Joichi Ito

Identity and Privacy in a Globalized Community

From Atoms to Bits

In his *Wired Magazine* column of January 1, 1995 “Bits and Atoms” Nicholas Negroponte’ describes the shift in focus from atoms to bits.[1] The shift from atoms to bits is still one of the most significant shifts impacting society today. As with most technical trends, people have over-anticipated the short term impact (the dot-com bubble) but have severely under-estimated the long term impact.

The Impact of Digital Communication Networks and Globalization on Identities and Nations

The industrial revolution triggered a cultural shift causing nations to become powerful entities in a globalized geo-political world. The world began to focus on the products of mass production and the world began to focus mostly on the “atoms.” Individuals became able to travel easily and individuals began to be identified and tracked as physical units and physical borders were rigorously managed. Digital communication technology and cyberspace has increased greatly the power and value of the non-physical world and is affecting the nature of national borders and identity. Here I would like to explore some of the changes facing an era of digital transnational communications, focusing on value shifting to cyberspace and its impact on identity, authentication and privacy.

Scalability of Communications as Profound as Mass Production

Although cyberspace and bits are rather new, non-physical space is an old idea. A major step toward large-scale shared virtual communities and the scalability of communications was the creation of the printing press and the public. The invention of the printing press created another huge virtual world, the world of literature and public opinion. Before the printing press, there was no public. The next and much more significant step was the invention of electronic communications. Electronic communications such as the telephone changed speed and in turn the nature of markets, warfare and politics. The more scalable digital communications and the Internet have allowed the public to wake up from its semi-conscious state to an actively aware state where the public can now think for itself and communicate.[2] The technology of the mass production of physical things allowed a new level of scalability and division of labor to form. During the industrial revolution, markets were suddenly flooded with entities rich from the benefits of the ability to mass-produce, and money became a much more central component of our reality and perception of reality. As Marshall McLuhan points out, the metaphors and language we use mold very much what we can imagine or do.[3] The abstract management of resources was possible in the modern world of mass production. Yet, money generally represented atoms, most companies in the 1920’s being valued primarily according to the value of their physical assets.

As information technology has made communication and the transportation and the management of bits scalable and low cost, more and more of our wealth represents information—information about atoms and information about information. Companies are now generally valued at premium on the value of their physical assets. This “Intellectual Capital ” is the value of the information and other intangible assets held by the company. More and more of our value, identity and time exists in the digital world.

John Perry Barlow once described cyberspace as “where your money is.”[5] Cyberspace is not just the Internet, but everything digital. The balance of your bank account is just some entry in some computer. This value is information about information about some value somewhere, but much of it is self-referential and mostly very contextual.

Entities Beyond Physical

There are many instances where entities exist primarily in the digital world.

MUD’s

MUD’s are multi-user role playing games where players invest thousands of hours developing characters which own assets, have attributes and relationships with other players. The time and the knowledge of the players is invested in the game and the game becomes a rich highly contextual entity in the digital world which one could argue has substantial control over its representatives in the physical world.[6]

VISA

VISA for many years was just a contract between its members who wished to perform transactions electronically. The members created the rules and the system was completely distributed and each member was responsible for their own risk. VISA was able to be a brand recognized entity when necessary, but could disappear from regulators because it was not a legal entity and did not have a physical location.[7]

Multi-national corporations

Multi-national corporations or “legal persons” often have the benefit of existing in a limited liability state of global distribution, but often also suffer from the paralysis of being exposed to multiple jurisdictions because of the necessity to interact to a great extent with the real world.

Identity

Most people believe that identity is simply one’s name, age, sex and address. In fact, we all have multiple identities that are aspects of the entity which is uniquely human,

being flesh and blood as we are. Actually, companies, government agencies and political bodies are also entities. Identities can be roles such as shareholder, officer, rape victim or spouse. Identities are identified by identifiers. Some identifiers require the authentication of the entity whereas some identities can be authenticated by uniforms, passwords, secret hand-shakes or other identifiers which do not expose the entity behind the identity.

