Abstract

Strong tendencies exist to apply information technology to support centralist, authoritarian world views. It is argued that alternative architectures can be readily created, which are more attuned to the openness and freedoms which are supposed to be the hallmarks of democratic government. It is questioned whether authoritarianism will be capable of surviving the complexities, dynamism and widely distributed power which are features of the emergent information societies.

1. Introduction

The genre of 'anti-utopian' novels described futures repugnant to humanity. The classic image of an information-rich government dominating citizens' thoughts and actions is associated with Zamyatin's 'We' (1922) and Orwell's '1984' (1948), but the technological basis of the surveillance culture had been established as early as the late nineteenth century by Jeremy Bentham's designs for a model prison, incorporating the all-seeing and ubiquitous 'panopticon' (1791). Foucault (1975) argued that the prison metaphor was the *leitmotiv* of authoritarian society. Bradbury's 'Fahrenheit 451' (1953) and Umberto Eco's 'The Name of the Rose' (1980) speculated on the process and implications of denying information to the public.

Art anticipated reality. Information technology (IT) is now being systematically applied to public administration in ways consistent with the anti-utopian nightmare. This paper's purpose is to review the authoritarian model as a basis for applying IT in government, and to champion an alternative, democratic model of IT use.

2. Authoritarianism's Underlying Assumptions and Values

An authoritarian society favours obedience to Authority over individual freedoms, to the extent of demanding subservience of the individual to the State. The notion clusters with tyranny (the cruel exercise of power), despotism and dictatorship (the exercise of absolute power), totalitarianism (single-party government) and fascism (a usually savage blend of authoritarianism with nationalism).

Authoritarianism is associated with logical positivist and utilitarian philosophies. These perspectives place very high value on rational social engineering, law and order, and resource efficiency. The populace is perceived as unsophisticated, uneducated, unreliable, chaotic, and/or incorrigibly venal and immoral. For their own good, the organised State must impose control on the unruly people.

A further assumption of the authoritarian perspective is that there exist humans with a level of both intelligence and morality superior to the common herd. In different ideologies, their innate superiority derives from different sources, such as the divine right of kings, wealth, force of arms, mystical power, what Machiavelli called virtù, wisdom, intellectual merit, technical capability, political cunning, demagogery, and/or public popularity. These superior humans are accepted as being the appropriate ones to make judgements on behalf of their society, with a minimum of checks and balances. They do this through social engineering; that is to say by organising and re-organising society in what they consider the rational way of achieving order and efficiency, and hence of delivering material well-being, and therefore spiritual happiness, for all.

3. The Authoritarian Model of I.T. Applications

Under an authoritarian regime, the populace must be managed. Tools and techniques that have proven effective in managing raw materials, manufactured goods and animals, can be applied to humans too. A unique identifier for each person, and its general use by government agencies and other organisations which conduct transactions with people, are highly desirable tools for efficient social administration. Public administration systems must be designed to exercise control over people, in all of their various roles. There may be scope for at least some semblance of choice by individuals, but employees need to operate within a
corporate culture, consumer demand needs to be statistically predictable, and citizens' freedom of choice needs to be constrained, lest unworkable parliaments eventuate, with too many splinter parties, independents and conscience votes.

It is only logical that an authoritarian society should recognise the benefits of a unary executive branch, in which the boundaries between agencies are porous. In this way, data can flow freely (such that transaction data and client histories can be cross-verified, and changes of address and status cross-notified), and systems can be tightly integrated and efficient (and hence mise BRAND ANALYSIS: How to Identify and Understand Issue Nexuses in Complex Systems)

Authoritarian IT-based systems use a centralised architecture. Elements may be physically dispersed, however, to achieve efficiency in data transmission, and to provide resilience against localised threats such as natural disasters and sabotage by dissidents. The general shape of such systems is that provided by cyberneticians: a cascade of control loops, culminating in a master-controller. In authoritarian regimes, information privacy and data security play important roles. These have little to do with the protection of people, however, but rather serve to protect the integrity of data, and of the system, and to legitimate the repressive system through the provision of nominal rights for data subjects.


4. Instances of Authoritarian Application of I.T.

The reader is by now (hopefully) annoyed by the extent to which the foregoing description has been a caricature, hyperbole, a 'straw man' designed to be easily criticised. However there are manifold instances of just these features in IT-based public administration systems, both those in operation and being conceived, in countries throughout the world. In North America, whose use of IT has been well ahead of that in most other countries, a 'national data center' was proposed as early as 1966. Elements of it have emerged, such as the widespread use of the Social Security Number (SSN) as a unique identifier, proposals for a health id card, and the all-but uncontrolled use of computer matching and profiling. Some protagonists in the current debates surrounding the national information infrastructure (NII) are seeking a network consistent with authoritarian control; for example, by insisting on use only of those cryptographic techniques which are 'crackable' by national security agencies.

