

STRATEGIC ISSUES SERIES

rp02-9e

SOCIAL IMPLICATIONS OF CURRENT
TRENDS IN INFORMATION /
COMMUNICATION TECHNOLOGIES

Andrew Clement
Associate Professor
Coordinator, Information
Policy Research Program
Faculty of Information Studies,
University of Toronto

with the assistance of

Craig McTaggart and Felix Stalder



Research and
Statistics Division

2000

The views in this discussion paper are those of the author and do not represent the views or positions of the Department of Justice, Canada. The paper was commissioned as an opinion piece to stimulate research and discussion.



Strategic Issues Series

The Research Papers included in the Strategic Issues series generally have been prepared for the Statistics and Environmental Analysis Unit of the Research and Statistics Division (RSD). This series is part of the Research and Statistics Division's efforts to look ahead and to scan the environment to provide contextual facts and perspectives on a wide range of social and economic issues. Topics covered include: the policy challenges of bio-technology and genetics; speculation on markets for crime and a proposed typology for understanding crime; the impacts on children of divorce and separation; globalization; and global governance of the Internet.

The papers that will be included are thought-provoking. In general they have been written by academics whose commission instructed them to be wide-ranging in their critique of current practices and provocative in their suggestions for new approaches.

Discussion papers and think pieces in this section of the RSD library have already stimulated discussion for exercises such as: new mandate planning, strategic policy planning by senior executives or as backgrounders for research planning. It is our intention to offer them here so that they now can contribute to wider discussion among researchers and policy-makers.

For further information, please contact

Valerie Howe, Senior Research Officer
Telephone: (613) 957-9597, E-mail: vhowe@justice.gc.ca

Biography

Andrew Clement is an Associate Professor in the Faculty of Information Studies at the University of Toronto and coordinator of the Information Policy Research Program with an interest in the social implications of information technologies. He is also active in the Information Highway Working Group, a coalition of public interest groups which seeks to ensure that citizens' interests and needs are a primary focus in the public policy debate around Canada's 'Information Highway'. Dr. Clement is principal investigator of a 3-year SSHRC strategic grant entitled "Developing Information Policies for Canada's Information Infrastructure: Public Interest Perspectives"

He has completed research projects for the Federal Government in areas of access to information systems and is co-author of:

1998. Clement, A., & Shade, L.R. "Debating Universal Access in the Canadian Context: Public Interest Organizations and the Information Highway Advisory Council", in *Internet and Politics*, Maar, C., & Leggewie, C. (editors), Bollman Verlag, Mannheim.



1.0 Introduction

We are currently experiencing a period of extraordinarily rapid development of information/communication technologies (ICTs) with widespread social ramifications. The most prominent of these developments are those accompanying the rise of the Internet as an increasingly integral aspect of many transactions in daily life. The pace, scope, and complexity of the changes pose severe difficulties in making sense of what is actually going on, let alone figuring out how to influence development in positive directions. The pervasive hype, largely self serving, that surrounds ICT development compounds the challenge of thinking clearly about these important phenomena. A short paper such as this can therefore only attempt to clarify some of the most serious misconceptions concerning current trends and make suggestions about a few of the issues that have been inadequately treated in the prevailing discussions. A unifying theme that runs through the paper is the continuing need for responsive public oversight.

Making Sense of the Internet: Some Key (Mis)conceptions

Probably the biggest obstacle to understanding better ICT development and its social implications is the widespread assumption that the social effects flow directly from inherent characteristics of the technology. Popular versions of this “technological determinism” claim that the “impact” of the Internet is inevitably such and such – e.g., “the Internet will bring democracy” or “the Internet is destroying families” or “the Internet is reuniting families.” While this makes for eye-catching headlines and reassuring advertising slogans, its constant repetition misleads us muddles by obscuring the role that social factors play in mediating practical outcomes of ICT implementations.

