

Do we trust U?

Trust: a firm belief in the reliability or truth... of a person or thing... a confident expectation. But how much do we, and should we, trust technology? **Robin Mansell** highlights some information dilemmas facing us in the next decade.

Innovative information and communication technologies (ICTs) continue to bring huge benefits to us all – can you imagine your life now without email, a computer, a phone? The flipside is that they also reach into our public and private spaces and raise complicated issues for each of us. How do you know, for instance, who you are dealing with when you receive an email? How might we receive benefits, health care and financial services in the future, but securely enough for us to have confidence in the systems? How can we use these technologies to reduce crime, yet at the same time limit the crime opportunities they offer? What standards of protection should we apply? Who should be liable if something goes wrong? If we do not tackle these issues, we risk delaying or losing some of the potential benefits that these technologies can bring.

To form decisions on these issues we need to take into account the existing empirical evidence, technologists' views of what might be possible, and a wide range of individuals' views about how the future might evolve.

The software industry accounts for around three per cent of the UK's gross domestic product, with more than one million people working in ICT-related jobs in the UK. Some 80 per cent of the British population can access broadband. In poorer countries, access is much more restricted

but there is some – and growing – use of the internet. In China it is estimated that there are now more estimated internet users in real terms than anywhere else in the world except the United States. The importance of 'ubiquitous computing' will increase as ICTs work their way through societies and as new technologies emerge.

The term 'ubiquitous computing' was coined in 1991 by the computer scientist Marc Weiser to describe an era in which computer devices would be embedded in everyday objects invisibly at work and at home. He expected that intelligent, intuitive interfaces would make computer devices simple to use and unobtrusive and that communication networks would connect these devices to facilitate anywhere, anytime, always-on communications. Key trigger points making this possible today and in the future include radio frequency identification (RFID) chips at less than US \$0.05, US \$20 mobile phones and US \$200 computers.

Today, sensor networks are used to provide flood warning systems, and to improve food traceability. RFID chips are used to distinguish legitimate pharmaceuticals from counterfeit ones. They are being proposed for use in ID cards and passports and have been used in road pricing schemes, for inventory management and in maritime transport. Bio-medical applications include

RFIDs that contain identity information or medical records and that can be implanted in dental prosthetics or injected into the body. RFIDs are also used for controlling access to tourist areas and to monitor purchases of drinks and food.

The potential benefits of RFID applications range from better and more efficient medical care to increased convenience at points of sale, improved crime prevention, and streamlined business processes. In some economies, there is a shift from 'e-strategies' to 'u-strategies' in considering issues of universal service and the ubiquity of access for potentially excluded groups and new codes of social conduct.

An important issue in any assessment of these developments and their policy and regulatory implications (as well as the likelihood of compliance with legislative measures) is the extent to which people will remain a systemic weakness as ubiquitous computing takes hold. How much people are liable for technology 'mistakes' will depend on many distinctive social, cultural and other values consistent with agreed ethical norms.

Ubiquitous computing

It will be essential, as well, to ensure that we use ubiquitous computing to reduce existing crime and to reduce the extent to which ICTs introduce new forms of crime or extend the scope of existing crimes. ICT security problems are a fact of business life now. In the UK over two thirds of businesses reported that they had experienced at least one security breach in 2004, and the breaches included viruses, staff misuse of ICT systems, fraud, theft and unauthorised access by outsiders. The average cost of an organisation's most serious security incident is about £10,000. For large companies, this is more likely to be £120,000. Incidents are costing businesses billions of pounds.

But who and where are the new security 'police' when it comes to protecting ourselves from u-crime? Although ICT security is an increasing priority for business, many companies lack the expertise to

address this issue. In the UK only one in ten staff have formal ICT security qualifications. Information assurance strategies and e-crime strategies are being devised, but the empirical evidence in many important areas relevant to tackling crime related to ICT use is limited. Plus the complexity and ubiquity of ICTs require new ways of thinking, particularly about how to manage the threats to people and society. There may be an increasing number of small failures and irritations, or a small number of widespread failures, that disrupt life at home or at work. Current governance frameworks will be hard pressed to deal with the full range of consequences associated with ICT use in the future.