It is essential to consider the issue of identity independently from the issue of authentication of the entity. When one is engaging in a transaction with some identity, one is concerned with the risks and attributes of the identity with respect to the transaction. When one is trying to sell diamonds, one is concerned with the authentication of the other identity's financial attributes. If one is trying to receive donated blood, one is concerned, not with who it came from, but the type and whether it is safe. If one is selling liquor, one is concerned with the age of the purchaser, not the address.

It is true that for many transactions, it is necessary to authenticate the entity, but often knowing the name, age, sex and address of the entity one is interacting with gives us no value. For police dealing with entities within their jurisdiction, the authentication of the identity gives them to ability to throw the entity in jail, but for most of us, the reputation of the entity, cash on hand, validity of the third party insurer or some other attribute is probably more important. With the global Internet, the ability to punish an entity beyond the borders of our community does not generally exist. For this reason, authentication of the entity is much less important than the authentications of identities and the attributes of these identities.

In fact, in many cases, it is essential that the entities are not identified and are able to remain anonymous. When one asks questions at a public help desk, or consults someone about sexual abuse inside of an organization, or tries to reveal information about war crimes in inside of a country ruled by an oppressive government, it is essential that one is able to remain anonymous.

Although pure anonymity is often very important, pseudonymity, the ability for people not to link identities with each other or with the entity, but for the identity to be authenticated, is important. For the sexually abused student who is consulting the counselor, both parties need to know that it is the same identity that they have been corresponding with, but neither need to know the actual name and address of the other. In fact, many common law countries allow people legally to use nick names or pseudonyms. Such pseudonyms are common on the Internet and very useful. The tendency for us to try to force entity authentication on all pseudonyms is a very simplistic and policeman-like view of identity. Pseudonyms are like roles and by limiting their use to transactions or participation in communities where reputation or other forms of collateral like attribute can be secured, they can be regarded as a very important and functional tool.[8]

Privacy

Definition

Roger Clarke defines privacy as "Right to privacy is the freedom from unreasonable constraints on the construction of one's own identity" and calls this digital identity a Digital Persona.[9]

As law enforcement, national security interests, political interests and commercial interests continue to collect more and more information about us and trade and

analyze this information, a great web of databases of digital identities are created linking physical entities to a massive dynamic body of information which represents our digital personas, their attributes and the relationships between these personas. We currently have very little control over how these personas are formed and managed and often we do not even know they exist.

The future of privacy, as Roger Clarke describes, lies in our ability to manage the construction of one's identity. In order to do this, one must understand the current state of privacy, the threats to privacy and technologies and methods that can better protect our privacy.

The EU Directive on Data Protection[10] and most of the world's privacy policies are based on the OECD's 8[11] guidelines on privacy that deal more with data protection than data format and architectures. These guidelines were written over 20 years ago when we were dealing with large mainframe computers, centralized databases and very little trans-border dataflow. Today, we are dealing with a distributed network, much more computing power and much more invasive data collection. The EU Directives talk about destroying information when it is no longer needed. In today's world, it is impossible to destroy information once it is created. It lives on in traces on hard disks, backup tapes, log files, surveillance databases. Once information has been created, it is important to assume that it will one day become public. Therefore, what is essential today is for us to manage the creation of information about ourselves. The best policy is to create information only when necessary and disclose only the information necessary for the particular transaction. It is essential to keep identification information to a minimum and to keep identifiers as separate as possible in order to make it difficult or hopefully impossible for the information about a particular transaction to be used in ways unknown or unintended by us.

