The Royal Academy of Engineering

Dilemmas of Privacy and Surveillance

Challenges of Technological Change

The Royal Academy of Engineering

Dilemmas of Privacy and Surveillance

Challenges of Technological Change

ISBN: 1-903496-32-2

March 2007

Published by
The Royal Academy of Engineering
29 Great Peter Street
London
SW1P 3LW

Copies of this report are available online at
www.raeng.org.uk/policy/reports/default.htm

Tel: 020 7227 0500 Fax: 020 7233 0054
www.raeng.org.uk
Registered Charity Number: 293074

Foreword

Advances in technology have the potential to do great good, but they also carry the risk of doing damage if they are introduced without proper care and forethought. One of The Royal Academy of Engineering's priorities is to lead debate on matters of engineering by guiding thinking, influencing public policy making and providing a forum for the exchange of ideas. This report is a contribution to the public debate on information technology and its possible impacts on our privacy.

The report argues that the collection, storage and processing of personal data can be of great benefit to citizens, but that users' privacy must be protected. Engineers have some responsibility for designing systems that enhance data protection. The report outlines some of the critical points where technology could be used for unreasonable or unnecessary surveillance, where technical failures can lead to loss of data and diminished trust, and where computer processing of personal data can have unwarranted consequences for fair treatment and human rights.

In order to comment on these issues, a combination of engineering expertise and social scientific understanding is required. The group that authored the report is almost uniquely well-placed in this respect, with eminent members from The Royal Academy of Engineering and the UK's Academy of Social Sciences participating in the discussions that led to its publication. Both the engineers and the social scientists made individually valuable contributions, but it was the debates between them that sparked the best ideas and that has made this report especially innovative and authoritative.

The report includes a number of recommendations for improving the benefits and reducing the problems likely to stem from advances in information technology that could affect privacy and surveillance. Some of these recommendations are directed at engineers, especially those involved in specifying and designing systems. Some of them are aimed at policymakers, including the Government and the Information Commissioner, who need to be aware of and pro-active in relation to technological developments. Some of the recommendations are for commercial organisations that collect data about individuals as part of their everyday business. In addition, the report notes that there are some important areas where we do not yet know enough and where additional research needs to be commissioned by, for example, the Research Councils.

The report and its recommendations focus on the United Kingdom. However, issues of privacy and surveillance are not confined within national borders. The Internet and its disregard for state boundaries means that policies to protect privacy have to be made with an understanding of the limits to what can be achieved through national legislation. Policy in the UK has to be made within the context of the directives of the European Union and the laws of our trading partners. It is therefore important that the report and its recommendations should influence policy not just within the UK, but also internationally. I am glad that the increasing interchange of information and opinion between Information Commissioners and between academics and policy makers in different countries is making that more likely to happen.

Privacy is a topic that we all feel strongly about. We all also resent the emergence of the 'surveillance society', yet demand that wrong-doers and terrorists are identified and apprehended before they can do mischief. We see the growing numbers of TV cameras in the streets and hear about biometric passports and identity fraud. Engineers' knowledge and experience can help to inform the debates that surround these contentious issues. The Royal Academy of Engineering offers this report as a contribution to these debates.

Nigel Gilbert FREng AcSS
Chairman of the Academy's group on Privacy and Surveillance

Index

1. Executive Summary

This study identifies likely developments in information technology in the near future, considers their impact on the citizen, and makes recommendations on how to optimize their benefits to society. The report focuses on an area where the developments in IT have had a particularly significant impact in our everyday lives - the use of IT in surveillance, data-capture, and identity management. It looks at the threats that these technologies may pose and at the role engineering can play in avoiding and managing these risks. The following is a summary of the central concepts and issues that the report investigates and the judgments the report makes about them.

Technological development: Technologies for the collection, storage, transmission and processing of data are developing rapidly. These technological developments promise many benefits: improved means of storing and analysing medical records and health data could lead to improvements in medical care and in management of public health; electronic logging of journey details can promise improved provision of public transport and more logical pricing for road use; and more details of peoples' everyday behaviour offer the possibility for developing better public policy generally.

However, the development of these technologies also has the potential to impact significantly on privacy. How they develop is to a large extent under the control of society. They can be allowed to develop in a way that means personal data are open to the view of others - either centralised spies or local peeping toms. Or, they can be allowed to develop so that personal data are collected and stored in an organised, controlled and secure manner. There is a choice between a 'Big Brother' world where individual privacy is almost extinct and a world where the data are kept by individual organisations or services, and kept secret and secure. The development of technology should be monitored and managed so that its potential effects are understood and controlled. The possibility of failures of technologies needs to be explored thoroughly, so that failures can be prepared for and, where possible, prevented.

Designing for privacy: There is a challenge to engineers to design products and services which can be enjoyed whilst their users' privacy is protected. Just as security features have been incorporated into car design, privacy protecting features should be incorporated into the design of products and services that rely on divulging personal information. For example: means of charging road users for the journeys they make can be devised in such a way that an individuals' journeys are kept private; ID or 'rights' cards can be designed so that they can be used to verify essential information without giving away superfluous personal information or creating a detailed audit trail of individuals' behaviour; sensitive personal information stored electronically could potentially be protected from theft or misuse by using digital rights management technology. Engineering ingenuity should be exploited to explore new ways of protecting privacy.

Privacy and the law: British and European citizens have a right to privacy that is protected in law. The adequate exercise of that right depends on what is understood by 'privacy'. This notion needs clarification, in order to aid the application of the law, and to protect adequately those whose privacy is under threat. In particular, it is essential that privacy laws keep up with the technological developments which impact on the right to and the expectation of privacy, especially the development of the Internet as a networking space and a repository of personal information. The laws protecting privacy need to be clarified in order to be more effective. As well as making the letter of the law more perspicuous, the spirit must be made more powerful - the penalties for breaches of the Data Protection Act (1998) are close to trivial. The report backs calls for greater penalties for misuse of data - including custodial sentences.

Surveillance: The level of surveillance of public spaces has increased rapidly over recent years, and continues to grow. Moreover, the development of digital surveillance technology means that the nature of surveillance has changed dramatically. Digital surveillance means that there is no barrier to storing all footage indefinitely and ever-improving means of image-searching, in tandem with developments in face and gait-recognition technologies, allows footage to be searched for individual people. This will one day make it possible to 'Google spacetime', to find the location of a specified individual at some particular time and date.

Methods of surveillance need to be explored which can offer the benefits of surveillance whilst being publicly acceptable. This will involve frank discussion of the effectiveness of surveillance. There should also be investigation of the possibility of designing surveillance systems that are successful in reducing crimes whilst reducing collateral intrusion into the lives of law-abiding citizens.

Technology and trust: Trust in the government is essential to democracy. Government use of surveillance and data collection technology, as well as the greater collection and storage of personal data by government, have the potential to decrease the level of democratic trust significantly. The extent of citizens' trust in the government to procure and manage new technologies successfully can be damaged if such projects fail. Essential to generating trust is action by government to consider as wide a range of failure scenarios as possible, so that failures can be prevented where possible, and government can be prepared for them where not. There also need to be new processes and agencies to implement improvements. If a government is seen as implementing technologies wisely, then it will be considered more trustworthy.

Protecting data: Loss or theft of personal data, or significant mistakes in personal data, can have catastrophic effects on an individual. They may find themselves refused credit, refused services, the subject of suspicion, or liable for debts that they did not incur. There is a need for new thinking on how personal data is stored and processed. Trusted third parties could act as data banks, holding data securely, ensuring it is correct and passing it on only when authorised. Citizens could have their rights over the ownership, use and protection of their personal data clarified in a digital charter which would specify just how electronic personal data can be used and how it should be protected.

Equality: Personal data are frequently used to construct profiles and the results used to make judgements about individuals in terms of their creditworthiness, their value to a company and the level of customer service they should receive. Although profiling will reveal significant differences between individuals, the results of profiling should not be used for unjustifiable discrimination against individuals or groups. Profiling should also be executed with care, to avoid individuals being mistakenly classified in a certain group and thus losing rights which are legitimately theirs.

Reciprocity: Reciprocity between subject and controller is essential to ensure that data collection and surveillance technologies are used in a fair way. Reciprocity is the establishment of two-way communication and genuine dialogue, and is key to making surveillance acceptable to citizens. An essential problem with the surveillance of public spaces is that the individual citizen is in no position either to accept or reject surveillance. This heightens the sense that we may be developing a 'Big Brother' society. This should be redressed by allowing citizens access to more information about exactly when, where and why they are being watched, so that they can raise objections to surveillance if it is deemed unnecessary or excessively intrusive.

Recommendations

R1 Systems that involve the collection, checking and processing of personal information should be designed in order to diminish the risk of failure as far as reasonably practicable. Development of such systems should make the best use of engineering expertise in assessing and managing vulnerabilities and risks. Public sector organisations should take the lead in this area, as they collect and process a great deal of sensitive personal data, often on a non-voluntary basis.

R2 Many failures can be foreseen. It is essential to have procedures in place to deal with the consequences of failure in systems used to collect, store or process personal information. These should include processes for aiding and compensating individuals who are affected.

R3 Human rights law already requires that everyone should have their reasonable expectation of privacy respected and protected. Clarification of what counts as a reasonable expectation of privacy is necessary in order to protect this right and a public debate, including the legal, technical and political communities, should be encouraged in order to work towards a consensus on the definition of what is a 'reasonable expectation'. This debate should take into account the effect of an easily searchable Internet when deciding what counts as a reasonable expectation of privacy.

R4 The powers of the Information Commissioner should be extended. Significant penalties - including custodial sentences - should be imposed on individuals or organisations that misuse data. The Information Commissioner should also have the power to perform audits and to direct that audits be performed by approved auditors in order to encourage organisations to always process data in accordance with the Data Protection Act. A public debate should be held on whether the primary control should be on the collection of data, or whether it is the processing and use of data that should be controlled, with penalties for improper use.

R5 Organisations should not seek to identify the individuals with whom they have dealings if all they require is authentication of rightful access to goods or services. Systems that allow automated access to a service such as public

transport should be developed to use only the minimal authenticating information necessary. When organisations do desire identification, they should be required to justify why identification, rather than authentication, is needed. In such circumstances, a minimum of identifying information should be expected.

