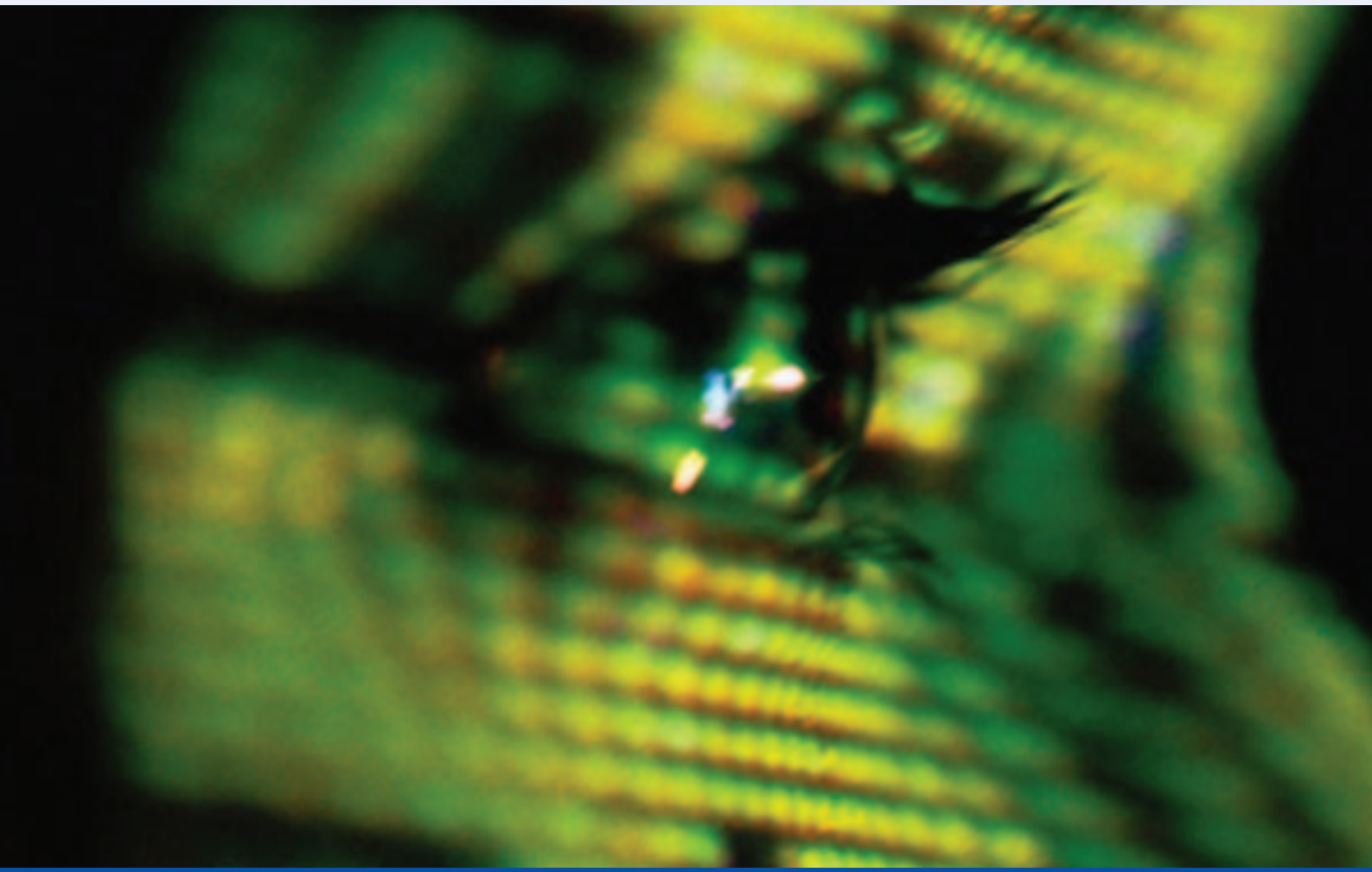
THE ROYAL SOCIETY

Public dialogue on cybertrust and information security

Key findings and recommendations from regional workshops and a national forum held by the Royal Society's Science in Society programme



October 2004

excellence in science

1 Summary

1.1 The Royal Society Dialogue on *Cybertrust and Information Security* enabled a cross section of the public, together with scientists, representatives from business, members of civil society groups and non-government organisations to discuss and debate the implications of likely developments in information and communications technology (ICT) over the next 20 years.