Law enforcement and national security concerns are pushing money-laundering laws to make our financial privacy illegal. They are trying to implement a myriad of biometric database to link information about our identities to our physical entities to be able to profile and model individuals. All of this information greatly enhances their ability to find and capture criminals, terrorists and other people who are not friendly to their concerns. Much of what these agencies do is essential for order in the world, but most criminals intentionally avoid identification and regularly thwart efforts by authorities to track them through such methods. In the meantime, great databases of the profiles and relationships of regular citizens end up being compiled and these databases can and will be abused by governments, politicians, organized crime and eventually terrorists. The greatest threat to the freedom of individuals in our great new globalized information economy is the "ends justify the means" sort of thinking prevalent in counter-terrorist and law enforcement agencies without thorough consideration of the risk that such massive surveillance means for the freedom of normal individuals.

In fact, law enforcement and spies have more technology than ever before. They can read licence plates from spy satellites, recognize voices on telephone lines with computers, plant microscopic tracking devices and genetically identify strands of hair. Our fears are increased by fraud committed by trusted executives, terrorist attacks, computer viruses and a variety of new threats. We need to be aware that throwing away our privacy and giving unlimited access to government agencies will not solve these problems.

Privacy enhancement technologies and architecture

In the past, being a privacy advocate meant that one was anti-information technology. Most information technologies in the past calculated things such as the efficiency of factory workers or sorted people to send them to concentration camps. Today there are many technologies that protect or enhance privacy.

For instance, David Chaum's blind signature technology allows users to authenticate the fact that a piece of digital cash is authentic, but allows the users to remain anonymous. This allows us to create the digital equivalent to real cash. This could create problems for agencies trying to clamp down on money laundering, but it could also help protect the privacy of activists in a totalitarian regime.

Huge databases of fingerprints or other biometric information can be very invasive and potentially dangerous, but companies such as Mytec Technologies of Toronto are working with technologies which allow the biometric information to be stored on the user's card, rather than in the database. The organization uses cryptographic technology to authenticate the validity of the information in the card and provides access with a card and biometric combination, but does not retain an image of the fingerprint, retina or face that might be used to provide access.

Zero Knowledge Systems provides a set of products that help users manage their identities, the cookies they receive, the privacy policies of the sites that they visit and a variety of other things that are usually not visible or selectable to the user.

Eric Hughes once talked about the "open book protocol" which describes an encrypted accounting system that allowed people to audit a group of linked accounts while retaining the privacy of the individual entries.

Pharmanet in British Columbia, Canada, through the insistence of Mr. Flaherty, the Privacy Commissioner, allows patients to assign a password to prescription records.

I have proposed an idea as a replacement for profiling, database marketing and recommendation engines. If one were able to store on some small device or IC card, a local profile of one's shopping habits and one's computer or phone had a recommendation engine built in, shops and online merchants could provide us with the profile of the products and we could recommend things to ourselves. This would allow much higher privacy than the current system which profiles users on the merchant's servers. My method is also superior because one's profile could help recommend products even on a first visit to a site. The difficulty would be in standardizing the product profiling codes.

The Internet itself has become a method for activists to organize and disseminate information. A new breed of privacy activist exists who uses technology and tries to come up with technical methods for protecting privacy and, most importantly, tries to influence the architecture of computer and network systems.

Lawrence Lessig-Code

Lawrence Lessig in his book *Code*[14] describes how computer codes are like laws and the architecture of databases and networks like politics. It is this war over architecture which occupies the battles of the digital privacy activists. New data formats will make it easier and easier to merge databases and link isolated transactions for bits of information about individuals. It is cryptography that will create the boundaries and limit the use of information.