R6 Research into the effectiveness of camera surveillance is necessary, to judge whether its potential intrusion into people's privacy is outweighed by its benefits. Effort should be put into researching ways of monitoring public spaces that minimise the impact on privacy - for example, pursuing engineering research into developing effective means of automated surveillance which ignore law-abiding activities.

R7 Information technology services should be designed to maintain privacy. Research should be pursued into the possibility of 'designing for privacy' and a concern for privacy should be encouraged amongst practising engineers and engineering teachers. Possibilities include designing methods of payment for travel and other goods and services without revealing identity and protecting electronic personal information by using similar methods to those used for protecting copyrighted electronic material.

R8 There is need for clarity on the rights and expectations that individuals have over their personal information. A digital charter outlining an individual's rights and expectations over how their data are managed, shared and protected would deliver that clarity. Access by individuals to their personal data should also be made easier; for example, by automatically providing free copies of credit reports annually.

There should be debate on how personal data are protected - how it can be ensured that the data are accurate, secure and private. Companies, or other trusted, third-party organisations, could have the role of data banks - trusted guardians of personal data. Research into innovative business models for such companies should be encouraged.

R9 Commercial organisations that select their customers or vary their offers to individuals on the basis of profiling should be required, on request, to divulge to the data subjects that profiling has been used. Profiling will always be used to differentiate between customers, but unfair or excessively discriminating profiling systems should not be permitted.

R10 Data collection and use systems should be designed so that there is reciprocity between data subjects and owners of the system. This includes transparency about the kinds of data collected and the uses intended for it; and data subjects having the right to receive clear explanations and justifications for data requests. In the case of camera surveillance, there should be debate on and research into ways to allow the public some level of access to the images captured by surveillance cameras.

2. Introduction

This chapter sets out the aims, style and method of the report. It explains how the report was produced and the intentions behind the report.

2.1. Aims

This study was established by the Royal Academy of Engineering in order to identify likely developments in information technology (IT) over the next five to ten years, to consider their impact on the citizen, and to make recommendations to optimise their benefits to society. It was intended that the recommendations would encompass proposals for additional research (both technical and social); suggestions for changes to the regulatory environment; and guidelines for operators, institutions, government and individuals on dealing with the future digital world.

The report focuses on an area where the developments in IT have had a particularly significant impact in our everyday lives - the use of IT in surveillance, data-capture, and identity management. Technologies such as mobile phones, number plate recognition systems, surveillance cameras and even London Transport's Oyster card can all be used to monitor people's daily movements. Underlying these technologies is the rapidly increasing capacity for data storage, allowing the information collected using these technologies to be stored for indefinite periods.

A major section of the report is dedicated to analysis of this area of technology, and a projection of its future development. This involves predicting the different ways that technology and society could develop together and imagining how the world might be if these technologies were designed and deployed in different ways.

A report recently produced for the Office of the Information Commissioner (ICO) by the Surveillance Studies Network highlighted the extent to which everyday life has become the subject of surveillance (*A Report on the Surveillance Society*, November 2006). The Royal Academy of Engineering's report seeks to analyse the dilemmas inherent in this surveillance - the protection it offers compared with the threats it poses to privacy - and to offer suggestions, technical and regulatory, for ways to navigate these dilemmas and to protect privacy wherever possible.

2.2. Method, scope and style

The report has been produced by an inter-disciplinary group, and deals with issues at the interface of technology and social policy. The Royal Academy of Engineering is a body with expertise in the field of engineering, but in this report it has not restricted itself to the engineering aspects of the technologies that it is exploring. Rather, it is also examining the policy issues that will arise as these technologies come into mainstream use, and in order to do this, it also looks at social and political concepts - such as privacy, identity and trust - central to these policy issues. Despite the location of the report at the interface between technology and society, and the reference to the impacts that technology has on society, it is not assumed that these two areas are separate with technology acting on society from without. It is widely accepted that the course of technological development is influenced by social, political and economic factors. This report assumes that social and personal values are essential in determining which technologies come to be developed and deployed. It must make this assumption, since its aim is to play a part in ensuring that identity management and surveillance technologies develop ways that are maximally beneficial to society.

The report is aimed at both experts and non-experts in the various fields it addresses. Its aim is to raise awareness of the issues it discusses, rather than giving the final word on them. The report is not an academic article, and as such generally refrains from using detailed references or quotes. However, the literature that has informed the production of the report is listed in detail in the bibliography.

The report was produced largely through the personal research of the working group members. The working group also issued a call for evidence. Evidence received was used to inform and direct the group's discussion.

2.3. Theme - dilemmas

The technologies described in this report both promise great benefits and pose potential threats. In some cases those benefits and threats are so sharply opposed, and yet so equally matched in importance, that dilemmas arise. The key

aspect of a dilemma is the absence of clear agreement about right and wrong actions in a conflict. Dilemmas can derive from a clash of values, opposing ethical perspectives, and disagreements about how particular costs and benefits are to be weighed. Dilemmas also arise in relation to risk, uncertainty and trust. The difficulties of predicting future social and political developments, and of foreseeing how technologies will develop, mean that there is always uncertainty regarding the sensitivity and security of data. For example, developments in the analysis of DNA made over the last two decades mean that people may have concerns over the retention of blood or other medical samples that they would not have had some years ago. This raises problems in deciding which kinds of data should be requested of people - and deciding when it is safe to divulge data.

2.3.1. Privacy dilemmas

The major issue for most of the technologies considered in this report is the extent to which they require us to trade some aspect or degree of our personal privacy in exchange for some other benefit or convenience - either to ourselves or society as a whole.

However, dilemmas concerning privacy are many and varied, as privacy itself is a multifaceted concept. Privacy comes in many forms, relating to what it is that one wishes to keep private:

- privacy as confidentiality: we might want to keep certain information about ourselves, or certain things that we do, secret from everyone else or selected others;
- privacy as anonymity: we might want some of our actions (even those done in public) not to be traceable to us as specific individuals;
- similarly, we might wish for privacy of identity: the right to keep one's identity unknown for any reason, including keeping one's individual identity separate from a public persona or official role;
- privacy as self-determination: we might consider some of our behaviour private in that it is 'up to us' and no business of others (where those 'others' may range from the state to our employers);
- similarly, we can understand privacy as freedom to be 'left alone', to go about our business without being checked on: this includes freedom of expression, as we might wish to express views that the government, our employers, or our neighbours might not like to hear;
- privacy as control of personal data: we might desire the right to control information about us - where it is recorded, who sees it, who ensures that it is correct, and so on.

These various forms of privacy can potentially clash with a number of values. Each has to be weighed against one or more of the following:

- accountability for personal or official actions;
- the need for crime prevention and detection and for security generally: our desire to be able to engage in our personal affairs without anyone knowing is always offset against our desire for criminals not to have the same opportunity;
- efficiency, convenience and speed in access to goods or services: this relates particularly to services accessed online, where access might depend on entering personal, identifying information;
- access to services that depend on fulfilling specific criteria such as being above an age limit or having a disability, or being the genuine owner of a particular credit card;
- the need to monitor health risks, such as outbreaks of infectious diseases;
- public and legal standards of behaviour which might weigh against some personal choices.

The varieties of privacy and the various values it can be in tension with mean that one cannot appeal to a straightforward, singular right to privacy. Privacy is inherently contingent and political, sensitive to changes in society and changes in technology. This means that there needs to be constant reappraisal of whether data are to be considered private and constant reappraisal of the way privacy dilemmas are handled.

2.3.2. Surveillance dilemmas

Surveillance is frequently treated as inevitably infringing liberal conceptions of the rights of individuals and citizens. However, some surveillance has aims that do not deserve to elicit criticism and alarm. Surveillance can be a source of social knowledge, a check on what we think is happening, a 'streetlight' in the public domain, or as a 'searchlight' in specific cases. Some of the benefits of surveillance, such as security, better information, monitoring and learning, can become available to all manner of stakeholders, and work for or against authority in the public as well as private sectors.

There has been pressure for increases in the extent and means of surveillance as there have been increasing numbers of large-scale, organised terrorist attacks. The so-called 'war on terror' is often appealed to in order to justify closer and more extensive monitoring of behaviour, and fear of terrorism may mean that that this justification is more likely to be accepted. This increased monitoring ranges from increased video surveillance to retention of records of phone calls for a longer period. But devastating as terrorist acts can be, this justification of increased surveillance is open to scrutiny, not only on the basis that it intrudes on privacy, but on the basis of its actual effectiveness. The more that the everyday behaviour of citizens is monitored and recorded, the greater the amount of data there is to be searched in order to detect suspicious behaviours. Concerns arise as methods of surveillance that are established for one purpose are used for other, more intrusive purposes (for example the use of traffic or congestion charge cameras for more general surveillance of motorists).[1] Concerns also arise about the implementation of surveillance. Are camera operatives to be trusted when there are reports in the news of the use of camera footage for titillation? Can camera operatives be trusted to monitor surveillance images objectively, without bias or stereotyping?

Shaping a world where surveillance technologies are deployed to bring about maximum benefit will necessarily involve trade-offs between different values and different ways of apportioning benefits across stakeholder groups. However, some surveillance dilemmas can be avoided by designing surveillance in a way that is more protective of privacy - see sections 7.2.5 and 8.4.2.

A Dilemma

The following is an extreme example of the kind of dilemma that surveillance technologies can give rise to. Terrorist attacks on passenger air flights have had devastating consequences in the past and civilian air travel continues to be a target for terrorism. The threat of attacks on planes in mid-flight could be seriously diminished by putting cameras in the back of all airline seats, so that suspicious activity could be spotted and hopefully stopped in good time. This would surely be beneficial in terms of reducing a serious threat, but it would represent a great intrusion on the privacy of passengers, who would be constantly watched from close range - including when they were sleeping and eating.

This is the kind of dilemma that arises in relation to data collection and surveillance technology. These technologies may be useful in reducing crime and preventing terrorism - something we all wish for, yet they threaten our personal privacy - something that most of us object to. To what extent are we willing to trade privacy in order to tackle crime or terrorism?

