E.Society - panacea or apocalypse? The rights and wrongs of the Information Age

Prof. Simon Rogerson

Originally published as ETHIcol in the IMIS Journal Volume 9 No 5 (October 1999)

This special edition edition of ETHIcol presents the inaugural lecture of Professor Professor Simon Rogerson delivered at De Montfort University on 26 May 1999.

Introduction. The advances in information and communication technology (ICT) present many opportunities and threats to individuals, organisations and society as a whole. Computers can be shaped to any activity that can be described in terms of inputs, transforming processes and outputs. It is the nearest thing to a universal tool [Moor, 1985]. Consequently, society and its organisations are becoming more dependent upon ICT as the means of providing information, the new life blood of society. There is increasingly wider access to and application of this powerful resource.

Inevitably there will be winners and losers, costs and benefits. Information empowers those who have it but it also disenfranchises those who do not. Wealth and power flow to the information rich, those who create and use ICT successfully. They are primarily the well-educated citizens of industrialised nations. The information poor, both in industrialised countries and in the developing world, are falling further and further behind.

The world has changed. Once people had to go to a particular place in order to communicate with others. This is no longer the case with the advent of pagers, mobile phones and laptop computers with communication cards. Communication now comes to people. Indeed, the creation of the fax, the mobile phone and the Internet have permanently changed the way people live and work [Anon1, 1997].

Some of the issues that surround the advancing Information Age are considered here. It is evident from this discussion that perceptions of what is appropriate and beneficial may be very different to what really is appropriate and beneficial.

What can go wrong. ICT is not without its problems or its disasters. Many of these issues tend to go unnoticed unless they result in some newsworthy story. Recent press

stories include those about the Melissa computer virus that infected more than 100,000 mostly corporate PCs within only three days and one of the most destructive known viruses, the Chernobyl virus which infected over one million PCs mainly in countries with developing and transitional economies. Computer abuse is an increasingly serious problem. The recent Audit Commission report (1998) stated in three year there had been a 9% increase to 45% of organisations in the UK reporting incidents of computer abuse.

Two illustrations as to what can go wrong are briefly discussed here. The first concerns the important issue of information integrity whilst the second covers a headline-grabbing problem - the millennium bug.

Information. There are concerns about the accuracy of information held within computer systems. The potential impact is exacerbated as the distribution and use of information has become global rather than the localised focus of older media. The inputting of raw data is prone to error with the natural error rate for an experienced keyboard operator being one keystroke in 100. It has been reported that inaccurate information in systems could be as high as 2%. Given each adult has about 200 computer files relating to them then there will probably be four errors per person on these files [Anon2, 1997]. If people were wary of these potential errors then maybe pressure would be brought to bear to minimise this danger but there is a tendency by the public to treat computer-generated information with a degree of blind faith. Consequently, integrity is assumed and possible errors go unquestioned.

The growing moves to create electronic patient records covering a patient's complete medical history from the cradle to the grave is a good illustration of why we must be extremely careful in the way information is created and distributed. Certainly the electronic patient record allows providers, patients and payers to interact more efficiently and in life-enhancing ways. It offers new methods of storing, manipulating and communicating medical information which are more powerful and flexible than paper based systems and can accommodate processing of non-textual medical information such as images, sound, video and tactile sense. There are, however, potential problems. The electronic patient record will hold a complete profile of the individual comprising personal and medical details. Access to this information much be carefully controlled ensuring such access is limited to only the relevant and authorised portion of the information. Since medical details contain some sensitive information such as past drug use or genetic predisposition to various diseases it is important to keep this information truly private. There will always be tension and trade-off between the need-to-know and the right to confidentiality. Misdiagnoses are quite rare, but far from unheard of. Procedures must be in place to ensure that once an error is identified the electronic patient record is corrected and all points of distribution informed of the error. Finally, inaccurate data input can be potentially life threatening in this application. It is particularly difficult to correct inaccurate data given the global distribution of this information to primary and secondary healthcare providers.

