

People matter

Prof. Simon Rogerson

**Originally published as ETHicol in the IMIS Journal Volume 14
No 6 (December 2004)**

Information and communication technology is really about people not technology. It is a social construct. How people behave in developing and using the technology makes the difference in realising a society that is good for us all.

Two recent examples illustrate questionable actions by those who should know better!

The Financial Times on Wednesday October 6 2004 ran a story about new forms of mobile phone technology. It described a software product developed by Simedia called SounderCover which is designed to deceive when using mobile phones. The web site for SounderCover urges you to "hide behind sound, make it your alibi :)". It continues, "Did you wake up late for work and you want your boss to think you're caught in traffic? Select the Traffic Jam background and give him a call from your bedroom :). He will hear your voice on top of this." (see www.simedia.com/soundercover.html) (<http://www.simedia.com/soundercover.html>)

The FT article quoted the founder of Simedia, Liviu Tofan as saying, "They [the nine back ground noises] sound very genuine and they give you the potential to pretend you're in a different place. We also give you a function which plays a telephone ring after 15 or 30 seconds, so you can say you need to get another call. Certainly people use it [SounderCover] to give plausibility to their excuses - both for work and in relationships." Sales for the product have soared.

It is hardly surprising that such products have become popular in a society where traditional values are put aside in the quest for celebrity and the obsession with reality entertainment.

This action by Simedia is clearly antisocial. Sometimes software product designs inadvertently provide opportunities for users to exploit its functionality in pursuit of unacceptable actions and goals. But this is different. Simedia are marketing this software on a ticket of deception. They want us to deceive. They want us to lie. To advocate such things challenges some of our core values such as truth and honesty. Such action is unacceptable and unprofessional.

The second case concerns the UK Passport Service (UKPS) which is currently running a six-month trial to test the recording and verification of facial recognition, iris and fingerprint biometrics. The claim is that the results will help inform the Government's

plans to introduce biometrics to support improved identity authentication and help prevent identity fraud. These issues have been covered in previous ETHicol columns.

The author of this column had the opportunity to participate as a volunteer in the trial. In doing so name, address and age had to be divulged but assurances were given that this personal data together with the biometric data would be destroyed after the trial. The trial consisted of two stages, the first where biometrics were recorded and a mock identity card produced and the second where this card was tested as a means of electronic identification. By chance the next volunteer was a person in a wheelchair. She was ushered into the first stage booth. The official assumed that given she was wheelchair bound she required the personal data on the computer screen to be read out to her so she could verify its correctness.

Given the proximity of the booths for the two stages, the author of this column, whilst undertaking stage two, was able to hear all Margaret's details being read out. He challenged the official that the trial was in fact illegal as personal data was being divulged to a third party without consent through the lack of proper procedures. What was concerning was the response to this challenge. In the first instance the official failed to understand the breach of privacy that had taken place regarding the data subject Margaret. On further explanation his response was to ask the author to write a comment on the feedback form that volunteers were asked to complete. He seemed totally disinterested in this breach of privacy. Such actions seem to contravene the published privacy statement of UKPS (see www.ukpa.gov.uk/privacy.asp). It states, "We will take every precaution to protect your data" and "Your data is protected from unauthorised or accidental disclosure". Both were breached in this instance.

Given the sensitive nature of smart identity cards based on biometrics the unprofessional conduct of these officials is disturbing. If they fail to recognise and uphold the rights of citizens in trials what will be the attitude when this technology is fully implemented by UKPS? Use of technology, particularly in new situations, requires people to trust it. This unprofessional conduct does little to instil a sense of trustworthiness of this system by the general public.

These two cases highlight questionable behaviour by both developers and authorised users of technology. If technology is about people then those involved must be seen to be beyond reproach. Such people must exhibit virtuous behaviour. Indeed DiPiazza and Eccles in *Building Public Trust* suggest that to secure public trust organisations must exhibit a spirit of transparency, sustain a culture of accountability and employ people of integrity. Would the organisations in the two examples pass these three tests?

As can be seen from the UKPS example organisations will have policies to cover good practice. Many will acknowledge they subscribe to a professional code of conduct such as the IMIS Code of Ethics. But that is not enough. In his article "Business Ethics for IT Managers--What You Can Do", Clinton Wilder argues that organisations must, "Be

proactive. It's not enough to have a great ethics policy that sits on a shelf with the corporate mission statement. Institute regular ethics training and awareness programs. Move ethics away from "rules to be followed" to becoming a way of doing business."

The message is simple for IS professionals in all contexts - Actions speak louder than words - act ethically when developing and implementing ICT.

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>)