1.2 ICT was seen to be a major force for social good, with particular benefits for crime reduction through surveillance technology; healthcare through the capacity to better understand, predict and control disease by the intelligent mining of health records and genetic information; and business through developments in e-commerce.

1.3 However, only one in five participants was confident in society being able to control the technology and there was low trust in business and government to protect information.

1.4 People wished to gain control over who had access to their personal information and informed consent was paramount to this. They were also keen to have better control over their own information security – however felt they lacked the basic skills. E-literacy was thus paramount.

1.5 There were concerns that complacency will undermine the trust necessary for the successful development of ICT. For the benefits to be realised, a coordinated effort between government, business and the public to make systems more secure, to use information responsibly and develop appropriate regulation and enforcement is required.

1.6 A watchdog to govern the use of information by government and business, particularly concerning the use and storage of information, was supported by three quarters of participants as the most effective way to develop trust in information security.

For further information on the Cybertrust and Information Security Dialogue, please contact Dr Darren Bhattachary, Science and Society Manager at the Royal Society on 020 7451 2566 or visit www.royalsoc.ac.uk/scienceinsociety

2 Introduction

2.1 The Royal Society Dialogue on Cybertrust and Information Security held earlier this year formed a key component of the Society's privately funded Science in Society programme, now in its fourth year. A major aim of the programme is to further the role of a responsible and responsive science, engineering and technology in society, through engendering informed public debate on science and technological development.

2.2 The Cybertrust Dialogue comprised four regional workshops and a National Forum that engaged 130 members of the public in a discussion with specialists on developments in information and communications technology. The Society's decision to address this theme resulted from a horizon scan meeting in June 2003, in which a cross section of individuals highlighted information security as a promising subject for investigation and debate.

2.3 The regional workshops were held in Bristol, Doncaster and Leicester, with the Bristol event also including a young persons' workshop. Adult participants were recruited through a market research agency to a quota sample reflecting the demographic profile of the local area. Participants were also selected to have a range of different attitudes towards science and technology. Young people were recruited through three Bristol schools. The regional sessions were conducted in March and April 2004.

2.4 The regional workshops explored views upon ICT in general and then considered future developments through the discussion of a scenario (appendix 1). The sessions comprised a mixture of plenary and small discussion groups, with a technical and a social science specialist acting as a resource for participants. The discussions were facilitated by a moderator.

2.5 The National Forum was held at the Royal Society in April 2004. It was designed to enable the issues that emerged from the regional meetings to be explored in depth and to allow discussion of particular case studies (appendix 2). Participants who had attended the regional workshops were reconvened, together with invited policy makers and influencers based in London. The public were divided into one of seven facilitated groups, each with two specialists. Interactive handsets enabled participants to vote on findings and recommendations emerging from the discussion.

2.6 The Dialogue attracted extensive media coverage (appendix 3).

2.7 The Dialogue also had a positive impact on the views of participants towards developments in science and technology (appendix 4).

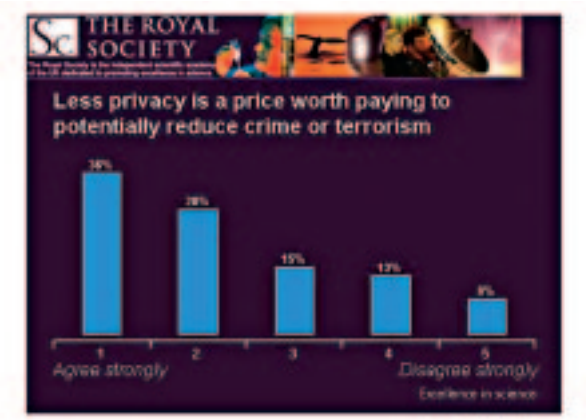
2.8 Key findings (in italics) and recommendations (in bold) from the Dialogue as expressed by the participants follow. The views do not necessarily reflect those of the Royal Society.