2.3.3. Dilemmas and the aims of the report

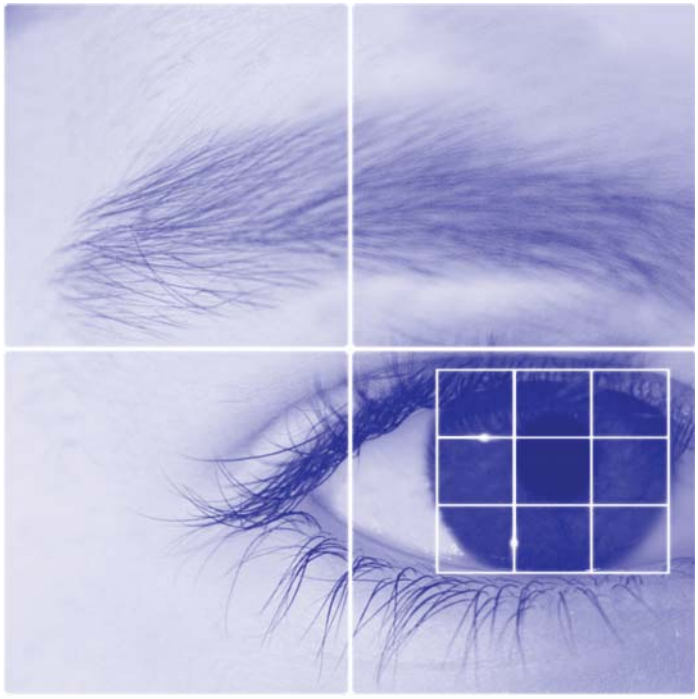
There are no easy answers to the questions posed here. This report therefore does not offer a set of solutions to the problems faced by regulators, policy makers and other organisations and individuals with responsibility for overseeing the place of these technologies in society. If the working group behind this report has a position as such, it is that issues of privacy, surveillance and identity are of growing significance and need to be understood by a broader public if well informed decisions are to be made on policy and practice.

Given the position that the group has taken, the recommendations made in the report are not, in general, definitive directives to policy makers. The recommendations are intended to act as a call to take seriously the dilemmas that will arise as surveillance and identity management technologies are designed and implemented by public and private organisations. They aim to ensure that policy makers, government and other organisations are aware of the potential problems so that they can be prepared to confront these problems. They also offer suggestions for technological and regulatory solutions to privacy issues which are intended to be taken as ideas to stimulate debate and research into protecting and designing for privacy.

The recommendations in this report are also intended to provide inspiration to researchers. The problems that novel technologies can give rise to can often be avoided if they are foreseen, and the technologies designed to avoid or diminish them. The report gives some suggestions of where engineering effort can be focused on 'designing for privacy' - developing technologies in order to diminish threats to privacy and designing novel technologies that can be used to actively protect privacy.

2.4. Structure

The report is divided into three parts: the technological future; the impact of technology on privacy; and the effect of new technologies on trust. Each part outlines how new and emerging technologies might pose threats and discusses how new technologies can be used to deal with these threats and, where possible, diminish them. The first part begins with a look at the likely developments of technologies and the effects that they could have on everyday life.



Part One: Technology

3. Looking into the future

This chapter explores the ways in which technologies for collecting, storing and processing data are likely to evolve over the next five to ten years. It also considers the different ways in which these technologies may affect society, depending on the strategies used for managing or controlling them.

3.1. Technology roadmap

Envisaging how the world of personal data use, management, audit and control is likely to evolve over the medium term need not involve conjuring up any imagined new technologies. All the information and communications technologies that will have an impact over the timescale relevant to this report already exist. The aim of this chapter is to provide a realistic forecast of how these technologies might evolve and be deployed over that timescale and to use that forecast to develop scenarios that can stimulate and inform discussion. This chapter primarily concerns identity management technologies - defining 'identity management' as the access to, administration and audit of information used for identifying people (or in some cases, goods). Chapter 6 looks more closely at video surveillance technologies.

Adopting the above definition of identity management automatically yields a reasonable idea as to the key identity management technologies. But technologies evolve in an interconnected way and so a much wider spectrum of kinds of technologies must be taken into consideration in order to form a realistic picture of the future of identity management. In this report, such a picture will be produced by means of a technology roadmap.

The roadmap which follows was constructed by adopting a layered timeline approach. This identifies the technologies and classifies them in a manageable way in order to highlight the key trends. The technologies are organised in three layers:

- Connection technologies: These are technologies that affect how organisations move data around, as well as how they deliver information and services to customers. Improvements in connection technology have the potential to widen the distribution of products and services and lower transaction costs. They also contain the potential for disintermediation: that is, to connect customers and suppliers directly without middlemen.
  NFC (Near Field Communications) is an example of a connection technology: this is the kind of technology that can allow mobile phones to be used for payment, by passing an NFC enabled phone over a reader. This technology has recently been used as a means for season ticket holders to gain entry to football games.

- Disconnection technologies: These are technologies that provide access control to services and resources, to maintain the security of data. If connection technologies are analogous to doors, disconnection technologies are analogous to locks.
  Tamper-resistant SIM cards are an example of a disconnection technology. SIM cards securely store information like phone numbers as well as storing information that uniquely identifies the phone user. The SIM card on a phone means that only a phone with a given SIM card can make calls chargeable to a given account.

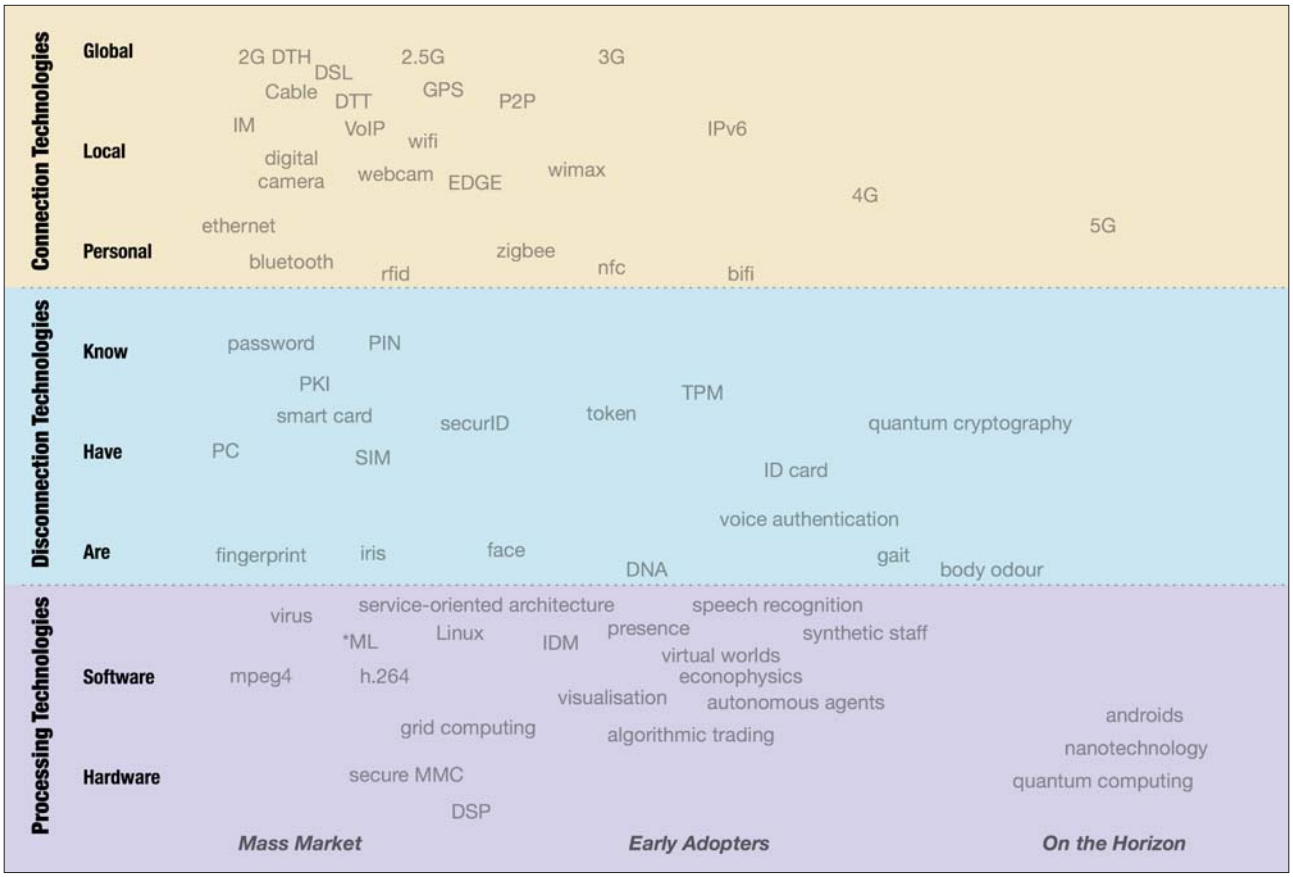
- Processing technologies: These are technologies that affect how data are handled internally within organisations. As connection technologies bring more data across organisational boundaries, so the ability to process data and extract information becomes either a limiting factor or an opportunity for adding value.
  A search engine is an example of a processing technology. Search engines are used to find particular information on the Web, a single Web site, a database or an individual computer.

Dividing the roadmap into these three layers is significant because of the differences between them. Most importantly, while connection is easy disconnection is difficult. That is to say, it is relatively simple to create a network between a set of computers, but it is difficult to partition the data on a computer within a network so that the data can only be accessed by certain computers or users. Disconnection will obviously be crucial to privacy and security of data, the central theme of this report.

The time axis in the roadmap is divided into three broad periods, identifying whether technologies are currently seen as:

- Mass-market: deployed and widely used today.
- 'Rising stars': in development and in some cases deployed today, but generally likely to be commercially widespread in 5-10 years.
- 'On the horizon': still in early stage development and unlikely to have a major impact in the next 10 years.