Cryptography provides us with the tools to communicate securely with authenticated peers. Cryptography allows us the flexibility to create a variety of architec-

tures. Authentication systems range from centrally controlled to completely distributed systems. Identification systems range from totally anonymous to pseudonymous to identification of entities. Cryptography gives us the ability to make technically possible what we want possible and make technically impossible that which we decide should be impossible. Creative use of cryptography allows us to trust whoever we would like to trust and be seen with, and communicate with only those we wish to communicate with and keep separate and unique. Each community and the group of identities in that community can have its own rules and architecture with the proper cryptographic technologies supporting it. According to Philip Agre, privacy is no longer a simple discussion of "the simple tradeoff between privacy and functionality" but a "more complex tradeoff among potentially numerous combinations of architectures and policy choices." [15]

Online Communities[16] and Reputation Capital

Online communities such as mailing lists, conferencing systems, online games, online auctions sites, networks of BLOG's and the Linux community represent communities that have many of the same attributes as nations.

There are many fundamental differences, but one of the biggest differences is that, because of the lack of physical access and usually the lack of the ability to access directly the entities behind the identities, these communities have to govern themselves without the ability to punish the entities behind the identities physically, such as throwing someone in jail.

The two most important items that a community has to manage for its participants is the securing of reputation which can take the form of personalities developed through interaction, attribute points in games, reputation points on eBay or ability to influence and participate in development in the Linux community. It is this reputation and the ability to take away access to the identity tied to the reputation which help enforce the rules and behavior within the community.

In fact, this is not just an online phenomenon. Organizations such at the WTO use membership and trade sanctions rather than physical attacks as its primary method of enforcing its rules. These are processes that are in place with any community, but the online versions are unique in the ability to attach these processes to online personas as opposed to identities tied to physical bodies.

In this way, communities that provide value for their members can govern themselves and manage accountability without access to the physical entities, and provide us with a model for pseudonymous networks.

Culture, Communities and the Sovereignty of Nations

As the events of the last year have shown us, it is very difficult for many communities to occupy the same space. Each community has its own culture and rules and each makes sense in its own context.[17] Before, all we needed was the ability to physically isolate the incompatible communities and create a sense of identity within these borders, and sovereign nations and physical borders helped to do this. Now with globalized media, the economy and the Internet, people occupying the same space can have access to multiple cultural contexts.

We have spent the last 20 years trying to get everyone connected together in the "Global Village". The problem with the global village is that it is impossible to create a "Global Culture." The solution is to increase tolerance for different

cultures, but also to allow different cultures to co-exist by creating distinct boundaries between communities, each with its own rules and culture. It is diversity that makes gene pools, politics and the Internet robust.

Each community will be able to interact with other communities based on bilateral or global rules. Each community will be able to enforce its rules through its ability to sever ties with communities or individual identities.

Human beings will continue to be physically exposed to the rules of the nation where they live, but digital personas will be able to freely associate with and join communities globally and will be governed in each community based on the rules of those communities.

Governments currently try very hard to extend their jurisdiction beyond their physical borders, examples being the French concern over Nazi paraphernalia on Yahoo or the American "War on Terrorism." Most nations try to tax income and track the assets of their citizens beyond their boundaries. Eric Hughes once said, "You can't tax what you can't point a gun at." The difficulty that these nations face is that unlike the days when our assets were physical, there is really very little to prevent digital assets from moving freely and the cost and difficulty of enforcement becomes extreme. Global companies will choose tax havens to set up their funds, countries with loose labor laws for their factories, and countries with good food to host their board meetings. Nations should view themselves more as service business´s landlords, their taxes being the price and their rules, infrastructure and culture being the services they provide. Physical nations that provide physical services can and will charge for these services in the form of tax or service fees. The easiest way to levy such a tax is where the money enters the physical world, such as in the form of consumption tax. Other service providers for non-physical services, such as online security, transactions, underwriting and data protection, can charge for their services in the form of transaction fees or service fees. There will be additional layers of services where the physical nation-states and commercial entities meet and overlap. Yet, these borders are already quite blurred. Some people in the UN are calling for the more active use of mercenaries to fight their wars and many agencies of governments in countries such as Singapore are very hard to distinguish from commercial entities. In the future, nations will mostly likely be more concerned about trying to be popular and maximizing the value created by their tax income rather than trying to forcefully beat their own culture into the hearts and minds of the global community.