3 Key findings and recommendations

3.1 Privacy and crime reduction

3.1.1 The use of ICT for crime reduction was a dominant theme of the Dialogue, particularly the potential deployment of an extensive surveillance technology network with coordinated, pervasive and intelligent systems for data mining. A number of concerns were noted, particularly the impact on different social groups; whether crime would be reduced, displaced or new forms of crime would develop; the capacity of the system to cope with large amounts of information; whether surveillance would be enforced; the effect of poor enforcement on the social acceptance of technology; and the accuracy of identifying crime and perpetrators. There were also concerns about being able to disprove erroneous digital 'evidence' in miscarriages of justice. Three quarters of participants thought that there would be less privacy in the future. This withstanding, *two-thirds of participants thought less privacy was a price worth paying to potentially reduce crime or terrorism* (figure 1*).

Figure 1.
Interactive vote on whether less privacy is a price worth paying to potentially reduce crime or terrorism



3.2 Healthcare

3.2.1 In healthcare, there were perceived to be real benefits in the capacity to better understand, predict and control disease through the intelligent mining of health records and genetic information. There was concern about the potential for such databases to contain lifestyle information, together with anxiety about information security – particularly confidentiality, data security, and the potential for disclosure, either through actuarial pressure or through criminal activity. **To promote security, the idea of dedicated servers and sophisticated authentication devices for the health service were suggested together with the importance of public consent to data collection and compensation if rights are contravened.** The potential for private sector partnerships to provide capacity and expertise in systems management for the NHS was held up to some scrutiny – with concerns raised about the potential for fractured management of complex systems. *On balance, people felt that the prospect of better healthcare outweighed potential problems of breaches in data collection and management.*

3.2.2 As well as the analytical and predictive potential of intelligent data mining for healthcare, specific applications were discussed, such as the use of remote devices for health monitoring and diagnosis. While *the use of ICT to manage chronic conditions such as diabetes or asthma was generally supported, its application for general practice online diagnosis was criticised - particularly in terms of accuracy and patient assurance*. Many participants were concerned of their ability to be able to describe the symptoms to enable effective diagnosis, or felt that greater impetus would be on them to self diagnose. This, together with the issue of liability and the importance of face-to-face contact in healthcare, meant that this application met with only a lukewarm reception.

* For all graphs n=130

3.3 Business

3.3.1 In terms of business – while people recognised the value of customer information for supply chain management, they were less keen on large data sets being held on individuals for direct marketing, and thought that a too tailored shopping experience was intrusive. Some people were not convinced that the benefits offered to them for the exchange of information were a sufficient incentive. The usefulness and legitimacy of vast quantities of individuals' information held by business was questioned and the issue of consumer sovereignty, individual choice and consent highlighted. **A big concern was unlawful data sharing amongst companies. Effective governance of business was thus paramount and a watchdog was suggested to safeguard the interests of people**. The difficulty of successfully regulating such complex systems, however, was duly noted.

3.3.2 E-commerce and e-payments were also discussed. The issue of trust of sites and transaction security was key to the success of e-commerce. People currently adopted either a risk management strategy (liability held by third parties through insurance; use of intermediataries such as Paypal) or risk avoidance (using the Internet for research, but completing the transaction over the telephone). **Investment by business in the security of systems would be needed to promote greater trust and uptake** – though there were currently few market incentives for this and it was recognised that it would be hard to guarantee a level of security. **The importance of brands was particularly highlighted as a means of establishing trust in the virtual world – and the potential of some sort of Quality mark or accreditation scheme**. The use of consumer ratings of products and vendors by individual purchasers was also noted as a means of the internet policing itself. **There was agreement of the need for business to store transaction records in order to clamp down on fraud and other criminal activities**. Some were concerned over the loss of anonymity involved through e-payments, though most were fairly indifferent about the issue. With regard to e-cash, its lack of transferability and potential currency fluctuations meant that the idea was not well received.

