star and Bowker (2002) term *infrastructuring* - the work of making technical systems disappear into taken-for-granted, everyday use, purpose, and meaning.

THREE PARADIGMS

This presentation describes the technical structure of each of three systems, and analyzes how that technical configuration could possibly be used to negotiate contextualized identities. It places those possibilities within the ethics and political economy of information exchange, describing to whom each would be useful and how each might consolidate or realign social and economic power. The systems include X.509 PKI certificates, ZeroKnowledge System's *Freedom* network, and Microsoft's .Net Passport. These are chosen in order to compare across several axes - successful and unsuccessful deployments, different paradigms of identity, naming, and context, and different strategies and resources in the infrastructuring process.

The initial analysis is in terms of contextualized identity. It asks:

- what attributes of the subject are known; how is subject understood and constituted?
- in what context is the subject known?
- what attributes of context are known to subject?
- what possibilities does it afford subject of influencing, or being influenced by, context?

Public Key Infrastructures

Properly used, public key cryptography can ensure that messages are read only by their intended recipient, and that messages have not been altered since they were created by their author. They are therefore used for both security and authentication of digital communications. In public key cryptography, the user generates a key pair (the public key and the private key) with the mathematical property that any message encrypted with one key can be decrypted only with the other. To send a message securely from Alice to Bob, Alice gets Bob's public key, encrypts the message with it, then sends the encrypted message to Bob. Bob decrypts the message with his private key. To send a signed message to Bob, Alice encrypts it with her private key, and sends both the plain text and the encrypted text to Bob. Bob decrypts the encrypted text with Alice's public key, and compares it against the plain text for alterations.

As the nomenclature implies, public keys are widely distributed, private keys are closely held by a single entity. The distribution of public keys requires organization - hence the development of Public Key Infrastructures (PKIs). The most pressing problem with public key distribution is ensuring that the public key associated with Alice in fact belongs to Alice, and not to an imposter.

The most common solution to this problem is the use of the IETF X.509 certificate standard. An X.509 certificate is a record containing, among other fields, Alice's public key. The certificate is itself signed by a certification authority (CA), which vouches for the correspondence between Alice and the key contained in the certificate. To check the validity of a certificate, the recipient checks the CA's signature using the CA's public

key. But how can one be sure that that public key was not issued by an imposter? The CA itself will present a certificate, signed by yet another CA, vouching for the validity of its public key. Of course, that certificate must be validated using another certificate..., and so on until one is presented with a certificate with a trusted signature.

Coordinated use of X.509 certificates entails the institutionalization of several processes. In order to discuss these trends toward common infrastructure, it is necessary to delve somewhat more deeply into the structure of the X.509 certificate itself. Version 3, the most current X.509 version, is intended to be completely general and extensible. It accomplishes this goal by permitting the addition of any number of optional fields. However, the standards includes both requirements and strong suggestions regarding the presence (or absence), as well as the structure, of certain fields. Any suggestion from the standards body carries a great deal of weight with PKI developers. So, although, in theory, X.509 can support any conceivable PKI, it strongly favors certain institutional features.

The X.509 v.3 consists of the following required fields¹:

- Issuer's (CA's) 'distinguished name'
- Subject's 'distinguished name' (this field may be null iff alternative name extension is present)
- Subject's public key
- CA's signature

¹ This description includes only those fields necessary to this analysis.

V.3 permits optional extension fields. These extensions may be marked critical or non-critical. Critical extensions must be processed for the certificate to be validated.

Defined extensions include :

- Valid usages of key in certificate (For example, a key may be valid only for verifying e-mail signatures, time-stamping, or SSL.)
- Subject alternative names. The certificate may refer to the subject not by a distinguished name, but by an alternative naming method, for example an e-mail address or IP address. If present, alternative names are just as binding as distinguished names. The alternative name field is a critical field if the distinguished name is absent.
- Basic constraints. This field specifies whether the subject is a CA or an end-entity. If the subject is a CA, then the field further specifies the how many CA's the subject CA can authorize. For example, if the field value is zero, the subject CA can authorize only end-entities, not further CA's. If the field value is 1, then the CA subject CA can authorize CA's, but those CA's can authorize only end-entities. The standard mandates that this field be present and critical if the subject key is used to verify signatures on certificates - that is, if the subject is a CA. (Adams and Lloyd)