It is beyond the scope of this report to comment on all relevant technologies and their exact position on the timeline. There will be some potentially relevant technologies that do not appear on the roadmap or in the discussions that follow. It should also be noted that the timeline is presented to illustrate some general points and is not intended to be a prescriptive model of technology roll-out. Terms in the roadmap are explained in the glossary, as are bold terms in the text.



A technology timeline (see the Glossary for explanations of the acronyms)

Each technology layer has been further subdivided into two or three further bands. Connection technologies can make global connections, connecting many devices over long ranges, as in 3G telecommunications technology or GPS (global positioning systems) in vehicles. They can make local connections, for example, connecting a computer to the Internet wirelessly using **WiFi**. Or they can be personal, making a connection between individual people or objects over short range, as with Bluetooth. Disconnection technologies are divided into three strands according to the mechanisms by which disconnections are made and security provided. Mechanisms of disconnection can involve the need to present something you know (eg, a password or pin); something you have (an object such as a SIM card); or something you are (eg, a person with a close to unique face or fingerprint). Processing technologies are subdivided into the familiar categories of software and hardware.

Although all of the technologies that will impact the mass-market in the 5-10 year timescale already exist, some of them will still just be rising-stars, used only by a small number of people. In order to explore these technologies it is helpful to look around at various early-adopter technology 'sandboxes' such as virtual worlds, where millions of people worldwide

already spend a significant amount of their time.[2] Identity and identity management technologies are clearly going to be used to provide infrastructure both for identity management as well as platforms for other services, so one might also expect to see some trends reinforced as new applications come along for those platforms.

The trends that are hardest to spot are those that follow disruptive innovation, since it is the nature of disruptive innovation to upset the smooth and therefore predictable development of trends. The potential for disruptive innovation seems to occur where there is a demand within a sector that is not matched by existing technologies in the mass market, or where there are technologies already in the mass market that are under-utilised by a sector. For example, mobile phone technology is under-utilised in the banking sector: mobile phones are in the hands of almost all customers but they are not yet widely used to combat phishing or reduce credit card fraud.[3]

Having looked at the variety of relevant technologies in this way, we can now go back to the three layers of technology on the timeline and highlight (briefly) some ideas about which technologies will form part of the mainstream evolution and which may be disruptive.

3.1.1. Connection technologies

Connection technologies vary greatly in applicability and in potential usage. For example, **Wimax** (wireless interoperability for microwave access - standard implementation of IEEE 802.16 wireless networks) is likely to develop as an alternative to other means of networking such as Ethernet or cable and so have minimal disruptive influence in terms of deploying identity-based applications. This is likely to be true of other global connection technologies on the roadmap, such as **4G** and **5G**.

Other technologies in this layer will have a greater impact on identity management. **RFID** (Radio Frequency Identification - see the box below for a discussion of its uses) is a highlight of this layer because identifying material goods is just as central to the evolution of identity management as identifying people. Furthermore, RFID tags can be used to identify people too.

Technologies in this layer such as Near-Field Communications **(NFC)** or **Zigbee** have the potential to be disruptive. **NFC**, a specific kind of RFID technology, is used for short-range wireless interactions and extends the capabilities of contactless technologies such as RFID to allow two-way initiation of communications. For example devices embedded with NFC chips can be used as payment devices; payment being made by passing the device (a phone, for example) over a reader. Commercial schemes are working in Japan to embed NFC chips in mobile phones and are likely to combine proximity communications with the longer-range mobile network capabilities. The combination of NFC with mobile technology in particular appears to be a disruptive threat: if mobile phones become security tokens (capable of supporting everything from logging-in to corporate systems to e-Passports) it seems probable that together they will displace a wide variety of existing implementations.

Zigbee refers to a set of specifications for wireless sensor networks, an application of which could be a network of sensors used for home automation which uses sensors to control switches on household devices. Zigbee and other wireless sensor networks create new opportunities for recording data about movements within a particular space; this may be particularly relevant to the insurance industry, for example, through more timely event capture. Spin-off benefits may not be directly linked to identity-related businesses but could still be of interest.

3.1.2. Disconnection technologies

The elements of the emerging disconnection infrastructure can be categorised into a number of distinct groups:

- The **token** group: These are technologies to support tamper-resistant tokens, such as smart cards, mobile phone **SIM**s and so forth. A primary use for these is **authentication** (authentication being the confirmation that someone has the right to access a service or to receive goods, eg., because they have been authorised to do so, they are the appropriate age, they have paid for it etc).
- The biometric group: These are technologies that use biometric data to identify and authenticate individuals, often for local authentication of a person against a token (eg, a chip on a passport).
- The **platform** group: These are technologies that provide platform security - eg, protecting an individual computer. Examples include hardware security modules (**HSM**s) and firewall software and devices.

RFID tags: from goods and livestock to students and drivers?

RFID tags are small wireless devices that provide unique identifiers which can be read by remote sensors. The original aim of these small low cost devices was to enable companies to keep track of stock. However, there are RFID tags which can be 'active' - they emit signals over a greater range and can be sensed remotely - and so concerns over their use have grown. These tiny devices are inconspicuous, meaning that an individual might not be aware that there is an RFID tag in a product they have bought which is transmitting information, nor will they be aware of who is able to pick up the data.

A case in the US in 2005 highlights the way such new technologies can be deployed - and the adverse public reactions to perceived violations of privacy. A pilot scheme in Sutter, California required school pupils to wear ID cards containing RFIDs around their necks. Parents in the small town were unhappy about their children's movements being tracked in this way. The scheme had to be abandoned after protests from parents and civil liberties groups. One of the parents was quoted in the American Civil Liberty Union press release: 'Our children never should have been tagged like pieces of inventory or cattle. The RFID tags violated the students' privacy, they were demeaning and it put them in danger.' (Electronic Frontier Foundation, February 15, 2005 http://www.eff.org/news/).

However, some individuals will gladly be tagged with an RFID chip. A nightclub in Barcelona offered queue-jumping privileges and free drinks to VIP customers willing to have an RFID chip implanted under the skin in their upper arm. (http://news.bbc.co.uk/1/hi/technology/3697940.stm)

In the UK the Department for Transport has approved the trial of car licence plates with embedded RFIDs. The technology is seen as an improvement over optical character recognition for number plates which can fail to read 10-25% of plates. It is also harder to tamper with or clone an RFID tag compared with a standard number plate - an issue highlighted by the introduction of the London congestion charge.

'e-Passports' with RFID chips in them have been issued in the UK since spring 2006. The RFID tag on the passports contain the information and picture from the identification page of the passports - though in future they may also contain further biometric information such as a fingerprint. The information can be read simply by passing the passport over a reader.

Both of these last uses of RFID by UK Government schemes have raised concerns. Firstly, it is possible to use a reader to copy the information from a passport and thus create a 'clone' passport. Secondly, the use of RFID tags for road user charging raised worries of surveillance, since it could potentially be used to create a record of everyday journeys. However, the technologies could be used in a way that better protects privacy (see section 4.2.1 & 7.1.1).

Within the roadmap of disconnection technologies there are several clusters that may have significant impact on identity management, beginning with the more widespread use of tokens for authentication. Although the mobile phone may become the "universal" token in the long run, used to validate one's identity, pay for services and so on, in the short term identity management will be achieved in a number of ways. This is likely to involve a plethora of cards, secure **MMC** (secure versions of the Multimedia Memory Cards used in mobile phones and palmtop computers), secure **USB** (using secure USB keys as a way of authenticating oneself on the Internet - with access to online accounts or online payments requiring the presence of the USB key in the computer) and other solutions.

Voice-based interaction is another salient disconnection technology, promising significant opportunities for the future. The ability to execute transactions securely over voice channels of all kinds would not only provide a high level of convenience, but would also mean advances in compliance (in terms of automating and enforcing rules - because customers will be talking to software agents rather than people in call centres) and forensics (it will be possible to search for a specific individual in voice-recordings). Voice is especially attractive as a biometric identifier because it is passive and non-invasive compared with biometrics that require samples or scans of parts of the body. Although these technologies currently do not work sufficiently well, if voice recognition and speaker identification technologies were to undergo significant improvement, they would clearly represent a disruptive innovation.[4] Another novel technology in this category is gait recognition. This is likely to be used in surveillance systems to identify and trace individuals and is one of the technologies that make modern surveillance systems more powerful (see section 6.1.1).

At the centre of the roadmap are the complementary technologies of identity tokens that may be issued by corporates, Internet service providers, financial services organisations and national governments for physical security (security of people, places and objects - including computer hardware); and Public Key cryptography **(PKI)** for logical security (security of data and of 'virtual identities' (see Processing technologies below)). If they are to become part of a successful identity management infrastructure, they must be integrated. In other words, it would be reasonable to expect citizens, customers, employees, suppliers and business partners to be able to do business online on the basis of some kind of virtual identity communicated, securely using PKI and authenticated using some form of physical identification token.

3.1.3. Processing technologies

Technologies for managing, searching and analysing large quantities of data occupy a distinct position on the roadmap because improvements in them (in combination with advances in connection technologies) entail significant threats to privacy. There are many reasons for improving and standardising in this field: to reduce the cost of reporting and compliance; to provide better forensic capabilities; and to support pattern recognition. When it comes to technologies for exploiting connection infrastructure (grid technology, service-oriented architectures and so on), developments continue apace.

Some technology clusters may have real impact on identity management. Digital signal processing is one such case: it is used in this context to mean the nexus of specialised hardware and software technologies used to extract patterns (i.e. signals) from incoming data in real time. If street sensors reading RFID clothing tags could feed data to a processing centre that spots a pattern (eg, your particular combination of clothes) in the data, then the combination of using RFID tags in clothes and implementing digital signal processing technologies has significant impacts on the possibility of maintaining anonymity.