Conclusion

In the new world of colliding cultures, a blurring of physical and virtual identities and a dissolving of the sovereignty of nations, governance and order become the crucial issue. One thing that the Internet has taught us is that very difficult problems can be solved by unbundling the pieces and creating protocols for each of the layers or objects to interact and work together. The Internet has also taught us that no one has to be "in charge." (When people try, they fail. See ICANN.) The key to success in governing the communities of the future will be a combination of global rules and practices for trade and interaction and technical architecture that allows communities to be independent and separate from each other. Conduct in the physical world will be governed by physical nations and physical policemen while conduct in the virtual world will be governed by the rules and

methods of each of the virtual communities. Protocols will have to be created and enforced by both virtual and physical communities where the bits change to atoms and vice versa. It is this protocol that will be the core issue and topic of debate between computer scientists, lawyers, politicians and citizens for the years to come and the answer will be as much technical as it is legal.

See *www.neoteny.com/jito/english/notebook/privars.html* for updates

---

1 Negroponte, Nicholas. "Bits and Atoms," *http://web.media.mit.edu/~nicholas/Wired/WIRED3-01.html* (June 4, 2002). *Wired Magazine.* January 1, 1995.

2 See de Kerckhove, Derrick.Connected Intelligence. Somerville. 1997.

3 McLuhan, Marshall. The Gutenberg Galaxy. Routledge & Kegan Paul, London, 1962.

4 Edvinsson, Leif and Malone, Michael. Intellectual Capital. HarperBusiness, 1997.

5 It is not clear when John Perry Barlow started saying that cyberspace was "where your money is," but many people quote him. Barlow, John Perry. Barlow Home(Stead)Page *www.eff.org/~barlow/barlow.html* (June 4, 2002).

6 Mizuko Ito describes people who play MUD's and the level of reality that these identities assume. See Ito, Mizuko. *Cybernetic Fantasies: Extensions of Selfhood in a Multi-User Dungeon.* Paper presented at the 1994 meetings of the American Anthropological Association, Atlanta *www.itofisher.com/PEOPLE/mito/Ito.AAA94.pdf* (June 9, 2002)

7 Dee Hock is the founder of VISA and describes his VISA and the distributed nature of the organization in his book. See Hock, Dee. *Birth of the Chaordic Age. www.chaordic.org/* (June 4, 2002). Berret-Koehler Publishers Inc. , San Francisco, 1999

8 Roger Clarke describes clearly the various types of identities and the difference between entities and identities. See Clarke, Roger. *Authentication: A Sufficiently Rich Model to Enable e-Business. www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html* (June 9, 2002)

9 Roger Clarke coins the phrase "Digital Persona" and ties it to a discussion of privacy. See Clarke, Roger. "The Digital Persona and its Application to Data Surveillance." *www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html* (June 2, 2002)

10 "The European Directive on Data Protection" *www.privacy.org/pi/intl_orgs/ec/eudp.html* (June 9, 2002)

11 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data *www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM* (June 9, 2002)

12 *www.mytec.com/* (June 16, 2002)

13 *www.zeroknowledge.com/* (June 16, 2002)

14 Lessig, Lawrence. Code and Other Laws of Cyberspace, Basic Books, 1999.

15 p. 5., Agre , Philip E. and Rotenberg, Marc. Technology and Privacy: The New Landscape, The MIT Press, 1997.

16 One of the first books about online communities. Rheingold, Howard. The Virtual Community: Homesteading on the Electronic Frontier, *www.well.com/user/hlr/vcbook/* (June 9, 2002) Harper Perennial., USA, 1993.

17 For a discussion on how difficult it is for different cultures to co-exist and the impact that culture has on the basic nature of a community, nation or civilization see Hall, Edward, T. Beyond Culture, Anchor Press., Garden City, N.Y.,1976.