In general, X.509 certificates are authentication certificates, they verify a link between a public key and a particular entity. They don't usually describe that entity in

much detail, or grant authorization for that entity to do anything in particular.² Therefore X.509 certificates may be accompanied by an attribute certificate, issued by an organization vouching for certain properties of an identified entity. Such a certificate consists of:

- Issuer's distinguished name
- Subject's distinguished name (or other identifier)
- Subject's attribute (For example, the subject's birth date or citizenship)
- Issuer's signature

Theoretically, X.509 and attribute certificates together could be used to administer online resources. For example, to access an adults-only site, Alice would present a signed request to enter the site, along with an X.509 certificate and a birthdate attribute certificate. The site administrator would authenticate the X.509 certificate to verify that the request came, in fact, from Alice, then authenticate the birth date certificate to verify Alice's age.

This practice implies an institutional infrastructure, including:

- *Registration Authorities* to vouch for Alice's identity and assign her a distinguished name
- *Certification Authorities* to vouch for the link between Alice's name and her public key, and to issue and revoke certificates.
- *Repositories* to hold and distribute certificates

² The X.509 standard does permit of, but discourages, an optional authorization field.

- *Attribute Authorities* to vouch for and issue certificates regarding any number of attributes (age, citizenship, membership, etc)
- *Certification Status Responders* to verify validity of certification chain.

The social, legal, technical, and economic intertwining of these authorities shape, to a large extent, the implications for contextualized identity of any working PKI. Since the early 1990's, the Canadian Federal Government has developing a centrally managed PKI for the electronic delivery of services and programs (Treasury Board of Canada Secretariat 2001a). The following section examines the primary policy document of that effort in order to understand how that particular implementation shapes identities and contexts (Treasury Board of Canada Secretariat 1999).

The Canadian PKI is designed to facilitate communication with and between Departments of the Canadian federal government, and to facilitate communication between citizens and the Departments. The PKI cannot be used for any purpose other than communication with the government of Canada. It operates on an x.509 certificate format. Governmental Departments act as CA's, verifying the identity of subjects, assigning subjects' distinguished names, issuing and revoking certificates vouching for subjects' public keys.

Each certificate, and each key, is associated with a particular purpose. In particular, a key may be used either for encrypting data for confidentiality, or for signing data for authentication. The same key cannot be used for both purposes.

Certificates are issued according to one of four standard policies – rudimentary, basic, medium and high. The standard under which the certificate is issued determines

the reliability of the certificate and the legal liability of the CA for errors in issuance. These policies are standard across the PKI, though each CA determines the particular practices used to ensure that certificates are issued appropriately.

If the key contained in a certificate is used for encrypting confidential records, the CA keeps a copy of the corresponding private key. The CA never keeps copies of private keys used for signatures.

In compliance with the Privacy Act, CA's must tell certificate subjects what information is in the certificate, gain consent to the use of such information, allow the withdrawal of consent, and guarantee the subject's rights of access to and correction of personal info. Subjects who are not government employees may withhold consent without penalty. In effect, this means that they may choose not to use the PKI to receive government services. If they are issued a private key and a public key certificate, they are required to secure their private key against unauthorized use.

Departmental CAs become members of the Federal PKI by signing a Memorandum of Understanding and agreeing to the policies outlined here. In becoming a member of the PKI, they agree to recognize each others' certificates. Cross-certification (that is, verifying certificates among CA's) is handled through the Canadian Central Facility, which thus acts as the root CA. Members of the PKI become voting members of the Policy Management Authority, which sets cross certification standards, and may revoke the cross-certification of member CA's.

Constitution of subject and context

- What attributes of the subject are known? How is the subject understood and constituted?
 - The subject is known as a distinguished name, which is always linked to a particular citizen through standard forms of ID, include the Passport, Driver's License, Baptismal Certificate, or Birth Certificate. This distinguished name may be associated with numerous certificates, but only with one embodied individual citizen. Further, the role of that subject is to verify or attest to her legitimate relation to the government, through the signing of documents.
- In what context is the subject known?
 - For now, knowledge of and awareness of this constituted subject is limited to the Canadian federal government.
- What attributes of context are known to subject?
 - The disclosures mandated under the Privacy Act afford the subject some sort of awareness, or mirror, of her position in the information environment. Moreover, the rule based bureaucracy governing that environment affords some sort of predictability and recourse regarding the ways in which the data subject is known and treated.
- What possibilities does it afford subject of influencing, or being influenced by, context?