Another cluster is 'virtual identity', used in this context to mean the technologies supporting sophisticated interaction and trading between online (virtual) entities. Current developments in the field of virtual worlds already provide a mechanism to explore an online future where synthetic staff interact with customers and autonomous agents interact with the market. Virtual worlds are only just being recognised as part of the future mainstream, yet already have a major impact: every year, more than twice as many people visit virtual worlds made by South Koreans than visit South Korea itself.[5]

3.2. Visions of the future - scenarios

This section examines the potential impact of the evolution of these technologies by considering three scenarios, differing according to the balance between and control of the three kinds of technologies.[6]

3.2.1. The 'Big Brother' scenario

In this scenario, both connection and disconnection technologies remain fragmented and beyond central control. In contrast, continued advances in processing technologies mean that it is relatively simple to scan and record all forms of communications: thus, a 'Big Brother' can easily exist. But the implicit mental model of Big Brother that is invoked is curiously old-fashioned, because it is Orwell's vision that has become so dominant. This vision is rooted in a post-war perspective with a bleak political future, where technology is used to create giant databases so that a centralised government can exercise control of society.

However, the danger more likely in present times is that if technology continues to evolve along current lines, 'Big Brother' will end up being more powerful than Orwell envisaged (in the sense that we will have far less individual privacy), though it may not be government that will be empowered. In a world of matchbox-sized camcorders and camera-phones, of always-on broadband and RFID, ordinary people (not a government agency, supermarket or the police) will be the nemesis of privacy. The Internet has the potential to democratise and decentralise Big Brother, as it democratises and decentralises many other phenomena; Big Brother may be 'us', not 'them'.

This form of 'ground-level' surveillance has been called "sousveillance".[7] By its nature it is not under control and there are no transparently obvious ways to bring it under control. If a major retailer were to abuse customers' privacy, those customers could at least look to an industry code or to a watchdog to do something about it. If a government department does something irresponsible with personal data, there is recourse to complain to an ombudsman. But if someone with a camera - phone takes a picture of a businessperson going to a sensitive meeting and then e-mails it to a competitor, it is hard to imagine what could be done about it.

Sadly, some people will find the temptation to do such things as putting a **Trojan horse** on a neighbour's TV or in a colleague's PC overwhelming. It is not only blackmailers or tabloid journalists that will be tempted to look at a celebrity's medical records or a politician's itemised phone bill. This is hardly a far-future speculation; the state of PC and Internet security is often so poor that it is already easy to do. A vision of the future can be found in the 2005 scandal in Israel, in which a number of businesses-including a TV company, a mobile phone operator and a car importer - apparently used a Trojan horse (believed to have been written in the UK) to spy on business rivals.

3.2.2. The 'Big Mess' scenario

This is close to the current situation, where connection dominates and both processing and disconnection are uncoordinated (except in certain specialised subsectors such as defence). Individuals and organisations find it difficult to disconnect and even those organisations with legitimate requirements for processing find it hard to bring together the information they need. The huge volumes of data involved and poor 'navigation aids' result in law enforcement having difficulty tracking links. However, for most people, information security is lacking, be it evidenced by hotels leaving guests' credit card details in skips or privacy commissioners' mobile phone records for sale on the Internet. Each day seems to bring new concerns that serve to undermine public confidence and make it harder for society to reap the benefits of e-health, e-government, e-business and so on.

3.2.3. The 'Little Sister' scenario

In this scenario, disconnection technologies are widely used in a co-ordinated manner: personal data is routinely encrypted and managed in a secure fashion, so co-ordinated connectivity does not threaten it and even substantial processing resources are not a day-to-day threat. This leads to Little Sisters[8] who, by themselves, watch over only a fragment of a person's identity, but when co-ordinated can reveal all.

It would be possible to devise a store loyalty card which incorporated a computer chip that could perform the same functions as an ID card, but without giving away the real name of its owner. Someone might choose a loyalty card in the name of their favourite celebrity, even with the celebrity's picture on the front. If they were to use that card to log on to Internet sites, the fact that they are not really the film star whose name they have used would be irrelevant for most applications, and the privacy of the consumer would be maintained. However, if they did something they should not, such as posting abusive messages in a chat room, law enforcement agencies might then ask Little Sister (ie, the company that runs the loyalty card scheme, in this case) who the person really is, and Little Sister will tell them. In this scenario, government departments are just more Little Sisters, sharing parts of the picture without immediate access to the whole.

This approach exploits both mathematics and economics. If it is technically possible to find out who has done what - for example when a crime has been committed - but cryptography makes it economically prohibitive to monitor people continuously on a large scale, then a reasonable privacy settlement can be achieved.

Lots of Little Sisters might be better than one Big Brother or the current chaotic big mess. However, each of these scenarios has its strengths and weaknesses, risks and benefits. They may all be manifested to some extent in different parts of society and fill different societal needs.

3.3. Conclusions

The world created by the design and deployment of novel technologies is one of our choosing. The different paths that technological development could take result in quite different societies, some more welcome than others. Therefore technological development needs to be steered along the preferred path - what that path should be, which scenario we prefer and how technological development can be influenced are matters that need extended debate. The following chapters provide considerations crucial to that debate.


ENTRANCE-2-1902
2
ENTRANCE-1-1901
3
EXIT-5-1905
4
EXIT-4-1904
5
EXIT-3-1903
6
OFFICE-P1-1941
7
CUST-SERV-1951
8
POF-01-1917
POF-02-1918
9
STAIR-NE-1950
10
ELEVATOR-1-1931
11
ELEVATOR-2-1
12
ELEVATOR-3-1933
13
ELEVATOR-4-1934
14
ELEVATOR-5-1935
15
RAND-ENT-195
16
20:42:44 12/15/2004

4. Predicting and preparing for failure

Like all technologies, those used to collect, process or protect personal data are at risk of failure. Because many of these technologies are new or have only recently been deployed on a large scale, the potential for failure is high. Moreover, in some circumstances, because the technologies are concerned with protecting privacy and establishing identity, failure can have drastic and irreversible consequences. It is therefore essential that good engineering practice be put into place to develop contingency plans for potential failures, as well to encourage system design to minimise the chance of failure and to make systems failsafe where faults or failures are inevitable. This chapter surveys a range of potential failures and their effects and suggests actions that can be taken to avoid them.

4.1. Failure Scenarios

4.1.1. e-Passports

According to current plans, passports will contain increasing amounts of biometric data, stored digitally. Initially this will be a photograph and facial geometry; in future this may extend to fingerprints and iris patterns. These data will be read and used to check the identity of the holder, at passport control, for example. The passport therefore has to be designed to deliver these data quickly and reliably so RFID chips have been proposed (see box in section 3.1.1.).

However, problems could arise based on the way that the data are stored on RFID chips. If the data are stored in an unencrypted form, two vulnerabilities pose problems. Firstly, the passport may be *read covertly* by someone other than passport control. If this were possible (and it could be possible – RFID readers are easily available and someone close enough to a person carrying a passport could potentially read the information on that passport) then not only would the passport holder be revealing identifying and personal information to passport control, but they could also be unwittingly revealing their personal data to 'spies' who had equipped themselves with readers. These Radio Frequency eavesdroppers could use these data for identity fraud of various kinds – for example, if they could access biometric details held on the passport they could use that to access other services using biometrics (eg, a fingerprint template could be used to commit fraud over pay-by-touch systems). With sensitive personal details readable over a distance, it could even become possible, with appropriate antennas and amplification, to construct a bomb that would only detonate in the presence of a particular nationality or even a particular individual.

Secondly, unencrypted data can be *forged*. This would make it possible to modify a passport so that it had the biometric information of the passport carrier, but with forged personal details such as name, date of birth and citizenship. To prevent this, every passport would have to be checked against a central database to ensure that the centrally-held data matched what was on the passport. However, if this were to be the chosen method of operation, it would be unnecessary to store the data on the passport at all because it would be retrieved from the central database. Therefore, the only reason to have the data on the passport is so that it can be checked without recourse to a central database, in which case it must be encrypted to prevent forgery.

Encrypting the data on the e-Passports can help to avoid these problems – but even then there is potential for failure. Firstly, if the encryption codes can be broken, then the two vulnerabilities reappear. Secondly, a problem with current plans for e-Passports in the UK is that the key for the data on the chip is stored on the passport itself – so the encryption does not in fact lock out eavesdroppers.[9] To ensure against these failures, there needs to be a way of encrypting the data with codes that are extremely difficult to break and it should be made impossible to access the encrypted data on the passport by using a key stored on the passport itself. Otherwise, efforts should be focussed on an altogether different way of designing e-Passports.

4.1.2. Database Failures

Databases are vulnerable to a wide range of failures. The following is a list of the kinds of problems that can affect databases.

Large scale loss of data

Data can be lost in a number of ways. It may occur through physical destruction of the storage media (for example, a

server may be destroyed in a fire); through loss of an encryption key – encrypted data are effectively lost if the decryption key is lost; or through corruption by erroneous or malicious programs. If the lost data cannot be recovered quickly from backup storage or by some other means, there will be partial or total loss of the service that the data supported.

This happened when a data centre serving eight major hospitals and more than seventy primary care trusts in the North West of England and the West Midlands failed in July 2006. The result was that staff could not check patients' appointments or access details of admissions and transfers. In this case service was restored within a few days and no clinical information was affected, but if patients' data had been permanently lost, the consequences would have been far more serious.[10]

Leaks of sensitive data

The data on supposedly secure databases could become accessible to unauthorised eyes in a number of ways. Such leaks are almost inevitable if the data are on computers attached to the Internet, because of security weaknesses in all commercially available systems. Leaks are also inevitable if the data are of sufficient value to make it worth bribing someone who has legitimate access to it, or if it is accessible to a wide range of staff.

The consequences of such leaks could be extremely serious – either on a large or an individual scale. Take, for example, leaks of data held on the national children's database proposed by government. Information on this database includes the names, addresses and personal circumstances of children deemed to be at risk and this information could be used by paedophiles to target those children for abuse. Leaks of credit-card data a few years ago allowed newspapers to publish damaging details of a politician's alleged excessive purchasing of alcohol. Leaks of the addresses of staff who work at sensitive sites could expose their families to physical danger: for example, the homes of staff at Cambridge University were targeted by animal rights terrorists earlier this decade. Leaks of health records could jeopardise the lifestyle or employment prospects of patients or even expose them to risk of violence; examples might be HIV status, or a record showing that a woman had had a pregnancy terminated (if this was unknown to her partner or parent), or data (such as DNA or blood group) showing that the paternity of a child could not be the presumed father.