*While the rapid growth in what ICTs **can** do is intriguing and important, what matters much more is what people **actually** do. This involves the complex interplay of a host of social, political, organizational, cultural, psychological, aesthetic, economic as well as technological factors.*

While the rapid growth in what ICTs *can* do is intriguing and important, what matters much more is what people *actually* do. This involves the complex interplay of a host of social, political, organizational, cultural, psychological, aesthetic, economic as well as technological factors. In particular, a variety of established institutions exert powerful, often stabilizing, influences that may be much more decisive than any technological breakthrough. In significant ways, it is even institutional factors, such as competitive consumer markets and military funding of high tech research, that drive technological change itself. This dynamic relation between social and technological processes leads to contradictory trends. The safest technological projection is that there will be continuing rapid development in capabilities (e.g., memory, processors, transmission). On the other hand, the safest institutional projection is that things will continue much as they have been going. The interplay of the varied factors means a diversity of possible results that are highly contingent on the specifics of the situation. While this makes any sweeping predictions quite unreliable, the outcomes are not simply capricious or random. The good news is that what people chose to do or not can make a real difference. The future course is not predetermined by the technology alone. To varying degrees we all exert some influence.

What we are witnessing is the development of a more complex information ecology in which documents shift back and forth between paper and digital form over the course of their life cycle depending on the specifics of the use situation.

This complex interplay can be seen in the speculations about the future of documents. There are numerous predictions that the growing use of electronic digital representations is making paper-based media (e.g. books, magazines, newspapers, annual reports, contracts, etc.) obsolete. However, casual observation and the growing purchases of photocopiers, printers, scanners and fax machines belies the imminent demise of paper. What we are learning instead is that the creation and use of paper-based documents is highly evolved and surprisingly sophisticated, with each of the various forms tightly associated with a rich set of enduring individual and institutional practices. Paper has particular advantages in many circumstances, which are difficult to replicate with electronic media. What we are witnessing is the development of a more complex information ecology in which documents shift back and forth between paper and digital form over the course of their life cycle depending on the specifics of the use situation. This emergence of hybrid media is becoming recognized by such leading companies as Xerox, which is developing a range of products that eases the conversions between paper and digital forms in both directions. An example is a



photocopier that creates a web page from a paper document while producing a single cover page which when copied, can regenerate the full document from the saved version. Amazon.com is another company successfully pursuing a strategy based on hybrid media - employing digital networks to sell books, of all things.

So digital media are not inexorably driving out the physical, a common myth exemplified by Nicholas Negroponte's *Being Digital*. Rather than attempting bold leaps into the cyber-future, leaving as much of the old behind as possible, we would do better to focus on what Lucy Suchman, an anthropologist at Xerox's Palo Alto Research Center (PARC), refers to as "artful integrations". This requires a careful attention to combining diverse assemblies of social and technical elements, traditional and novel, into working wholes. It also requires a skepticism of simplistic hyperbole.

We will return to this theme of artful integration on the next section. In each of the following issues areas, we will see how the social/organizational/political aspects must be considered along with the technological, in order for us to derive the societal benefits we should expect of ICTs.

2.0 Integrating Administrative Systems: The Elusive Search for the Holy Grail of the Seamlessly Integrated System

Drivers of Integration

A longstanding feature of ICT development has been the ambitious attempts to integrate administrative information systems across ever wider organizational regions. The main driving forces are familiar:

- continuing rapid improvement in performance and unit costs of component technologies;
- convergence of disparate media into standardized digital representations;
- pressures to reduce marginal production costs, particularly labour costs;
- inflexibilities of standalone legacy systems;
- enhanced customer service through faster and more informationally refined responses;
- techno/cultural utopian visions of smooth, seamless automaticity;
- contemporary fashion that celebrates the latest, grand high technology; and,
- aggressive promotion by prominent management consulting firms.

The growth of the Internet reflects and amplifies these driving forces by offering a high profile example of the integrative ideal, combining a futuristic vision of boundless potential with the practical benefits of instant access to an extraordinary variety of information independent of location.

However, while the appeal of large-scale integrated administrative systems is obvious, the overall track record of such attempts has been mixed at best, with numerous debacles. In a wide range of fields, including manufacturing, finance, petrochemicals, health, and more recently justice, ambitious integration projects that were launched with stirring proclamations floundered embarrassingly with little to show for the enormous expenses. Given the strength of the forces behind integration, this pattern is very likely to be repeated for years to come unless the lessons of failure are well learned.