The Millennium Bug. The widespread concern over the millennium bug is indicative of a society becoming increasingly dependent on ICT. There are many estimates of how much it will cost the companies and governments of the world ranging from a conservative $52 billion by the British investment bank, BZW to a staggering $3.6 trillion by Software Productivity Research in Boston, USA [Anon3, 1997]. Companies are undertaking corrective work on a large scale. For example, Centrica which trades as British Gas, stated in the 1997 annual review to shareholders that during 1997 Â£3 million was incurred in millennium compliance. It stated a further Â£43 million was required in 1998 and a further Â£15 million in 1999. There are indications that 30% of companies world-wide will suffer a critical software failure due to the date problem. Information systems running on mainframe computers, personal computers and embedded chips in appliances all have to be checked. The size of this task is enormous with 180 billion lines of code and over one billion embedded microchips to be checked. It is estimated this requires around 700,000 person years of effort and that is why the top 100 European companies are spending 30% of their 1999 ICT budget on compliance [Tate, 1999]. It is clear the integrity of date-dependent information is at risk. The consequences may be very serious. For example, one manufacturer had to recall a heart defibrillator because its safety features only worked if a recent service had been undertaken. Not being millennium compliant meant that service dates after 2000 would be interpreted as 1900 resulting in a machine malfunction [Anon3, 1997].

These two examples illustrate the risks associated with information dependency. Quite simply, unreliable information and unstable information systems will lead to information bankruptcy.

People matter. The Club of Rome has identified the Information Society as one of the eleven global issues that must be addressed if the new global society is to flourish. It states that, "The globalisation of the economy, the fact that we live from now on in an Information Society, the complexity and the uncertainty which are the common trademarks of the present word lead us to take into consideration a number of these new factors. We have to understand these new data in order to have a better understanding of other cultures, other languages, other modes of reasoning." Clearly it is important to consider the role of people in the Information Society as illustrated by the following three issues.

Identity. There has been much speculation that people can play with their identities on the Internet and present different electronic persona. Such speculation is characterised in the famous cartoon entitled "On the internet nobody knows you’re a dog". This might be possible in the short term but such mimicry is likely to be spotted in the long term as identity is more than simply learning and applying rules, it is about learning within a context and reacting intuitively to different situations as they arise [Whitley, 1997]. In the Information Society, the impact of physical characteristics of those communicating has been minimised. This is potentially beneficial as removing the visual cues about gender,

age, ethnicity and social status allows different lines of communication to open up that might have been avoided in the physical world [Whitley, 1997]

Culture. The Information Society crosses traditional boundaries and as such comprises individuals from many different cultures. This cultural variability means that the expectations of individual cybercitizens can differ considerably. Nance and Strohmaier (1994) suggest there are two important dimensions to consider regarding this variability. The first dimension is the continuum from individualism to collectivism. Individualism emphasises self interest and promotes the self-realisation of talent and potential. Its demands are universal. Collectivism emphasises pursuit of common interests and belonging to a set of hierarchical groups where, for example, the family group might be placed above the job group. The demands on group members are different to those on non group members. The second dimension concerns cultural differences in communication referred to as low context communication and high context communication. In the former the majority of the information resides in the message itself whilst in the latter the communication is implicit. Nance and Strohmaier (1994) suggest that the USA utilises low context communication whilst Japan uses high context. Given this cultural variability it is clear that there are great difficulties in providing information in a form that is acceptable to all. This is certainly one of the great challenges of the Information Age. It involves establishing a set of common behavioural standards whilst ensuring that there is no dominant participant.

References

[Moor1985] Moor, 1985 J.H. Moor *Computers and Ethics* What is computer ethics?, Blackwell, Oxford 1985 T.W Bynum

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel:(+44) 116 257 7475
Fax:(+44) 116 207 8159
Email:<srog@dmu.ac.uk>

Home Page: (`http://www.ccsr.cse.dmu.ac.uk`)