The misuse of data

Data may be misused in many ways. The examples above show how data may be misused as a result of being leaked. However, sometimes the misuse will be by someone who has legitimate access to a database: for example, a 'mole' inside the DVLA provided an animal rights group with information about friends, family and acquaintances of the owners of a guinea pig farm in Staffordshire, after being given the registration numbers of cars visiting the farm.

It is not entirely absurd to imagine that supermarket loyalty-card data might one day be used by the government to identify people who ignored advice to eat healthily, or who drank too much, so that they could be given a lower priority for treatment by the NHS. Whether this should be considered a misuse of the data is debatable, but it would certainly constitute unwelcome 'function creep' for the individuals whose data were initially collected for wholly different purposes.

Human factors

Identity management technologies will be particularly vulnerable to failure due to human factors. The operatives entering data into and retrieving it from databases may cause the data to become vulnerable through malicious or non-malicious leaking or misuse of it. An example of an apparently non-malicious human failure was the widely reported case of a hotel in Brighton leaving personal data about guests, including their credit card details, in a skip (reported in the Guardian on January 9th 2006 as 'Risk of ID theft bonanza as thousands of credit card slips found dumped in skip'). These kinds of errors are dangerous but largely avoidable if proper procedures for handling customers' details are put in place.

Profiling errors

Datasets are routinely mined and profiled so that data subjects can be grouped into categories and receive treatment (eg, special offers, direct marketing, targeted health information) according to their assigned category. But profiling can go awry, either because an inappropriate algorithm is used or the data are bad in the first place. The dangers of profiling are discussed in section 8.3.

Errors in personal data

Errors in the data about individuals can cause distress even when those data are not profiled. In a recent case a practice manager for the NHS discovered that her health records had been sent by a hospital to a private company which in turn sent the records out to various computer systems used by the NHS. When she asked to see the records that had been shared, she discovered a mistake in them: she was detailed as being a patient at a clinic for alcoholism. She requested that her records were removed from the NHS system altogether, as she felt this was the only way to ensure that these incorrect data were not shared further.

Other errors could cause equal distress. For example, if there were erroneous information held by the Criminal Records Bureau on an individual, this could exclude them from any of the very many jobs that involve Criminal Record Bureau checks before working with vulnerable people such as children or the elderly.

Identification errors

A great deal of personal data is used for surveillance and for crime prevention. The data are used to identify individuals for further surveillance or as suspects in crimes. However, if the personal data are connected to an innocent person, what effect could that have? For example, innocent people have been prevented from flying because they have been confused with someone appearing on a US 'no fly list'.

The possibility of misidentification is part of the drive to pin down individuals' identities. Biometric data are often treated as incontrovertible – after all, no one could steal someone's eyeball to fool an iris scanner in the way that they could steal a pin number. ID cards are intended as the ultimate authority on who the cardholder is and the rights that they have and it is the intention to base these around biometrics as a means of identification on the assumption that biometrics are incorrigible. However, the following scenarios should counsel against such an assumption.

4.1.3. Biometrics

Biometric information can be used to identify individuals in two ways. First, it can be used to check a person's identity, by, for instance, taking their fingerprint and checking it against the fingerprint recorded in their file on a database, or checking it against a template held securely on a passport or ID card. In this way it is used to verify that an individual is indeed the person that they claim to be. Second, biometric information can be used to identify a person from traces that they leave behind. For example, fingerprints are used to identify people who were present at a crime scene, by looking for a match between prints found at the scene and templates stored on a database of fingerprints. Both means of biometric identification can fail.

An ID card, or other technology that checks identity by matching biometric information against a particular record, is only good insofar as it can be guaranteed that supposedly unique biometric information (fingerprint, iris pattern and so on) cannot be forged. However, it has been shown that a fingerprint could be forged from a good enough image (for example, the image stored on a biometric passport), by making what is known as a 'gummy finger' – a replica finger made of a gum-like material. This fake finger could be used to fool a reader designed to check fingerprints against records for authentication, or even to plant fingerprints at crime scenes.

The images of fingerprints can, by themselves, be used to commit fraud. A 'pay by touch' system, which uses a fingerprint to authenticate payment, could be 'fooled' by presenting the pay by touch reader with the image of a fingerprint. A pay by touch system could even be the cause of fraud. Imagine a pay by touch system that was tampered with so that it actually recorded the images of fingerprints placed on it, whilst capturing card details. The information intercepted by the reader would give a criminal a harvest of bank details along with the means to access the accounts to which they apply.

Even when biometric information is presented honestly, problems can occur. Identifying a person by their fingerprint, iris or DNA is not perfect with current technology. This is most problematic when it comes to matching trace biometrics with a database of records, as is done in the investigation of crimes. The more biometric identification is used and the larger the database of biometric information, the greater the likelihood of false matches between a person's biometric information and records on databases become. This could result in people being under suspicion of serious crime if their fingerprints are falsely matched with those on a database of fingerprints found at crime scenes. A police officer in Scotland (Shirley McKie) lost her job because her fingerprints were incorrectly identified as being present in a crime scene that she should not have entered.

Biometrics therefore do not provide incontrovertible evidence of identity. If systems which use biometrics as a means of identification are regarded as failure proof, then innocent individuals will suffer. It will become increasingly difficult to prove that they were not present, or did not perform some action, if biometric data or the presence of an ID card purported to be theirs suggests the opposite.

4.1.4. The Internet and the Semantic Web

For every adult in Britain there is a large amount of personal information about them in publicly accessible databases such as the Electoral Register. It is becoming increasingly common for such public data to be published on the Internet – generally for the convenience of the public. Local governments, for example, frequently publish information about planning applications on the Web to make consultation easier.[11] However, the more information that is available about individuals on the Web, the greater the threat of identity fraud.

Identity fraud already happens (see box) and often in a very 'low-tech' way, with fraudsters intercepting mail or even searching bins for personal information and the documents needed to prove identity. However, criminals are turning increasingly to the Internet in order to perpetrate identity fraud, as the crucial information needed to impersonate someone else can be found quickly and easily by Web searches. Moreover, the Internet makes it easier for fraudsters to identify the individuals who it would be most beneficial for them to masquerade as, since there is likely to be information about a person that indicates the kind of job they have and the kind of salary they are likely to earn (for example, CVs and professional homepages). This helps the identity 'thief' to target those people with the most money and the best credit ratings. It is possible that further developments of the Internet, coupled with the increasing amount of information published on the Web, could lead to an increase in this sort of identity fraud.

The Semantic Web[12] allows searches not only of documents published on the Web, but of the data held, and made publicly available, by different organisations. It also makes it possible to collate the results of a search so that all relevant data held by different organisations is displayed as one result. The Semantic Web holds great promise for increasing the power of the Web as a repository of information by allowing greater sharing of knowledge and thereby making the Web an even better research tool. It in effect makes the Web more 'intelligent', and it is the natural evolution of the Internet as it currently is. But as with many of the technologies described in this report it is double-edged – by improving the means for searching the Internet it may also lead to violations of privacy.

The Semantic Web potentially allows the information held about a person to be more easily integrated, thereby making them an easier target for identity fraud. Therefore, as the Semantic Web develops there must be careful monitoring of the documents and information made public on the Internet, to ensure that they do not disclose valuable or sensitive personal information. There also needs to be more research into means by which to protect this personal information from the prying Web-searches performed by Internet criminals.

Identity fraud is not the only worry. As more people use the Web as a social space, posting information about themselves on sites like *myspace* or putting their personal pictures on *Flickr*, the power of the Semantic Web will not only mean that a person's financial status is at risk. Many people, particularly the young, post information in a carefree manner, detailing behaviour that others may frown upon. Applications for jobs, university or school places could be jeopardised by easy access to information about people's pasts or leisure time activities. Given the choice between similarly qualified candidates an employer may well prefer to choose the one who has not posted information about their drinking behaviour on the Internet.

Identity Fraud

Identity fraud (IF) (or as it is often known, identity theft) is the impersonation of someone else in order to obtain financial benefits (for example, by purchasing goods on-line) or to avoid penalties (for example, speeding fines incurred when using a hire car). According to a study by the UK Cabinet Office: 'ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.' [13]

At its simplest, IF is the use of a stolen or cloned credit card: this causes losses to the banks and inconvenience to the credit-card owner as they sort out the liabilities and replace the card. Much more seriously, IF may involve stealing personal documents and using them to obtain a driving licence or other ID documents which can in turn be used to take out large loans, or as proof of ID if arrested. This can lead to a situation where the victim discovers that they have large financial liabilities, or even criminal convictions, and they are left with the problem of proving that the perpetrator was someone else.

If someone's personal details are fraudulently used to secure a loan, it is the provider of that loan who should cover the loss (after all, only the loan provider and not the impersonated individual, was in a position to prevent the fraud). However, the impersonated individual will still suffer if the fraud is not discovered for some time (as is common in such cases) because the defaulted payments will affect their credit score and could mean that they are subsequently refused credit.

4.2. Shaping the future – designing out threats

There are ways to avoid the kinds of faults and failures in the last section; strategies for doing so are outlined below. This section will begin with some general strategies for avoiding failure.

Two major steps need to be followed when designing any complex system that will involve processing personal data. The first step must be to clarify what the system is for, so that it can be designed to provide the necessary functionality in the simplest and most straightforward way. This will reduce the complexity that can lead to – and conceal – errors and vulnerabilities. The system should be designed so that the smallest amount of sensitive data are stored, for the shortest possible time, with access available to the fewest possible number of people. Step two is to carry out a threat analysis, to identify the potential risks and to decide on strategies to minimise them. Individual risks will have specific best-practice ways to minimise them.

In short, avoiding failure is a matter of good engineering, designing systems that are fit for purpose with careful assessment and management of associated risks. The possibility of failure can never be totally eliminated, but it is essential that, when dealing with individuals' personal information, engineering expertise is used in order to design the best systems possible.

4.2.1. Passports

A number of different strategies can be used to guard the security of passports and the privacy of the data held on them. One is encrypting the data held on any RFID chip or similar device that holds the information on the passport. Another is shielding the chip on the passport so that it cannot be read covertly – in the US passports have been designed with a metal shield to block communications between the chip and a reader when the passport is closed. Of course, a further option is to avoid putting information on a chip on the passport altogether and to rely on a database. Databases can be insecure, but suggestions for protecting databases are described below.