Australia has followed the North American tendency. It flirted with a national identification scheme in the late 1980s (Greenleaf & Nolan 1986, Clarke 1987, Graham 1990). When that was overwhelmingly rejected by the populace, senior executives in public sector agencies 'went underground'. They have variously gained Parliamentary support for, and smuggled through, a series of measures whose cumulative impact is in some ways already more emphatic than the 'Australia Card' would have been (Clarke 1992).

The cultures of many Asian nations are well-suited to authoritarian regimes. There are elements of high-social-efficiency applications of IT in such nations as Singapore. Busy Asian countries have shown especial interest in vehicle monitoring systems. Thailand and the Philippines appear eager to act as laboratories for United States corporations developing identification and surveillance technologies. Under China's strongly authoritarian political system, it is unlikely that IT will be applied in any way other than to bolster existing relationships between its citizens and the State.

In Western Europe, Scandinavian countries lead the way with their social welfare systems and the heavy dependence of their citizens on the State. Denmark's citizen register is a model for authoritarian regimes everywhere, and a looming export success. Other countries are keenly adopting proposals to use IT to constrain the populace, by such means as identification cards (variously for football fans, patients, and the public in general), and the integration of data systems between government agencies, and between countries within and beyond the European Community.

In Central and Eastern Europe, there was an expectation that democratic, free enterprise systems would arise to replace the authoritarianism of the collapsed communist regimes. In practice, few of those countries have ever known freedom of choice, and genuine democracy (as distinct from variants of authoritarianism referred to in local lexicons as 'democracy') is not on the agenda of many of these countries. Their focus is on economic growth, rationalist solutions to economic and social problems, and centralism. IT is seen as a tool of authoritarianism, not of democracy; of centralised power, not of a pluralist body politic; and of control, not of freedom.

It can come as no surprise that public administration systems are being conceived in these ways. Applications of all kinds are developed by well-trained and self-confident engineers, using unequivocally rationalist techniques. System design comprises the expression of relevant parts of the present and future world in a formal model which has the important characteristic of being 'mappable' onto a machine. The application's users and 'usees' (i.e. the people affected by it) are treated as objects to be modelled, not as stakeholders with interests in the process and its outcomes. Human language is treated as though it were an (imprecise) formalism, rather than a means of interaction among people. The designers fail to notice that their formalisms cannot reflect the complexities, ambiguities and dynamism inherent in social systems, and the negotiation and accommodation processes

Hence the problems highlighted in this paper are to a considerable degree inherent in the techniques currently used to develop IT applications generally. Nonetheless, their greatest impact on people's freedom is by way of public administration systems.

5. The Democratic Alternative

The technological determinism notion has been applied to IT. In particular, IT has been accused of being inherently de-humanising, centralist and authoritarian (e.g. Roszak 1986). The standpoint adopted by this author is that technology is essentially morally 'ambivalent' (i.e. it has potential applications and potential impacts variously supportive of, and iminical to, any particular social value - Ellul, 1990). IT may make some paths easier than others, but the choice is made not by blind fate, but by politicians, government executives, and, not least, IT professionals.

The alternative political philosophy to authoritarianism is democracy, popularly expressed as 'government of the people by the people', and commonly implemented through representatives chosen regularly and frequently by the combined and equal vote of all competent adults. The democratic ideal derives from the assumption that no class of people has the right to dominate other classes. It reflects the renaissance conception of mankind, whereby each individual should have the opportunity to access and interpret for themselves the ideas of other people and of Gods; and, in more modern terms, should have the scope for self-determination and self-fulfilment.

Early computer technology may indeed have encouraged centralisation, but since the marketplace debut of integrated circuitry and the mini-computer about 1970, modern IT has been readily applied in the service of democracy. Open IT-based systems involve nodes which are 'peers', with equal authority in respect of particular functions. For example, in a national health network, each node might take responsibility for all processing and storage relating to a particular aspect of the system's functionality (e.g. support of a particular regional clinic, or epidemiological research into a particular class of diseases), and have special rights recognised by all other nodes in that regard (e.g. the right of access, respectively, to identified data relating to specific patients, and to identifiable data relating to particular diseases and procedures). Similarly, particular kinds of data held at each node (e.g. data identifying a patient) might be recognised as being controlled by that node and require special authority before it could be released to any other node.