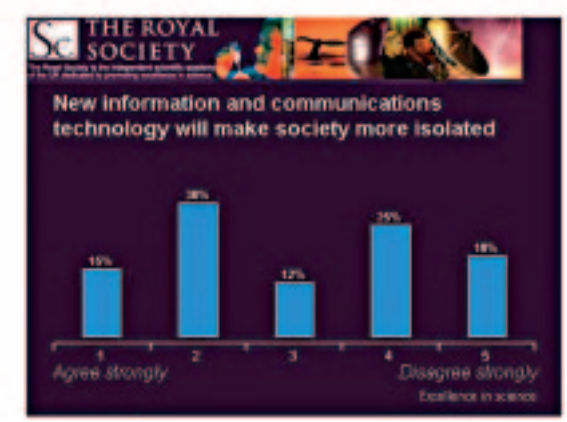
3.3.3 Overall, when considering applications in general, participants were asked to weigh up the potential benefits that the technology may bring against the risks involved, particularly concerning the propensity for fraud and the misuse of information. *Two thirds of people thought the benefit gained from using ICT in general was worth taking the risk, one in ten disagreed, and one in five was unsure* (figure 2).

Figure 2.
Interactive vote on whether the opportunities gained from ICT are worth taking the risks

3.4 The impact on society

3.4.1 As well as the impact of the technology on individuals, societal wide impacts were explored by participants. Key issues included the extent to which new technologies could act to control behaviour through the constant possibility of observation; the potential misuse of power by authorities, for instance to monitor and quell civil protest; the erosion of social and community fabric; and the development of an electronic underclass. The extent to which the technologies isolate society and reduce human contact was a subject of much discussion. For many, this likelihood increased with the potential to effectively work, shop and communicate from the safety of home. The point was tempered by the fact that as communications transform over the next 15 years, they will create new ways of interacting with each other and new social experiences. As such, the participants were fairly split with about 4 in 10 either agreeing or disagreeing that the use of information and communications technology would make society more isolated (figure 3).

Figure 3.
Interactive vote on whether ICT will make society more isolated



3.5 Privacy, trust and the governance of information security

3.5.1 Given the information security focus of the project, the issue of protecting information was discussed in depth. Only one in five trusted Government to protect information (figure 4) because large bureaucracies were not felt to be able to handle data effectively and securely. The potential for human error was believed to be high and many questioned whether the government would be sufficiently joined up and skilled to ensure data protection. Business faired even more poorly – with only one in eight people trusting it to protect information. This time the issue was not one of technical competence, but rather that people simply did not trust business to keep information held upon them confidential. Junk mail proliferation was cited as an example.

Figure 4.
Interactive vote on who the public trust to protect information

3.5.2 The majority of individuals wished to gain control over their own information (about seven in ten). A number of participants suggested that to enable individual control over information, where possible, personal information should be stored on SMART cards rather than networks of interconnected servers, with the level of access restricted by cryptography. In addition, people were keen to have better control over their own security. The main related issue to this is one of competency - it was generally felt that people did not have the basic skills to promote information security and often unwittingly engaged in unsafe on-line behaviour. E-literacy was thus paramount.

3.5.3 Finally, and related to the above, only one in five were confident in society being able to control the technology (figure 5). There were a host of reasons for this: low trust in organisations; human error and competence; experience of day-to-day problems with the reliability of technology; the complexity of systems and the potential for small problems to have large impacts; incentives for remote crime; lack of market incentive for business to invest in security of systems; and the practicalities of effectively governing and policing an international and remote technology effectively.

Figure 5.
Interactive vote on the confidence in the ability to control ICT

3.5.4 This withstanding, people were supportive of these technologies as a force for social good. To realise such benefits, a coordinated effort by government, business and individuals to make systems more secure, to use information responsibly and develop appropriate regulation and enforcement will be required. **Three quarters of participants viewed an independent watchdog as the most effective way of building trust in information systems with individual empowerment and consent at the heart of information security policy.** Complacency will be the biggest risk involved – without action now to address the issues raised through the workshops the potential for large scale problems to undermine confidence in ICT will increase which could in turn precipitate major social consequences.