In section 7.2.3 there will be an exploration of novel technologies for creating secure passports or identity cards. It is important that a range of solutions is considered given the possibility of serious failure of an RFID passports system. It is also essential to be aware of the propensity for the security in passports to be broken. Otherwise it may be difficult for victims who have had their passports cloned, or their personal information stolen and misused, to prove their innocence.

4.2.2. Protecting databases

There are a number of ways in which databases can fail, but there is a relatively simple set of principles for ensuring that they are secure. The following principles should be adhered to in order to reduce the prospect of failures relating to databases:

- Never store data in unencrypted form. If data are encrypted, the data remain secure, even if copied.
- If data are incorrect, errors must be corrected swiftly, and those affected informed and compensated equally swiftly.
- The minimum amount of data should be kept for the minimum amount of time – this will reduce the likelihood of data being leaked, lost or misused.
- Data in large databases should be checked regularly with data subjects to ensure that they are accurate.
- If data are lost, individuals affected must be informed and compensated swiftly.

Encrypting data cannot guarantee their security as encryption codes can be cracked. However, encrypting data means that it is far harder to make use of leaked data and means that if data are stolen it will take a certain amount of time before they can be used. This extra time provides the opportunity to take action – for example, if bank details were stolen it would provide time to change those details before a criminal made use of the data. Encrypting data would also mean that they would be less attractive to opportunist theft, for example, database operatives being bribed for information.

For databases containing valuable or sensitive data, systems should be designed to keep an automatic audit of when the data are accessed and by whom and especially when data are changed. This can help to prevent individuals misusing or leaking data. It may also help to deal with mistakes in the data by showing the origin of those mistakes and to whom the incorrect information may have been sent.

4.2.3. Using biometrics wisely

If biometrics are to be used as a means of identification, either in an ID card programme or as a means of security in banking or such, they have to be used in a way that limits both the possibility of those biometrics being compromised and the negative effects of their being compromised. They must also be used in way which excludes as few people as possible, to avoid situations where individuals are unable to enrol on a scheme or are unable to verify their identity.

To exclude the latter situation, identification needs to depend on a range of biometrics, so that each person has a better chance of being correctly identified by their biometric information. If an individual's fingertips have been smoothed through their work, they should be able to be identified by an iris scan. However, it is essential that identification of an individual, for whatever purpose, does not involve checking too wide a range of biometric details together. If fingerprints, iris and face, for example, were all needed for authentication, and one of these were somehow compromised (eg, stolen and used on forged documents) then the person affected would face difficulties in proving their identity.

Moreover, it is important not to use biometrics independently of other methods. A pay-by-touch system that needed both a pin and a fingerprint would be much more successful in preventing fraud than a system that used just the fingerprint. Using combined disconnection mechanisms will be far more secure and could lessen the possibility of committing fraud by stealing and synthesising biometric information. Ensuring that authentication relies on a combination of things that one *knows, has* and *is* (see section 3.1) means that disconnection can be all the more powerful and more difficult to override.

Biometrics need not be restricted to physical body parts as a basis for identification. A person's body is unique to them, but it also cannot be changed, so, once a biometric is compromised, it is compromised permanently. A signature is more or less unique to a person, but it can be changed. Signatures made on an electronic pad were trialled in Hammersmith Hospitals NHS Trust to control access to medication.[14] The trial showed that the use of signatures as biometrics had similar reliability rates as fingerprints, without some of the downsides, such as individuals of certain ethnic backgrounds or work history being unable to register their prints. It was also generally more acceptable to users.

Perhaps most important is consideration of the situations in which biometrics would be used and the mechanisms by which they would be checked. It is reasonable to use biometrics in supervised settings such as in banks where it can be verified that a person is presenting their own fingerprint to the reader. However, it would be unreasonable to use

biometrics as a means of authentication for payment or access to personal information on the Internet, as there would be no means of checking whether someone was presenting their own finger, or the forged template of another person's fingerprint.

In terms of the mechanisms by which biometrics can be checked, different mechanisms have different levels of reliability. If a person's identity were to be checked by searching for a match between their fingerprint or iris scan and a database of images, there would be a significant chance of mismatch or failing to match with the genuine database entry. However, if the individuals' identity were checked by comparing their fingerprint or iris with an image stored on an ID card or similar, so that the checking simply involved comparing two images, the chances of correct identification would be much improved.

The prevention of failures in this area as in others is a matter of good engineering – matching the solution to the need and to the context. For authentication technologies in general it is important to consider the context and the degree of 'proof' of identity needed. It is also important to use different disconnection mechanisms in combination wherever possible, to improve the security and reliability of the authentication process.

4.2.4. Web presence

It is not always possible to control the amount and kind of data available about oneself on the Internet or on public databases. However, people increasingly publish a large amount of personal data themselves. Many people have personal and professional webpages on which they post their CVs. Social networking sites have exploded in popularity over the last two years and many users freely post information about themselves and their everyday lives. Blogs (or weblogs) become ever popular as generic blogging sites make them ever easier to set up and bloggers are often very open in the comments they post on blogs. Therefore, a great deal of the personal information available on the net is posted by the subjects of that information.

In order to prevent people from compromising their own privacy it is essential to inform people of the risks involved in posting information online or submitting personal details to access online services. It is easy to assume that those people accessing your personal pages will be those people interested in your lifestyle and who share your values – and this might encourage a misplaced sense of trust. Greater awareness of the potential ramifications, from identity fraud to reminders of a misspent youth, may make people more cautious when they make personal information public.

There also need to be controls over the amount of information people are asked to submit online. Many websites require registration and the setting up of a username and password. The more passwords people need to create, the more likely they are to use the same password for different sites. Requests for passwords and identifying information should only be made when they are necessary for the delivery of a service.

Finally, there need to be measures in place to deal with the consequences of insecurity of personal data on the Internet. Processes are needed that allow the swift rectification of errors that occur if identity fraud does happen, and the issue of liability for the costs incurred need to be addressed. There is an increasing climate of fear surrounding identity fraud and, while individuals should do all that they can to prevent it (such as shredding personal letters and so on), they should not have to suffer excessively if they are victims. The issue of liability for misuse of and mistakes in personal data will be revisited in chapter 8.

4.3 Conclusions recommendations

The examples in this chapter outline some of the problems that will be encountered more frequently as identity management technologies develop and their use becomes more widespread. This chapter also seeks to give basic suggestions for how such threats should be managed. Key to this is preparedness – government should seek to identify in advance the potential flaws in identity management technologies so that failures can be avoided where possible and mitigated where not. Government and other public bodies should seek the input of engineers to identify risks associated with the technologies that they are employing and to design systems so that these risks are minimised.

Of course, it is not always possible to foresee failures or to predict all the ways that technologies might be used. For example, a team of researchers from the Vrije Universiteit Amsterdam showed that RFID tags can be infected with viruses, and can potentially pass them on to databases when they are scanned (the research is published on the website www.rfidvirus.org). The technology was revealed to have a vulnerability that had not initially been considered.

The chips used in passports and which may be used in ID cards have been cloned, and attempts will no doubt be made to manipulate the data on them. The rate of technological change means that it will always be difficult to proclaim that a technology is failure-proof, with the result that any implementation will involve trading the need to act promptly against the certainty that the technologies really are secure. New technologies will therefore always generate dilemmas, so careful consideration of the need for new technology, the means by which it is implemented and the impacts that it may have will always be necessary.

This chapter has focussed primarily on reactive ways of protecting privacy – by looking at the threats in existing technologies and suggesting ways to avoid them. In chapter 7 a more positive, active view will be taken, by looking at suggestions for how to design and implement technologies so that privacy is built into them from the outset.

R1 Systems that involve the collection, checking and processing of personal information should be designed in order to diminish the risk of failure as far as reasonably practicable. Development of such systems should make the best use of engineering expertise in assessing and managing vulnerabilities and risks. Public sector organisations should take the lead in this area, as they collect and process a great deal of sensitive personal data, often on a non-voluntary basis.

R2 Many failures can be foreseen. It is essential to have procedures in place to deal with the consequences of failure in systems used to collect, store or process personal information. These should include processes for aiding and compensating individuals who are affected.

Part Two: Privacy

5. The law today

Privacy is protected in law. This chapter outlines current legislation relating to privacy and discusses areas where the law is in need of refinement or development. In discussing the extent of the right to privacy, this chapter sets the scene for part two of this report - on how technology can threaten, or can be designed to protect, personal privacy.

5.1. Right to privacy

On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights. Article 12 states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The European Convention on Human Rights, Article 8, states:

> Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The UK is a signatory to the UN Declaration and has incorporated the European Convention of Human Rights in UK law. Freedom from *arbitrary interference with privacy* is therefore required by law and any interference with privacy must pass the test of necessity.

5.2. Data protection

The Data Protection Act 1998 (DPA) implements into UK law the European Data Protection Directive (Directive 95/46/EC). Under the DPA, anyone who is controlling the processing of personal information must comply with eight principles of good information handling. According to the eight principles, the data must be:[15]

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept longer than necessary;
- processed in accordance with individuals' rights;
- appropriately secure;
- not transferred to countries outside the European Economic Area, unless there is adequate protection.

In order for personal data relating to an individual to be considered fairly processed, at least one of the following six conditions must be satisfied:

- the individual has consented to the processing;
- the processing is necessary for performance of a contract with the individual;
- the processing is required under a legal obligation (other than one imposed by the contract);
- the processing is necessary in order to protect the vital interests of the individual;
- the processing is necessary to carry out public functions, e.g. administration of justice;
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it would unjustifiably prejudice the interests of the individual).

The DPA makes special provisions for 'sensitive personal data', which includes data about religious beliefs, political opinions and trade union membership, racial or ethnic origin, health condition and sex life. Further conditions must be met if this sensitive data are to be judged as fairly processed.