Recurring Pitfalls

There are of course many reasons why large projects fall apart, but often they can be traced to fundamental flaws in the way in which the integration project is conceptualized in the first place. The dominant and longstanding paradigm in the systems integration industry assumes that the core informational activities of organizational activities can be adequately modeled through precise, comprehensive descriptions of data and procedures. These descriptions are created through “systems analysis” based on idealized notions of information processes, but seldom through careful observation of the actual practices. Expressed in a variety of charts, tables, formulae and diagrams these descriptions are assumed to reflect enough of the functional needs and organizational realities that at they can be used to drive the design of the computer systems.

Unfortunately, in this enterprise integration approach, existing organizational divisions, traditional practices, embodied skills and other forms of established interests are often viewed as secondary – as outdated, even unnecessary, impediments to change imperatives.

The key feature is usually a central enterprise *data base*, which describes and contains all the relevant information for the enterprise. Once a data item is captured at its source, it can then be instantly available for all subsequent uses throughout the organization. In quite significant ways the system defines the way the organization should work. It therefore requires a close fit between the system and the organization it is intended to serve. Where the organization is large and diverse achieving a good fit is almost impossible. Unfortunately, in this enterprise integration approach, existing organizational divisions, traditional practices, embodied skills and other forms of established interests are often viewed as secondary — as outdated, even unnecessary, impediments to change imperatives. Those opposing the integration initiatives, even with good reason, are typically dismissed as “resistant to change”. At the very least



these non-rationalizable aspects of organizational life don't fit well within the formal description approach and hence are excluded from the process unless they carry significant political clout.

This top-down, “one best way” approach to integration traces its origins to the scientific management movement at the turn of the century, with its most recent incarnation referred to as “business process re-engineering” (BPR). While BPR has claimed some notable successes, it is now widely regarded as having failed overall, often being used more as an excuse for downsizing than delivering the dramatic performance improvements it promises. “Knowledge Management” (KM), currently in vogue as a successor to BPR, is less aggressive in its ambitions, but often reflects a similar approach. This is in part because the management consultants that are leading the shift from BPR to KM (notably Arthur Anderson and Ernst & Young) bring many of their old methods and attitudes with them. This is particularly problematic when firms with predominantly private sector experience apply their models to public sector enterprises without taking account of the key differences.

An Alternative “Artful Integration” Approach

The enterprise modeling approach is not the only way to achieve integration. Instead of making a central database the primary focus, greater attention could be paid to facilitating better communication between the differing organizational units. This would help them improve the sharing of information in ways that take account of their distinctive practices and competencies. Priority could be given to areas where the parties themselves saw greatest mutual benefit from making tighter connections. Some overall coordination would still be required, but much less than with enterprise modeling. Its role would be at least as much to support the wider learning from the on-going experiments in integration as it was to preventing incompatibilities.

This “artful integration” approach is clearly more modest, relying as it does on a series of incremental improvements. It can't claim to achieve total integration in short periods of time, but it is much more flexible and less risky. It allows the individuals involved a much better opportunity to participate more effectively in the development process, thereby bringing their skills and energy to bear on the project. The up front costs are lower and the initial results quicker to achieve.

Interestingly, this emphasis on facilitating communication between independent entities rather than enforcing uniformity of internal processes is analogous to the networking model that underlies the Internet's success. A major virtue of the Internet's communications protocols (i.e., TCP/IP) is that they place minimal requirements on the individual computers while avoid centralized operational administration. This allows a wide range of devices and uses to be added easily. (See Thomas Davenport, “Putting the Enterprise into the Enterprise System”; Carl Baar, “Integrated Justice: Privatizing the Fundamentals”.)