- Employees cannot opt out of this environment, nor can they be reasonably expected to influence the policies and procedures structuring the environment. Theoretically, non-employee citizens may opt out entirely and without penalty, receiving equivalent services outside the PKI structure. However, it yet remains to see what incentives of cost or convenience encourage participation.

State of deployment:

Since 1995, Canada has made PKI a part of its strategic information technology planning. This strategy has had as its goal ensuring Canada's global pre-eminence in a knowledge-based economy. The primary policy initiative in this goal has been a comprehensive plan to encourage the development of electronic commerce. It was to support electronic commerce on the whole that the government, in 1998, made the development of a secure environment for electronic service delivery its highest IT priority (after Y2K readiness) (Treasury Board of Canada Secretariat 2001b).

The federal government has actively encouraged departments and programs to develop online service delivery. While programs such as address changes, passport applications, customs processing, and spectrum auctions have utilized the federal PKI, adoption has been neither as quick, as smooth, nor as general as policy-makers had hoped (Treasury Board of Canada Secretariat 2002a, Treasury Board of Canada Secretariat 2002b).

Persistent pseudonyms: Freedom

The second paradigm for contextualized identity to be studied here is strong, persistent pseudonymity, particularly as implemented in the *Freedom* software suite. Developed by Zero-Knowledge Systems of Montreal, Canada, and deployed between January 2000 and October 2001, *Freedom* employed 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 started *Freedom*, and then chose which nym to assume during that net session. Once a nym was chosen, all packets to and from the user’s machine were encrypted and sent through an anonymous remailer network. That is, each packet was encrypted in layers and forwarded through a sequence of servers. Each server decrypts one layer of the packet. This decryption revealed the identity of the next server in the chain, to which the packet is forwarded. Only the last server in the chain saw the final destination of the packet. No server was aware of the entire path, and so no server could know who is communicating with whom. No one could associate the nym with its owner. In addition to this route encryption, the contents of the packet were encrypted. No server, except perhaps the last in the chain, could monitor the contents of any message.

Although no message was traceable, nyms were persistent. Recipients of mail from a nym could respond to the nym. Websites visited by a nym could set cookies on the machine of the nym owner. The *Freedom* system intercepted and segregated those cookies, placing each in the ‘cookie jar’ of the nym that was operational when the cookie was received.

Compared to Canada's PKI, *Freedom* was technologically complex, but institutionally simple. Naming was highly decentralized. User's chose their own nyms on a first-come first-served basis. There was no linking among nyms – Zero-Knowledge, as its name implies, had no ability to link nyms to embodied users. The most grievous action Zero-Knowledge could take was to remove a nym from the system.

Constitution of subject and context

- What attributes of the subject are known? How is the subject understood and constituted?
 - From the perspective of data collectors and other online co-participants, nyms looked very much like any other person online. They looked like an e-mail address, a style of writing, a set of cookies, a pattern of web interactions. Nyms were subject to all of the standard data-collection processes of the internet: registration forms, cookies, mailing list archives and search engines, etc. However, in breaking the link between nyms and the embodied individuals who animated them, nyms themselves became principals. A single embodied individual could vitalize any number of nyms, each with its own data trail and online reputation.
- In what context is the subject known?
 - Nyms lived and were known on the internet - in mailing lists, chat rooms, and the profiling databases of web sites. Yet each nym was known in its own subset of the internet. There were very strong design factors

inhibiting users from linking their nyms and a very strong emphasis on the segregation of nyms. (Phillips 2002)

- What attributes of context are known to the subject?
 - It is notoriously difficult on the internet to understand to whom one is visible, who is present in an online context and what signals are being gathered and interpreted and by whom. *Freedom* did nothing to make online contexts any more visible or comprehensible to its users. Indeed, privacy laws might not even apply to *Freedom* users, since information referring to a nym might not be considered “personal” information, since it can’t be linked to a locatable individual. (See Phillips forthcoming)
- What possibilities does it afford subject of influencing, or being influenced by, context?
 - In theory, and in the hopes of its designers, *Freedom* permitted of vocality and innovative performance. It was specifically understood and intended by ZeroKnowledge Systems KS to promote online presence of stigmatized identities or sensitive issues (specifically issues of finance, health, and sexuality).