4 Foresight and future work on Cybertrust

4.1 These findings reinforce the work of the Office of Science and Technology's Foresight programme on Cybertrust and Crime Prevention, whose results from the gaming seminars include:

- 'the desire for access to information on self and the greatest possible individual control consistent with the full range of objectives and technical realities'
- 'the desire for a clear governance structure to detect and react to abuses or failures'
- 'belief that issues for the criminal justice system that are raised by the need to collect and use digital evidence are sufficiently difficult that they are not capable of satisfactory resolution by 2018'

4.2 The findings also complement Foresight's 'next steps' to take forward the work of their project, in terms of future collaboration between bodies to explore project implications; and informing workshops for stakeholders to think about the impact of cybertrust and crime prevention issues in government and industry.

4.3 The Royal Society's Science in Society programme welcomes the opportunity to collaborate on emerging issues in information security, with a particular interest in those with a science and technology dimension.

5 Summary of key findings

- ICT a major force for social good
- Particular benefits seen in crime reduction through surveillance technology and healthcare though the intelligent mining of health records and remote management of chronic conditions
- E-commerce welcomed – providing risks involved in transactions can be successfully managed
- Concerns that complacency will undermine trust in ICT
- Issues of liability need to be clarified to promote trust
- Individuals keen to take control over their information
- Low trust in business and government to protect information
- Only one in five confident in society being able to control the technology
- Coordinated effort between business, government and the public needed to promote information security
- Overall, two thirds of people thought the benefit gained from using ICT was worth taking the risk

6 Summary of recommendations

- Dedicated servers and sophisticated authentication devices for the health service to protect confidential information
- Public consent to personal data collection and compensation if rights are contravened
- Investment by business in the security of systems to promote greater trust and uptake of ICT
- Quality mark or accreditation scheme for e-commerce
- Business should store transaction records in order to clamp down on fraud and other criminal activities
- Where possible, personal information should be stored on SMART cards rather than a network of interconnected servers, with the level of access to information controlled by cryptography
- Co-ordinated programme of e-literacy for all age groups to promote information security
- A watchdog to govern the use of information by government and business, particularly concerning the use and storage of information, supported by three quarters of participants as the most effective way to develop trust in information security

Appendix 1: Scenario

Cybertrust and Information Security: Planning in an uncertain future

Imagine that you are living in the year 2018. Computers and information and communications technology, once only limited to the middle and wealthy classes, have become a utility for everyone, just like water or electricity. Internet access, e-mail, digital radio and live video streaming have transformed entertainment and communication. In every household, fast and affordable Internet networks are connected to digital TVs, home entertainment and computer systems. A range of products exist - from intelligent kitchens that know when you running low on food and reorder online – to cars that are able to diagnose their own faults and book a garage appointment. At home or outside, you are always connected, through wireless transmission and mobile communication devices. The teenager with a mobile phone to their ear has now become a teenager with 3D multimedia headsets.

The Government has made all public services available electronically – with council tax, income support benefits, passport renewals and fines for speeding all delivered online. To implement this, and also to combat rising terrorism fears, there was the compulsory introduction of ID cards, carrying biometric information such as DNA and 'digital signatures' - an electronic code to verify who you are. Thus, your driver's license, passport, football season pass and travel pass are all on the same card. ID cards are combined with an extensive smart surveillance system, so that police can track just about anybody they wish just about all of the time. While physical crime has decreased, the hacking and disruption of government systems often causes problems.

In business, information technology has led to the SSS model - Selling things to you, Stocking in goods and increasing Security. A Loyalty Card is linked to your ID card and provides information on you to your selected stores, who now can track your shopping habits and lifestyle to permit tailored sales, in return for substantial price discounts. The electronic tagging of goods has a number of uses, from the automatic reordering stock to combating shoplifting. The travel industry has been transformed through the use of surveillance systems, electronic ticketing and biometric cards – with people now able to board a plane or ship with no human intervention.

While the information age works well for many people, identity theft is on the rise and accounts for the majority of fraud. Spam, once a major problem is more or less under control – however network crashes can be an annoyance as they disrupt the functions or access to many household, business or public services.

Cyberterrorism – a coordinated massive attack on the IT infrastructure of a city - is a major international concern. While law enforcement is effective in containing much of the threat, people have an uneasy feeling that the situation could easily get out of control.