One form of democratic topology is the unconstrained network, with maximum inter-connectivity, and dominion by each node over the services it provides. Another model is a variant on simple-minded cybernetics: a cascade of controllers which folds around, such that the ultimately controlled (the populace) are also the ultimate controllers (the voters). Before modern communications became available, the only practicable democratic mechanism for geographically large countries was periodic (typically, 3- or 4-yearly) election of representatives. In information societies of the very near future, however, major policy decisions can be instigated, formulated, and decided by direct democracy. Voters may choose to delegate the articulation of broad policies to their elected representatives, but even this can be subject to the over-riding of unpopular decisions, and the removal of representatives the electorate considers are not performing their functions.

Hierarchical topologies serve authoritarianism, whereas non-hierarchical ones are consistent with a free society. Access to data under the control of each node must be restricted, until and unless, via due process, disclosure is justified in fulfilment of some higher interest. Such topologies provide not only robustness and adaptability, but also integrity, because clients can trust them, and there is a lower risk of loss of quality (through suspicion and uncooperativeness), and of sabotage (through active attempts to mislead, and direct, destructive action).

6. Instances of Democratic Application of I.T.

Is this image of democratic computing just a caricature too? Possibly, but examples exist. Local Area Network architectures are inverting the old notion of centralist processors accessed by terminals. The now-conventional names reflect the fact that 'client' workstations demand data and processing from 'servers': the user's device is in control, and the central facility performs at its bidding. In wide-area networking also, peer-to-peer protocols are rivalling and may be progressively replacing the older, hierarchical or 'star' configurations. At the level of inter-networking, the topology of the world-wide TCP/IP-based Internet is essentially flat, the systems software is highly distributed, the redundancy is very high, and its robustness, its resilience and its capacity to resist authoritarian governments are therefore all of a high order.

The Internet's technical features have resulted in a culture very different from that on hierarchical nets. It provides a space in which imaginations have substantial freedoms. Some people use those freedoms to create new services and products; others to experiment with self-expression and group-experiences; some as a 'cybernetic' analogue to psychotropic drugs; and some just to distribute pornography or racist materials. Nor are the boundaries between these activities always clear-cut.

It seems ironical that the Internet was sponsored by the United States military complex, but the irony is more apparent than real. Systems which support military operations cannot risk the fragility of centralisation, but rather demand robustness and resilience, and therefore redundancy. Moreover, aero-space-defense R. & D. is dispersed across vast numbers of universities and private
and therefore redundancy. Moreover, aero-space-defense R. & D. is dispersed across vast numbers of universities and private sector research laboratories. It then seeks to complement competition by collaborative interaction among individual researchers and among potential research partners. To retain its technological and intellectual leadership, it was essential that the U.S.A. avoid the temptation to sustain centralised, authoritarian topologies; and to its credit it knowingly spawned a dynamic, worldwide, democratic network laboratory.

7. A Synthesis

This paper has considered the extremes of authoritarianism and democracy. Clearly, any society will demand not only freedoms, but also protections against those who use those freedoms to harm others. Naive authoritarian models are doomed to fail, because they deny freedoms; and naive democratic models are doomed to fail too, because they deny protections. Ronfeldt concluded that IT-based public administration (which he calls 'cyberocracy') "far from favoring democracy or totalitarianism ... may facilitate more advanced forms of both" (1990, p.283). How should new 'cybertocracies' be designed, and how should existing public administration systems be adapted to exploit the new opportunities, while balancing the needs for control and freedom?

Authoritarian aspects of schemes could be justifiable in some societies as interim measures. Lenin and then Stalin judged that the country's large peasant population, and its institutions, were insufficiently mature for immediate implementation of the full Communist platform. Unfortunately the repression inherent in their interim arrangements became ingrained, and was only relieved by counter-revolution. Authoritarian elements in public administration should therefore be not only justified, but also demonstrably interim, i.e. the means must be shown whereby they will be replaced, by evolutionary processes, with alternative mechanisms consistent with democratic principles.

In any case, the feasibility of grafting democratic features onto an essentially hierarchical model must be regarded as very slim. All power vests in the centre, and any softening of the system's features is by gift of the powerful. Moreover, the system can be manipulated by the powerful (for example, by monitoring nominally confidential communications), and privileges can be withdrawn by the powerful. No freedom-loving populace must regard such a system as credible, and would therefore only submit to it as a result of coercion.

Is the alternative feasible: to graft control mechanisms onto an essentially open model? Communication channels can still be tapped and storage devices searched (under warrant). Evidence arising from such interceptions and searches can still be presented in a court of law. Certain actions and uses of IT can be expressly made illegal. Their post facto controls can therefore still function within open, democratically conceived public administration. Toffler distinguished this form of IT application by coining the term 'practopia' (1980, p.368).