State of deployment

Freedom was deployed in the dotcom boom, with world-class cryptographic expertise and significant financial backing. While the financial resources of ZeroKnowledge may have paled in comparison to those of the Canadian federal government or of the Microsoft Corporation, nevertheless they permitted the company to

hire hundreds of employees and refurbish thousands of square feet of office space in downtown Montreal. However, their market strategy depended on uptake by end users, specifically those concerned with privacy. They also published the client software in open source, hoping to leverage the expertise of an impassioned community of programmers and entrepreneurs and spur the development of many front-ends to the network, creating more end users and subscribers to the network. However, public mobilization simply did not occur, and the network was taken offline in October 2001.

Microsoft .net Passport

Microsoft's Passport is a centralized database which serves identifying, authenticating, and descriptive information to various entities as a user traverses online contexts. The following description relies on Microsoft's ".Net Review Guide" (Microsoft Corporation 2003b).

The Passport database consists of records, which themselves consist of credential information fields, profile information fields, and a unique ID for each record. Credential information fields are the user's e-mail address and password. Profile information fields are name, credit card information, address, gender, occupation, state, ZIP code, time zone, birthday, and language preference. When a user registers for a Passport, she is required to fill out the credential fields. Profile fields are optional.

When a user logs in at a Passport-affiliated website, she is referred to the Passport site. There she logs in with her e-mail address and password. If the login is successful, she is returned to the affiliated site. The site also receives her unique ID, both authenticating and identifying her.

In this way, users need remember only one login name and password. Sites receive persistent identifiers from each user without the use of persistent cookies, and can then track the user through session cookies and the user's persistent, unique, Passport ID.

In addition to the unique identifier, users can opt to permit Microsoft to deliver some personal data to the site. The user may opt to send her e-mail address, her name, or all profile information to every site she logs into with her Passport. She cannot decide to have Microsoft divulge different information to different sites. Additionally, the site receives a flag indicating whether the user is registered in the Hotmail directory. This directory permits someone to send e-mail to a Hotmail account knowing only the recipients name, and without learning her Hotmail e-mail address. (Microsoft Corporation n.d.)

Participating sites are forbidden by contract to set persistent cookies containing personal info. Nor are they permitted to use the Passport profile information without user's prior consent, except to deliver goods and services. Additionally, the site must post a privacy policy and must be P3P enabled.

- What attributes of the subject are known? How is the subject understood and constituted?
 - The subject is understood as two linkable segments: a single, persistent and identifiable set of demographic information engaged in a pattern of web activity, and a human being animating that pattern. The link between those segments (that is, "identifying information" such as names or e-mail

addresses) is activated only under certain conditions, nominally controlled by the human being, and administered by Microsoft.

- In what context is the subject known?
 - The subject's identifier and demographic description are identical across all sites, though each site will have a different concept of how that subject interacts with the site. For each site, the subject is persistent across time; sites see the same entity with each visit. The subject is unary, that is, it is difficult to maintain more than one Passport persona at the same site.
 - A different subject is known to Microsoft and to available to law enforcement. This is the complete set of demographic and identifying data, as well as a record of login attempts.
- What attributes of context are known to subject?
 - Passport does incorporate an attempt to make the online context visible to the subject by requiring that participating sites post a privacy policy and incorporate P3P. However, these are notoriously difficult tools to use and interpret.
- What possibilities does it afford subject of influencing, or being influenced by, context?
 - The subject has some ability to influence the context in which she is known. The use of P3P gives her some power to avoid sites with certain privacy policies. Theoretically, though perhaps not practically, this gives her some market power to influence those policies. However, she is a

“contract taker” in these instances. Her only option is to accept or reject the policies offered by the site. She cannot negotiate with the site. Unlike Canada’s PKI, the site is under no obligation to provide equivalent services if the subject decides to opt-out of the Passport system.

State of deployment

Passport is certainly the most successful identity management scheme studied here, in the sense that it is most seamlessly integrated into everyday practice. Microsoft claims over 100 participating sites, over 20 million users, and over 3.5 billion authentications per month (Microsoft Corporation 2003b, Smith 2002). This success is largely due to Microsoft’s ability to bundle the system into other systems in which it enjoys market dominance. For example, users of Microsoft’s free e-mail service, Hotmail, as well as its ISP, MSN, are automatically registered with Passport (Microsoft Corporation 2003a). Early releases of the latest version of Microsoft’s monopoly operating system, Windows XP, repeatedly urged users to sign up with Passport, though later versions deleted this “hard sell” (Schwartz 2002). Nevertheless, .Net is integrated into XP’s credential manager, which gives the user the option of signing into Passport whenever they sign into XP (Microsoft Corporation 2003b).