Citizens have developed an unsure attitude towards information and communication services – they find it typically useful and, at times, necessary, if they wanted to get things done. However, concerns exist that people are not able to exercise any control—for all the increases in benefit, the harms, including the costs of preventing harms, are higher than what is deemed acceptable. This is reflected in television broadcasting; with current affairs programmes like Cyberrama discussing issues like privacy and security, while the most watched programme in the UK is the commercial reality series Your Daily Fraud hosted by the eternal Ant and Dec.

Appendix 2: Case Studies

Case study one: e-Payment

Online payments already exist, from Internet shopping for food, to selling things on sites such as e-bay. Internet payments are usually carried out using encryption (a means of encoding information) to make sure information about an account from which a payment is made is transferred across the Internet securely. To do this the identity and authenticity people involved in the transaction need to be known and proved - for instance you need to know your computer is really connected to the local garage when purchasing your new car online, subsequently you need to know you are really connected to the local council when paying a parking ticket.

To help person-to-person exchanges, on-line payment services such as Paypal have been developed recently. These provide a third-party 'go-between' to ensure buyers and sellers fulfil business agreements. Instead of paying a seller directly, buyers pay a company, which then shuttles the payment to the seller- only after the buyer receives and approves the goods.

In the future e-payments will take various forms. Some will be the money transfers described above. Other payments could be done using new forms of currency, such as e-cash, or other exchanges of some form of value agreed between parties, for instance swapping or bartering goods or knowledge.

Since money is involved, or something close to it, there is potential for crime. But like credit-card fraud, the amount of money lost due to on-line fraud may be difficult to measure as financial companies may be reluctant to reveal the levels of fraud they experience for fear of damaging their reputations.

Emerging technology will allow more devices to be used for e-payments such as mobile phones. For example, registered users can already pay the central London congestion charge by text message. This use of mobile phones is set to expand and other devices are not far behind.

To develop confidence in e-payments, a transaction in a virtual world must be enforceable in the real world. This means dependable systems and compensation will be needed where mistakes or failures occur, whether these mistakes are human error or criminal.

Because the Internet is world wide, e-payment also has to be legally enforceable across national boundaries. Privacy is an issue as this will mean transactions may be tracked. The liability of each party will need to be known and the technology may need to provide a verifiable audit trail for each transaction.

There are powerful incentives for this development in security. Business needs to avoid losses and the government need standards and regulations to enhance public confidence and the UK's reputation as a place to do business.

Governments are likely to make a verified identity a condition of any online or physical payment. It could be based on biometric measures at the point of payment, or use direct transfer to a verifiable account.

Case study two: On-line Medical Support

The potential for online medical support is vast and includes diagnosis, health management and treatment regimes. For instance, diabetes sufferers could be given instruments to measure blood sugar levels at home, the data would then be sent from their computer via the Internet to a NHS server, the results would be analysed and automatically sent back together with a warning if there are problems. Other applications could include healthcare advice provided over the Internet by a healthcare professional using a video-link or even a virtual Doctor.

As well as medical support, information technologies offer the potential for the development of large databases of online health records, lifestyle and genetic information. This will enable better analysis and prediction of health risks in society.

To deliver such online services, there will be the need to be partnerships between the NHS and the private sector to ensure the processes of healthcare delivery have an effective information infrastructure which is well integrated and secure.

There will be a number of legal, social and ethical aspects of the development of healthcare-related technology and products. In healthcare it is assumed that data gathered is confidential, a principle enshrined in common law. There is, however, a considerable debate about the ownership and use of patient data and human tissue, and on the ownership and use of such databases.

Medical information demands high levels of security and privacy. The medical database system described will have many access points, including hospitals, ambulances and doctors' surgeries. Security issues will also arise where treatment is automated - only authorised people should have the ability to apply, amend or terminate treatment. The market for medical information is huge. It includes insurers and credit agencies, and the even the media where celebrities are concerned.