At the same time, opportunities for threats are growing in number. Faults involve problems that only emerge after innovation has occurred and include major outages – the unwanted effects of software trading agents or bugs. Mischief stems from viruses, worms, DoS (denial of service) and hacking. Crime may involve a parasite/host like the Trojan Horse virus that exploits system vulnerabilities; organisational insiders may exploit systems, while outsourcing web services can reduce confidence; automation is supporting large numbers of small transactions, making it feasible to launch simultaneous attacks. In the case of terrorism, visible destruction may be the goal: there may be no need for sophistication, and critical ubiquitous computing infrastructure or symbolic services may be the targets.

So what should we be planning? I would suggest, firstly, that it will be necessary to influence business to 'design out' crime and 'design in' usability as a fundamental principle. But technical design does not provide a complete solution. People, cultures, social orders, politics and economic performance matter as well. This means we have to acknowledge that tackling online crime is not constrained by national boundaries and cannot rely on taken-for-granted norms and expectations about behaviour.

In the future, people will want to use ubiquitous computing differently in many areas of life. We

will apply different standards, for example, to identifying someone who is casting a general election vote as compared to someone from whom we are buying a second-hand book. People will also make different judgements based on their experience, education, the reported experience of others around them, and the way in which risks and benefits are reported in the media.

Trustworthiness

Isn't this all about trustworthiness and trusting behaviour? Trust seems to reduce the need for costly social control structures and make social systems more adaptable. Some evidence shows that people with little experience of the internet have low levels of trust or no opinion about risk. But we have to distinguish between reported perceptions of trust and the way in which people actually behave. We know little about the basis upon which people are prepared to trust others on the internet or to believe in the trustworthiness of ubiquitous systems.

Individual privacy and collective security – where will we draw the balance? We need to begin to identify the characteristics of the actual ways in which privacy is distributed in society, including the different ways in which it is surrendered and retained by different groups.

We need to consider ubiquitous computing and our internet applications in specific contexts because, in practice, the trustworthiness of new digital services will vary from case to case. Users will typically interact with new applications through branded services, with little opportunity to form judgements about the nature of the services and service providers. Some users may resist being treated by government as if being a citizen and being a customer were equivalent. The systems that enable e-services from health to education to commerce should reflect these distinctions. In creating trustworthiness, as in reducing crime, new technologies will provide new solutions (for example, new forms of encryption or intelligent agent software), but they do not offer 'silver bullets' to create perfect trustworthiness or zero crime.

There is considerable agreement that addressing the trustworthiness of future generations of ICTs will require different technologies and behaviours from those in place today. There are no universal answers for the difficult issues associated with ubiquitous computing environments or with the way the media report events relating to actual or potential risks associated with the internet.

The rapid pace of change and uptake of many new services mean that those trying to reduce crime will have to move more quickly to respond effectively. At the same time, they will have to ensure that privacy – however understood – and citizen's rights are respected. When first introduced, 'new' technologies from typesetting to the telephone have given rise to concerns about the need for new policies, and RFID chips and the internet are no exception. The difference today is the global reach of information and communication networks and the hugely increased need for coordinated action. The structures for dialogue between government, business and citizens groups will need to evolve to allow faster feedback on identifying and responding to potential for crime opportunities. ■



Professor Robin Mansell

is Dixons Chair in New Media and the Internet at LSE, based in the Department of Media and Communications. This article draws on results from a UK Office of Science and Technology (OST) Foresight project on Cyber Trust and Crime Prevention, the social science component of which was led by Professor Mansell with contributions from LSE colleagues in Information Systems and the Methodology Institute, see www.foresight.gov.uk; and R Mansell and BS Collins (eds) *Trust and Crime in Information Societies* (Edward Elgar 2005). It also draws on an ITU Workshop on Ubiquitous Network Societies chaired by Professor Mansell in Geneva in April 2005. The views are those of the author only, and are not necessarily those of ITU or OST.