Other factors have influenced the current shape of the Passport system. The U.S. Federal Trade Commission charged Microsoft with making false claims about the types of data collected under the system, and the security with which that data was protected. In August, 2002, Microsoft agreed to stop making such claims and to submit to an external audit every two years (Schwartz 2002). In January of 2003, Microsoft agreed to

alter Passport in order to comply with the European Union Data Directive. These changes included the user's ability, such as it is, to choose what data is distributed to participating sites, as well as notice to EU customers of their rights under the Data Directive (Meller 2003). For the most part, these policy actions tended not to alter the structure of the Passport system, but to make that structure more visible, both to regulators and to users, and to give it a certain official imprimatur.

CONCLUSION

In the introduction to this paper, we suggested that a socially empowering information systems would permit subjects to negotiate both contexts and identities. This would involve awareness of and influence over the models and data which constitute individuals in information environments, as well as awareness of the context itself. That awareness includes not only awareness of the scope of the context (that is, to whom one is visible, and the duration of that visibility) but also of the social rules influencing behavior and reaction in an environment. This concluding section reviews the models of contextualized identity, suggesting in what ways they meet these ideals. It also reviews the forces which permit certain paradigms to become dominant, and suggests reactions to those forces.

Canada's PKI limits subject to one identity within the PKI. Subjects' roles are quite circumscribed: they are CA's or not, they are citizens or employees in relation to the government. The scope of the PKI is correspondingly limited – specifically to interactions with the Canadian government. However, the system is also intentionally a first step toward a generalized infrastructure for electronic commerce. There are several

implications for this. First, it acts very much within, and so reinforces, the ideology of liberal bureaucratic democracy. The system itself is developed and operates within laws and policies that are, formally at least, decided via representative democratic processes. Secondly, as it reproduces the citizen, it also reproduces the market participant. It fundamentally understands and reproduces the subject as a unique, free, and contract-making individual. The purpose and effect of the system is to translate and reify enforceable contracts between individuals and organizations in new information environments. In its very formality, predictability, and conservativeness, it is in a sense familiar. It is available for relatively standard embrace or critique. It affords a ready cultural handle on how to manipulate and use it.

Freedom affords multiple individual personae, and very strong segregation of online social contexts. However, it offers little to help users understand the milieu in which they find themselves, or to understand how they are understood within that milieu. While it was fairly well integrated into technical infrastructures, in that it operated more or less seamlessly with various internet protocols, it was not well integrated into social infrastructure. It was never really clear to users why they would want, or what they would do with, a set of pseudonyms. It always enjoyed a certain radical cachet, a cutting edge bravado, that made using it seem like trailblazing. And trailblazing is hard work.

Passport reinforces the notion of the self as demographic pattern to be revealed or concealed as part of a market strategy. While literally conforming to privacy laws and to common notions of appropriate privacy policy, it in fact reifies and reinforces the ideologies subtending those laws and policies. That is, that we are everywhere a single

individual moving from one unrelated market to another, with the state overseeing all in the name of order and security. In this, it shares its ideology with Canada's PKI. However, Canada's PKI and Microsoft's Passport have entered the infrastructuring process from diametric points. Canada's PKI has been designed primarily to constitute the citizen. It has been policy driven from the start, and subject to the bureaucratic and democratic checks and balances of any federal project. Passport, on the other hand, is private and proprietary, designed from the beginning to facilitate and rationalize the distribution of demographic subjects. Passport gives primacy to the subject as market data. Those subjects are citizens only in that their constitution is constrained by certain policies; they are not fundamental to the policy process itself. By deploying a private infrastructure, integrated only peripherally with public institutions, Passport reifies online environments as private space, to be shaped and structured by market forces. Contracts are ascendant over policy. Those who can influence the infrastructure are exactly those with organized market power. A notable exception to this is the power of police, under subpoena, to use the data portions of the Passport system in any way they choose.

Microsoft, though its dominance in software and consumer-based online services, has unquestionably enjoyed the most considerable power in the deployment of its understanding of the subject in online context. That subject is a targeted consumer; her environments are markets. The subject of Canada's PKI is the bureaucratic citizen, her environment is the government. *Freedom* constituted the subject as a voice, a presence whose environments were particular subsets of the Internet. Both Passport and Canada's PKI are committed to unary subjects. That is, each embodied individual is to have one

legitimate online persona. Freedom's fracturing of the individual made it impossible for the system to be integrated with the cultural, legal, and market paradigms to which both Passport and PKI are committed. Yet that fracturing of the individual, and the informational chasm between online persona and embodied animator, theoretically permits the sort of play with identity and context that would allow individuals and groups to deeply influence the structure of information environments and the social relations within them. It was neither Microsoft's market dominance nor the existence of Canada's PKI that prevented this theoretical possibility from becoming social practice. Few people really seemed to want to play with online identity and context. Not to be too paternalistic, it falls, then, to policy makers and social activists to ensure that contexts other than markets, and identities other than consumers, exist online.