Case study three: Customer relations

Businesses want to know about their customers. Computer software and increasingly the Internet can help them do this. Customers can be identified (either by a postal or email address, or by a loyalty card) and data collected on them to determine their current shopping habits and suggest their future needs. In exchange for such information, customers may be offered discounts on particular goods or gain points that may be redeemed against certain prizes.

Today technology makes it possible for information on your local area to be available to you on demand – this might be using your mobile to find out the name and telephone number of your nearest take way. Alternatively, if you are lost, to have a map of your location sent to your mobile. In the future pervasive information technology will allow offers sent to your mobile to entice you into a shop or restaurant as you walk past.

Information on what you buy using your credit-card and store-card is already searched for relevant information such as what your favourite brands are in the supermarket. This information can show life style changes such as going on a diet. The use of your bank cards can locate you at a particular place and time. Some people use their credit cards only to withdraw money, to reduce the amount of data on them. Information from credit card transactions could soon be linked to information on your location picked up from your mobile phone or CCTV.

Information tags inserted into products may soon mean that everything you buy that's more expensive than a Mars bar can be tracked. This will cut down on shoplifting and help businesses stock and reorder goods. But it raises the possibility of being tracked though our personal possessions both in and out the store. Supermarkets are already starting to install "smart shelves" with networked information tag readers. Banks are considering embedding tags into banknotes. Shops may soon be able to relate the jumper that you are wearing to your name and address. Local shops will be able to flash ads on screens based on your spending patterns. Future muggers could canvass alleys with tag detectors, looking for expensive electronic equipment.

At the moment, data is not shared between companies or agencies without your consent. Moreover, there is no single means of identifying people across all their transactions. However, in the future, to make systems integrated one proved, verifiable and up-to-date identity may be needed. A potential is therefore that identity cards are used in this process. Such ID cards may contain a great deal of their personal information, such as health records. Privacy issues will therefore affect how such technology is employed.

Business may be less concerned with data accuracy where its costs outweigh the benefits, and may accept partial identities or even out of date data, if bringing information up to date is too expensive. Companies who are keen to keep a good image (to attract customers) will find it worthwhile to establish and maintain a trustworthy system.

Case study four: Crime Prevention

The police and the criminal justice system are making more use of information and communications technology. This requires the systems they use to be exceptionally trustworthy and secure.

Today the police use computers for forensic information to help solve crimes two main ways. The first way is concerns the computer itself storing incriminating evidence on information systems such as files, digital photographs, or software – e.g. in Internet paedophilia cases. The second way is for computers to store information and evidence that has been collected from a crime scene – e.g. information about a burglary suspect.

To make sure evidence can be admitted in court the police need to record where the evidence was found and how the evidence has been handled. An existing problem is how any computer that is seized is handled so that the information it contains is not tampered with. A clear audit trail of information collection will be required for a safe conviction.

Technologies can also assist with gathering evidence at the scene-of-the-crime. For example, a mobile DNA testing unit could be used to process DNA samples collected from a crime scene there and then. The unit would be linked to national DNA database and suspects can then be identified.

As well as DNA information the police could also hold information about a person's benefits, tax and financial information. Knowing a person's location from their mobile phone, electronic tags in goods and the increased use CCTV would increase privacy concerns, but could allow tracking of known or suspected criminals by the police or security services.

To help fight cyber crime, warrants to search cyberspace will need to be created, preferably on-line because speed of response can be critical.

The systems described will be expensive. But it could reduce costs elsewhere in the criminal justice system by saving police time and also some work could be done online, for example – an on-line version of the small claims court may be possible.

There will also be fears of the systems failing. The system will also be a target for criminals, particularly organised crime. Obtaining data from the system could yield high rewards. Data could also be discredited, damaging a prosecution case.

Case study five: Provision of benefits

Benefits provision is one of a range of government services that is highly dependent upon a proved verifiable identity, to ensure people get the benefits to which they are entitled. In the future, ID cards or smart-cards, incorporating biometric data such as DNA for authentication, could be used to allow people to gain access to government services. These services could be set up remotely, so claiming income support or your old age pension could one day be done from the home.

Benefits often provide for those most in need in society. A problem is that eligible people may not have access to the technology. They could also be targeted by criminals. There could also be a percentage of faulty claims which will need to be dealt with.