3.0 Digital Identities: Who can we be in cyberspace? (By Felix Stalder)

Social identity, or who we are to the world, is a complex and fluid concept which involves the myriad ways in which we appear to others. It is useful to distinguish between two ways social identities are constructed: the projected and the imposed persona. The projected persona is formed by images we produce for others to see: the clothes we wear, the slang we speak, or the products we buy. The imposed persona is built up from the images others project on us: social stereotypes based on gender, age, authoritative records or casual observation. Projected and imposed persona overlap to a greater or lesser degree, creating a tension which lies at the heart of the dynamic of the individual or collective identity. Social identity, thus, is communicative, it shapes and is shaped by our relations with others.

The emerging information society is characterized by more and more of our relations with others involving electronically processed information. Increasingly our actions leave electronic trails which can be combined into profiles. The more such profiles take on the characteristic of identifiable individuals, the more an identity emerges from this data: the physical identity of an individual has been extended into cyberspace where it is recreated as a digital identity. Roger Clarke has coined the term “digital persona” to refer to this phenomenon – “the model of an individual’s public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.”

Such digital identities are constructed at various places and for various purposes. As transactions between individuals are increasingly conducted on-line, without the ability to verify identities through face to face encounters, organizations are turning to sophisticated technical means to better link the legally accountable human body with the electronic version stored in their databases. An example is the encoding of biometric data (e.g., fingerprints, hand geometry, retinal patterns, etc.) on chip-based “smart” cards. The use of these cards is growing rapidly and could provide the basis for an infrastructure through which people will have to establish their identities for conducting many routine transactions in daily life.

[O]rganizations are turning to sophisticated technical means to better link the legally accountable human body with the electronic version stored in their databases. An example is the encoding of biometric data (e.g., fingerprints, hand geometry, retinal patterns, etc.) on chip-based “smart” cards.... [P]eople [may] have to establish their identities for conducting many routine transactions.



Digital identities are always related to, but never identical with, the physical identity, at the very least because a digital identity is limited to a finite set of digitally encoded attributes whereas the physical identity is not only analogue but also potentially an infinite number of attributes. The difference between digital and physical identity presents new challenges.

Because digital identities never entirely match a person's appearance in physical space, some of the problems of physical identities can be avoided. A person might choose not to disclose, or to alter, certain personal information to avoid negative stereotyping or physical repression. Thus a modified digital identity can increase an individual's scope to express him - or herself. This is amusingly captured in the famous *New Yorker* cartoon, "On the Internet, no one knows you are a dog."

The notion of a digital identity raises a number of conflicting challenges. Since individuals who can alter their appearance in cyberspace, some might be more willing to engage in socially negative activities because they cannot be held responsible for their actions. On the other hand, the growth and integration of databases with personal information diminishes the individual's privacy and potentially extends the influence of institutions over the lives of individuals. The potential for abuse caused by negative intentions or incorrect records is enormous.

The Issues

In ever more situations, a person's digital identity is the first, and often only identity, we encounter in a social interaction. In such situations, the digital identity does not passively mirror the physical identity, but actively shapes, and sometimes outright replaces, the physical identity. The construction of the digital identity, then, is of central importance to the development of the individual in the information society. The two most extreme poles of digital identity are total autonomy of the digital identity (i.e., there is no link between electronic information and physical person) and total surveillance through which every action of an individual is recorded and integrated in a personal profile. Neither of these extremes is realistic, nor desirable. These extremes can be avoided with a careful construction of the digital identity which includes a

The two most extreme poles of digital identity are total autonomy of the digital identity (i.e. there is no link between electronic information and physical person) and total surveillance through which every action of an individual is recorded and integrated in a personal profile... There is a range of identification techniques, relying on public key encryption, that permit the careful balancing of individual privacy rights with organizational needs for accountability.

variety of identification measures. There is a range of identification techniques, relying on public key encryption, that permit the careful balancing of individual privacy rights with organizational needs for accountability. These include:

- Anonymous authentication: a person's eligibility for a requested service, rather than the person's identity, is being checked and recorded;
- Pseudonyms: A pseudonym is an identifier for a party to a transaction, which is not, in the normal course of events, sufficient to associate the transaction with a particular human being. Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. The data may, however, be indirectly associated with the person, if particular procedures are followed;
- Multiple role identities: different digital identities cannot be integrated into one comprehensive profile. Thus different data sets must not be correlatable.