What is not so simple to contrive within open systems is effective real-time monitoring and control: Foucault's 'prison' is readily implemented using hierarchical topologies, but if the nodes and arcs of networks are not all under the control of Authority, then preventive controls become much harder to bring to fruition. That, then, is the essential battleground between authoritarian and democratic models of IT: should someone or some class of people, and in particular politicians and senior public sector executives, be permitted to have the power to prevent transgressions? Because it is that kind of control over the public which is at the very heart of the anti-utopian nightmare.

8. Conclusions

Power does not need to be explicitly and consciously granted to public administrators by the voting public, or by their elected representatives. It can accrue, slowly and gently, through developments in IT, through new applications of established techniques, through the gradual 'creep' of existing schemes into new functions, and through seemingly harmless refinements to statutes. As frogs are reputed to do, a society might resist being put into boiling water, yet be lulled to sleep in warm water slowly brought to the boil.

This paper commenced by referring to early literary premonitions of authoritarian applications of IT. The fictional literature has undergone a transition. The turning-point was John Brunner's 'The Shockwave Rider' (1975), which explicitly owed a debt to Alvin Toffler's 'Future Shock' (1971). For much of the novel, the hero appears to be putting up a brave fight against inevitable defeat by the State. By turning the power of the net against its sponsors, the hero discovers pockets of surviving resistance, and galvanises the latent opposition to the State. Unlike anti-utopian novels, the book ends on an ambiguous, but (from the humanistic perspective) an optimistic note.

Subsequent novels have adopted a quite different pattern. In such works as William Gibson's 'Neuromancer' (1984), and the 'cyberpunk' genre it spawned (see Sterling 1986), people are prosthetic-enhanced cyborgs, plug directly into the net, and induce their 'highs' through a mix of drugs and cyberspace. More importantly for the argument being pursued here, national and regional governments exercise very little power. The hypercorps (successors to the transnational corporations) are responsible for organised economic activity, the majority of the net, and a great deal of the information. Outside this limited, polite society shell, large numbers of people, in communities in which formal law and order have broken down and tribal patterns have re-
skulk large numbers of people, in communities in which formal law and order have broken down and tribal patterns have re-emerged. Officialdom has not been able to sustain the myth that it was in control; society has become ungovernable.

Little echoes of these patterns are evident in contemporary societies. The use of the Internet for anti-social purposes is proving much harder to control than similar behaviour using the telephone network. IT contributed significantly to the breakdown of the Soviet Union because, in addition to improving production effectiveness and efficiency, PCs delivered 'samizdat' - the means for cheap reproduction of dissident newsletters. Lies that had been lived for seven decades could not withstand the heat generated by eager users of a potentially democratising technology. And that was before inter-networking and computer-mediated communications had achieved any degree of sophistication.

IT may be applied to public administration in ways consistent with authoritarianism or with democracy. Proponents of hierarchical structures and social engineering, chief amongst them senior public sector executives, must at the very least appreciate the limits of tolerance of authoritarian measures within their society. Preferably, governments should ensure that social administration schemes are not emphatically centralised and incapable of adaptation towards more liberal patterns. And most desirably, public servants, governments and voters themselves, should be exploiting the opportunities for more effective democracy which are being created by information technology.

References

Bentham J. (1791) 'Panopticon; or, the Inspection House', London, 1791
Bradbury R. (1953) 'Fahrenheit 451 ... The Temperature at Which Books Burn' Ballantine Books, 1953
Brunner J. (1975) 'The Shockwave Rider' Ballantine, 1975
Ellul J. (1964) 'The Technological Society' Knopf, New York, 1964


Packard V. (1964) 'The Naked Society' McKay, New York, 1964


Weizenbaum J. (1976) 'Computer Power and Human Reason, Publisher, 1976

Zamyatin E. (1922) 'We' Penguin, 1922, 1980

---

**Navigation**


Go to the contents-page for this segment.

Send an email to Roger Clarke.

Created: 13 October 1995

Last Amended: 7 July 1998

---

These community service pages are a joint offering of the Australian National University (which provides the infrastructure), and Roger Clarke (who provides the content).

---

**The Australian National University**

Visiting Fellow, Faculty of Engineering and Information Technology,
Information Sciences Building Room 211

---

**Xamax Consultancy Pty Ltd**

ACN: 002 360 456
78 Sidaway St
Chapman ACT 2611 AUSTRALIA
Tel: +61 2 6288 1472, 6288 6916