Benefit fraud is a big concern for Government (currently estimated to cost the treasury £2 billion annually). Such technologies could help reduce this level of fraud. Governments may use the technology to store information and develop sophisticated agency checks.

The data held about an individual on central databases will be of interest to parts of the financial services industry dealing with credit worthiness and to insurers. The security of those databases will probably be critical for public confidence, providing a target for hackers, organised crime and cyber-terrorists. Robust systems and software will be required. The degree of acceptable access and the methods to manage it will be vital.

Appendix 3: Media coverage

- **Thursday 1 April 2004**
- Radio Leicester interview with Dr Darren Bhattachary about local debate on cybertrust

- **Wednesday 14 April 2004**
- Daily Telegraph p 14 'Will computers run your world?' by the Earl of Selborne,

- **Thursday 22 April 2004**
- Computing p 5 'National debate on IT trust'

- **Friday 23 April 2004**
- BBC Breakfast News interview with Dr Darren Bhattachary about the Forum Debate

- **Saturday 24 April 2004**
- BBC News Online 'ID cards have 'hidden dangers''http://news.bbc.co.uk/1/hi/uk_politics/3656083.stm
- The Scotsman 'Warning of ID Card 'Hidden Dangers' http://news.scotsman.com/latest.cfm?id=2826251
- News-Medical.net 'Sleepwalking into our technological future'
- http://www.news-medical.net/view_article.asp?id=820
- Sky TV News live coverage of the National Forum on Cybertrust interviewing The Earl of Selborne, Dr Darren Bhattachary and Bob Ward. Channel Four News and BBC TV News interviewed the Earl of Selborne

- **Sunday 25 April 2004**
- Epolitix.com 'ID cards could prevent attack, claims Blunkett' http://www.epolitix.com/EN/News/200404/027fff59-081d-4142-b740-04572a2f7b5e.htm
- Sunday Observer 'Muslim women exempt from ID pictures'
- Sunday Telegraph 'Scientist issues ID card 'wake-up' call'
- Sunday Times 'Straw leads bid to wreck Blunkett ID card scheme'
- World News 'Identity cards for all Britons' New Kerala, India http://www.newkerala.com/news-daily/news/features.php?action=fullnews&showcomments=1&id=13609

- **Monday 26 April 2004**
- ThisIsLondon.co.uk 'New powers back up ID cards' http://www.thisislondon.co.uk/news/articles/10435220?source=Evening%20Standard
- BBC News Online 'ID card plans due to be unveiled' http://news.bbc.co.uk/1/hi/uk_politics/3658489.stm

- **Wednesday 28 April 2004**
- Computing Weekly. 'Watchdog Needed to Build Trust' - interview with Dr Darren Bhattachary

- **Friday 30 April 2004**
- Times Higher Education Supplement p 2 'In the News' – Lord Selborne

Appendix 4 – Impact of process on participants' attitudes

Impact on public participants attitudinal statements towards science and technology: before Dialogue (n=82) and after national forum (n=79)
Interested / very interested in the following areas of science:

- Genetics: 46% (before) 71% (after)
- Computing: 81% (before) 86% (after)
- GM: 36% (before) 46% (after)
- Climate change 68% (before) 76% (after)
- Cloning: 33% (before) 54% (after)
- Telecommunications 78% (before) 80% (after)

Agree / Agree strongly with following statements

- Achievements science overrated: 40% (before) 27% (after)
- Public views should be taken into account when making decisions about science: 79% (before) 84% (after)
- People lack knowledge about science: 77% (before) 79% (after)
- Decisions on science should be left to scientists: 38% (before) 35% (after)
- Scientists want to make life better: 62% (before) 80% (after)
- Media sensationalises science: 44% (before) 65% (after)

Trust following to tell truth

- Doctor: 84% (before) 85% (after)
- NGO: 57% (before) 47% (after)
- Scientist: 50% (before) 61% (after)
- MP: 6% (before) 5% (after)
- Teacher: 71% (before) 79% (after)
- Police: 45% (before) 47% (after)
- Journalist: 12% (before) 4% (after)