These, and other, approaches to the construction of digital identities can be combined to maximize the control individuals can exercise over their appearance in cyberspace without limiting the potential for governments and businesses to harness the new opportunities.

4.0 Internet Governance: The Internet, global governance, domain name registration (By Craig McTaggart)

While at a general level no one owns or controls the Internet, there are important central points of control and coordinating bodies which influence the way the Internet works. As the Internet has developed, the significance of these relatively informal agencies has increased, along with calls for their formalization. Some of these non-governmental agencies are currently being institutionalized and given responsibility for the management and future development of the core technical functions of the Internet. This process has brought to the fore questions of what the Internet is, who should "run" it, and who owns what elements of it. The resolution of these issues has significant implications for national sovereignty and the public interest.

Institutional Context

While the action of no single institution is absolutely necessary to the functioning of the Internet, the activities of certain agencies are essential to the universal interconnectivity of all participants. Universal connectivity is perhaps the single

* See Shaw, R. Internet domain names: Whose domain is this? In B. Kahin & J.H. Keller (Eds.), *Coordinating the Internet*. Cambridge, MA: MIT Press.



greatest benefit of the Internet—the ability of people from all over the world to communicate with each other over a common platform. These agencies maintain the authoritative “address books” of computers connected to the Internet and lists of “official” standards and protocols for its operation.

These obscure, yet functionally very effective systems of Internet governance have recently gained prominence due to the ongoing reform of the Internet domain name system (DNS). The unimagined growth of the Internet and the equally unimagined commercial value of certain Internet domain names* are forcing Internet participants to consider how to expand the domain name space to accommodate new users.

This reform process has proceeded under the aegis of the United States government, which asserts jurisdiction by virtue of the Internet’s having been invented in the U.S., largely with U.S. government funding. In the summer of 1998, the U.S. Department of Commerce called for the creation of a private, non-profit, “international” corporation to operate the DNS and make policy for the development of the Internet going forward. That entity, known as the Internet Corporation for Assigned Names and Numbers (ICANN) is currently in the start-up phase and is proposed to gradually take over responsibility for the Internet’s coordinating functions from U.S. government contractors.

In the summer of 1998, the U.S. Department of Commerce called for the creation of a private, non-profit, “international” corporation to operate the DNS and make policy for the development of the Internet going forward. That entity, known as the Internet Corporation for Assigned Names and Numbers (ICANN) is currently in the start-up phase and is proposed to gradually take over responsibility for the Internet’s coordinating functions from U.S. government contractors.

ICANN’s responsibilities are:

- 1) establishment of policy for and direction of the allocation of number blocks in the IP address space;
- 2) oversight of the operation of the authoritative root server system;
- 3) oversight of functions and policy related to the coordination of the Internet Domain Name System, including policies for determining the circumstances under which new top-level domains could be added to the root system; and,
- 4) coordination of the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet.

Social and Governance Issues

While these responsibilities sound technical and narrow, in a network environment, where standards and protocols rule, technical decisions have far-reaching policy implications. Internet Protocol (or “IP”) numbers and domain names are essential to one’s participation in the Internet. It is anticipated that more and more types of electronic appliances will be connected to the Internet of the future, and each will need a unique IP number. Management of this scarce resource, until now done in a non-commercial environment, will become a key center of control over the Internet and must be carried out in a non-discriminatory fashion.

The second area of ICANN’s “jurisdiction”, oversight of the operation of the authoritative root server system, is nothing less than the power to determine whether one “exists” or not on the Internet. The “root” is essentially the list of Internet domains, such as “.ca” and “.com”. Control over the authoritative list of domains is an unprecedented “gatekeeper” power over global communication and electronic commerce.

ICANN [controls the] root server system, is nothing less than the power to determine whether one “exists” or not on the Internet. The “root” is essentially the list of Internet domains, such as “.ca” and “.com”. Control over the authoritative list of domains is an unprecedented “gatekeeper” power over global communication and electronic commerce... There is tremendous potential for anti-competitive behavior and interference with individual rights if the above responsibilities are held in private hands.