REFERENCES

- Adams, Carlisle and Steve Lloyd. 2003. *Understanding PKI: Second Edition*. Boston, MA: Addison-Wesley.
- Bechtold, Stefan. 2003. "Symposium: Ican Governance: Governance In Namespaces." *Loyola of Los Angeles Law Review* 36, p 1239-1320.
- Butler, Judith. 1998. "Imitation and Gender Insubordination." *The Critical Tradition: Classic Texts and Contemporary Trends. 2nd Ed.* David H. Richter, Ed. New York: Bedford/St. Martin's, p. 1514-1525.
- Giddens, Anthony. 1984. *The Constitution of Society*. Berkeley: University of California Press.
- Goldberg, Ian and Shostack, Adam. 1999. "Freedom 1.0 Architecture and Protocols." http://www.freedom.net/info/freedompapers/Freedom_Architecture_protocols.pdf. Accessed 12 January 2000.
- Meller, Paul. 2003 (January 31). "Microsoft to Alter Online System to Satisfy Europe." *The New York Times*: W 1.
- Microsoft Corporation. 2003a. "Microsoft .Net Passport: Q&A for Consumers" <http://www.passport.net/consumer/consumerQA.asp?lc=1033>. Accessed 15 September 2003.

Microsoft Corporation. 2003b (June) “.Net Review Guide.”

http://www.microsoft.com/net/downloads/passport_reviewguide.doc. Accessed 21 August 2003

Microsoft Corporation. n.d. “What is the Hotmail Member Directory?”

[http://help.msn.com/EN_US/data/hotmailv2_2.its51/\\$content\\$/WhatMemDir.htm](http://help.msn.com/EN_US/data/hotmailv2_2.its51/$content$/WhatMemDir.htm)

Accessed 3 September 2003.

Phillips, David J. 2002. “Negotiating the Digital Closet: Online Pseudonyms and the Politics of Sexual Identity.” *Information, Communication, and Society* 5(3): 406-424.

Phillips, David J. Forthcoming. “Privacy Policy and PETs: The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies.” *New Media & Society*.

Schwartz, John. 2002 (August 9). “Settling With F.T.C., Microsoft Agrees to Privacy Safeguards.” *The New York Times*: p. C 6.

Shaw, Bernard. 1951[1916]. *Pygmalion*. Baltimore, MD: Penguin Books.

Shaw, George B. 1964[1919]. *Heartbreak House*. New York, NY: Penguin Books.

Smith, Seagrump. 2002. “Microsoft and the European Union Face Off Over Internet Privacy Concerns.” *Duke Law & Technology Review* 14.

Susan Leigh Star and Geoffrey C. Bowker. 2002. 'How to Infrastructure' pp 151-162 in *The Handbook of New Media* (Leah A. Lievrouw and Sonia Livingstone, eds.) Thousand Oaks, CA: Sage.

Treasury Board of Canada Secretariat. 1999 (May 27). "Policy for Public Key Infrastructure Management in Canada" http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki-PR_e.asp?printable=True. Accessed 2 September 2003.

Treasury Board of Canada Secretariat. 2001a (21 June). "Government of Canada PKI." http://www.cio-dpi.gc.ca/pki-icp/gocpki/gocpki_e.asp. Accessed 3 September 2003.

Treasury Board of Canada Secretariat. 2001b (21 June). "History." http://www.cio-dpi.gc.ca/pki-icp/gocpki/history/history_e.asp. Accessed 3 September 2003.

Treasury Board of Canada Secretariat. 2002a (17 June). "Pathfinders." http://www.cio-dpi.gc.ca/pki-icp/pki-in-practice/pathfinders/pathfinders_e.asp. Accessed 3 September 2003.

Treasury Board of Canada Secretariat. 2002b (17 June). "Success Stories." http://www.cio-dpi.gc.ca/pki-icp/pki-in-practice/success-stories/success-stories_e.asp. Accessed 3 September 2003.