One can foresee a day when ICANN might receive a communiqué from the United Nations or NATO suggesting that the ccTLD for a particular country be temporarily or permanently deleted from the root server. The effect could rival the military blockades of earlier conflicts if global electronic commerce becomes as significant to the world economy as it is predicted to be. This example illustrates the enormous power which the custodian of the root server will come to wield in the wired world of the future. The extent and implications of this power can probably not even be known at present.

The fourth area of ICANN’s jurisdiction will likely prove to be the most significant in the long term. “Coordination of the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet” is a significant policy statement. The high level of interconnectivity which defines the Internet is the product of a shared belief in interconnectivity for its own sake, with little regard to economic



considerations. As private investment in the Internet has grown, commercial enterprises have begun to question the basis on which various Internet participants share the costs of the operation of the network as a whole. This process, combined with the need to make huge capital investments in “e-commerce” pay off, can be expected to put significant pressure on the Internet as we know it.

There is tremendous potential for anti-competitive behavior and interference with individual rights if the above responsibilities are held in private hands. They were considered to be in the nature of a “public trust” by the members of the small, cooperative community out of which the Internet has grown. The protocols and resources that make the Internet work are open and in the public domain. With the commercial pressures to which the Internet is now subject, the desire of some parties to see its infrastructure change to their benefit may present challenges to the goal of interconnectivity for its own sake. It is worth noting that to date, the largest financial supporters of ICANN have been IBM, Netscape (now owned by America Online) and MCIWorldCom.

The governance role of ICANN and other private Internet bodies will require a careful balancing of the interests of all interested parties. This type of activity is, of course, precisely what governments do. However, ICANN has been designed by the U.S. Department of Commerce to be “free” of “government interference” and to serve as private sector self-governance. Indeed, ICANN will exercise unprecedented private power over what is quickly becoming a public resource. The exercise of that power will have significant impact on the functionality and accessibility of the Internet to citizens all over the world.

While the Internet is frequently touted as existing outside the reach of law and public authority, governments should be watchful of the course of private development and governance of the Internet to ensure that the interests of consumers and citizens are protected, just as they do in the physical world. An excellent discussion of the role of governments with respect to the Internet is found in a draft paper titled “Governance” by Harvard Law School Professor Larry Lessig.

Possible Responses

While the Internet might be characterized as a “private” network, its importance and ubiquity make the governance of its underlying infrastructure a matter of public concern. The technical difficulty of dealing with objectionable content on the Internet highlights the significance of control over those elements of the Internet which *are* centrally administered.

At present, the U.S. government is overseeing the “privatization” of these administrative structures, handing the responsibility to ICANN piece by piece. The United States proposes to withdraw its legal support for this structure completely by September 30, 2000. At that time ICANN will become the completely private, non-governmental “government” of the Internet. The question of who gets to make what

decisions with respect to this global phenomenon is nothing less than constitutional law for cyberspace. Where the lines will be drawn in cyberspace may be no less significant than in the physical world.

While Canada has not made any official public statement to this effect, by participating in ICANN's "Governmental Advisory Committee" Industry Canada's Electronic Commerce Task Force appears to endorse this process.

Further, through its involvement with the creation of a new governance body for the ".ca" domain, Industry Canada has demonstrated both its awareness of the issues involved, and the importance of asserting public values in the governance of the Internet's infrastructure. Canada must remain vigilant and committed to ensuring that the Internet is administered in the public interest.

The United States proposes to withdraw its legal support for this structure completely by September 30, 2000. At that time ICANN will become the completely private, non-governmental "government" of the Internet. The question of who gets to make what decisions with respect to this global phenomenon is nothing less than constitutional law for cyberspace.

If the private sector bodies responsible for the management and future development of the Internet do not prove to be capable of accommodating the public interest in their activities, or if private interests appear likely to significantly change the Internet's fundamental characteristics, then governments should be willing to take the difficult step of finding an international approach to Internet governance. Governments all over the world are learning that national and sub-national approaches to many Internet-related legal issues are simply not technologically possible. Yet many issues, beyond those infrastructure-related issues which have been discussed here, suggest the need for some form of effective public oversight of certain aspects of the Internet. Such oversight may only be possible on an international basis.