Data subjects (i.e. individuals) have specific rights under the DPA. The principal rights are:

- the right of access - which allows the subject to find out what data are held about them;
- the right to prevent processing that causes unwarranted damage or distress to the data subject or another person;
- the right to prevent processing for direct marketing;
- rights in relation to automated decision-taking - individuals can object to decisions made using solely automated means;
- the right to compensation - when the act is breached;
- the right to rectification, blocking, erasure and destruction - when personal details are inaccurate or include opinions which are based on inaccurate information;
- the right to ask the Information Commissioner (see below) to assess whether the Act has been contravened.

The Information Commissioner's Office (ICO) is an independent supervisory authority that regulates and enforces the DPA. The Information Commissioner is appointed by HM the Queen and reports directly to the UK Parliament. The Information Commissioner has the power, once he is satisfied that the DPA has been breached, to issue an enforcement notice on the organisation that has breached the DPA. This notice orders compliance with the regulations. In addition to the DPA, the ICO regulates and enforces the Freedom of Information Act 2000, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Environmental Information Regulations 2004.

The role and powers of the Information Commissioner are described in detail on the dedicated website.[16] The ICO's aims at their broadest are to ensure that:

- Public information is out in the open, unless there are good reasons for non-disclosure
- Personal information is properly protected.

In order to be an effective force and to present a real deterrent against the misuse or reckless use of personal data, there need to be some changes to the DPA and to the role and powers of the Information Commissioner. In its publication *The Glass Consumer*, the National Consumer Council (NCC) argues that the DPA is in need of clarification if it is to provide proper guidance and to be used to monitor data use. Many of the key terms in the Act, even including 'personal information', are ill-defined, making the Act difficult to understand and adhere to. The Information Commissioner agrees with this recommendation, and one of the main current aims of the ICO is to simplify the DPA to make it easier to follow and enforce. However it is worth noting that clarification will in any case come about through the accumulation of a body of case law, and consistency is ensured by the ICO's published guidance on the DPA. The challenge is to clarify the DPA whilst maintaining its consistency with the rather flexible concepts contained in the Data Protection Directive.

However clear it is, the DPA can only deter misuse if there are appropriately punitive penalties for contravening it. In evidence submitted to The Royal Academy of Engineering, the British Computer Society (BCS) suggested that 'realistic penalties, including extraditable prison sentences, for the unauthorised copying and provision or sale of personal information are seriously overdue'. The Information Commissioner has argued that tougher penalties are necessary to deter breaches of the DPA. In the report 'What Price Privacy?' (May 2006), the ICO uncovered a black market for personal information in which addresses, details of car ownership, ex-directory telephone numbers and call records were sold to customers including journalists and debt collection agencies. In some cases, the perpetrators of these crimes had been identified and convicted in court, yet the penalties incurred by their illegal selling of data were far from prohibitive - amounting to fines which were small in comparison with the money they made from their activities. In the report, the ICO calls for prison sentences of up to two years for such criminals - a punishment that might really deter them from violating people's privacy.

The investigative powers of the ICO are limited in that, whilst the ICO, of its own initiative, can undertake assessments of organisations' processing and can issue information notices (requiring the provision of information to assist the ICO in an investigation) and enforcement notices, in practice the limited resources of the ICO tend to mean that its role is largely reactive: ie, action is taken only when a complaint is made. Unlike some of its European counterparts, the ICO

has no powers to carry out audits of information handlers without their consent. The lack of a threat of random checks may mean that many organisations are not as stringent as they would otherwise be in following the law. The ICO is unlikely in the foreseeable future to have sufficient resources to carry out compulsory audits itself, but auditing on behalf of the ICO carried out by approved commercial organisations could be considered (in return for some form of concession by the ICO). The costs of such auditing would need to be funded, perhaps by an increase in the annual notification fee charged.

In addition to having increased criminal sanctions, for the DPA to have its full force it is also important that the ICO continues to publicise people's rights over their information. This will empower individuals, giving them greater control over their data, and greater understanding of the consequences of giving away personal information.

5.3. Reasonable expectation of privacy

Legal decisions on privacy frequently hinge on the issue of what constitutes a 'reasonable expectation of privacy'. Should a celebrity, walking through a large city and going about their personal business, expect to enjoy privacy and not to have their picture taken? Should any citizen expect that when they are going about their law-abiding, everyday business, they should not be watched, nor have their picture taken, nor have any data recorded concerning their whereabouts and behaviour? Decisions in such cases often depend on striking a balance between Articles 8 (Right to respect for private and family life) and 10 (Right to freedom of expression) of the European Convention on Human Rights. Hence, many cases which relate to infringement of privacy pose dilemmas in themselves, where choosing privacy may seem like supporting censorship, while allowing freedom of the press means denying privacy rights.

A significant ruling on the right to privacy followed lengthy and widely publicised legal proceedings between the model, Naomi Campbell, and the Mirror Group of Newspapers (MGN). The case concerned The Mirror newspaper's publication of pictures of Ms Campbell leaving a Narcotics Anonymous meeting. The model had previously (and dishonestly) repeatedly insisted in public that she did not have a drug addiction. She won her case against MGN initially, but this was overturned in a court of appeal. She took her case to the House of Lords, in which the original verdict was reinstated. The fact that the judgment in this case was overturned twice, on the basis of a slim majority at the final stage, demonstrates that current boundaries of protectable privacy are far from clear.

A case taken to the European Court of Human Rights is that of Princess Caroline of Monaco (the case of von Hannover v. Germany (application no. 59320/00)). Princess Caroline had numerous pictures published in the German press of her doing a wide variety of ordinary activities in the course of her private life, and therefore complained that her privacy was being invaded. The Court ruled in her favour, because it distinguished between an official in public on official business and an individual in public in the course of their personal life. The Court stated that if pictures were taken of Princess Caroline when she was acting in the latter role, these were not of public interest and in these cases Princess Caroline had a right to protect her private life.

5.3.1. Privacy and technological development

The case studies above show that it is sometimes difficult to judge when an individual can expect to be acting in private. This is made all the more difficult by the rapid rise in popularity of user-generated websites and the availability of cheaper, better digital cameras and mobile phones. As discussed in chapter 3, 'Big Brother' may not be a figure in authority, but may be the person in the street, taking photos and publishing them on photo sharing sites. As this becomes more popular, everyone, celebrities and 'civilians' alike can expect their image to be captured not only by CCTV cameras, but by amateur photographers who will publish their pictures on the Web. It has commonly been accepted that a photographer wishing to publish a photograph must seek permission from anyone appearing in it, but current behaviour makes this almost impossible. As ways of searching the Internet also improve, pictures, and other personal information, on hitherto obscure webpages will become easier to locate.

Hence, the rise of ubiquitous camera phones and photo-sharing sites, along with more powerful means for searching the Internet, will inevitably change what counts as a reasonable expectation of privacy. There have certainly been major changes in technology since the 1998 Data Protection Act which may have consequences for the DPA. The law needs to keep up with these developments, both in order to have a relevant notion of what counts as reasonable with respect to privacy, and in order to be prepared for any legal issues that arise due to new technologies.[17]

5.4 Conclusions and recommendations

There is need for clarification of the notion of a 'reasonable expectation of privacy' in order that the right to privacy is better understood and better protected. In addition, efforts should be made to clarify privacy law to make it easier to follow, with less room for dispute over its application. Alongside this, there need to be more severe penalties for breach of privacy law, penalties which will represent a real deterrent to those who fail to respect the privacy of individuals.

R3 Human rights law already requires that everyone should have their reasonable expectation of privacy respected and protected. Clarification of what counts as a reasonable expectation of privacy is necessary in order to protect this right and a public debate, including the legal, technical and political communities, should be encouraged in order to work towards a consensus on the definition of what is a 'reasonable expectation'. This debate should take into account the effect of an easily searchable Internet in deciding what counts as a reasonable expectation of privacy.

R4 The powers of the Information Commissioner should be extended. Significant penalties - including custodial sentences - should be imposed on individuals or organisations that misuse data. The Information Commissioner should also have the power to perform audits and to direct that audits be performed by approved auditors in order to encourage organisations to always process data in accordance with the Data Protection Act. A public debate should be held on whether the primary control should be on the collection of data, or whether it is the processing and use of data that should be controlled, with penalties for improper use.

6. Technology, privacy and surveillance

Privacy comes in many forms: privacy as anonymity; the privacy of individual identity versus public persona; privacy as confidentiality of information about oneself or one's activities; and privacy as control of personal data (see section 2.3.1). This chapter discusses the ways in which these aspects of privacy are potentially threatened by the use of various recent and novel technologies.

6.1. Threats to privacy: surveillance on the streets

6.1.1. From closed circuit television to networked digital surveillance

The introduction of a video surveillance system using closed circuit television (CCTV) in 1961 at a London train station heralded the arrival of what is now one of the most ubiquitous and visible privacy-affecting technologies. Over the last ten years, government expenditure on CCTV has risen markedly. There are three features of this form of surveillance that create a series of social, political and technical dilemmas:

- First, it is citizens in public spaces who are the objects of surveillance. This threatens to destroy the 'public privacy' previously enjoyed by anonymous citizens in a public space.
- Second, citizens are in no position to agree to or reject surveillance. This limits the extent of the freedom of citizens to go about their lawful business without being observed and monitored. It also extends the capacity for agencies and institutions to subject a section of the public realm to surveillance for their own purposes.
- Third, the development of surveillance systems has changed what can be gleaned from observations of individuals. As well as recording the presence of and recognising individuals, surveillance systems now offer the possibility of evaluating and making inferences about a person's actions and intentions, drawing on stereotypes and profiling methods.

The ever-increasing extent and scale of such surveillance makes it much more likely that an individual in a large town or city will regularly have their image captured. Concerns also arise from the shift to digital technology, which has enabled two significant developments. First, digital recording capacities mean that images can be stored indefinitely, searched digitally, analysed, reproduced and manipulated with increasing ease. Second, images from any camera can be made available instantly to anyone with the capacity to receive data in this form. Given this potential, it cannot be guaranteed that surveillance images will remain private, or will not be altered, misused or manipulated. A development of a different kind is the addition of microphones to many cameras, so that they can eavesdrop on the conversations of people as they are filmed. Both kinds of development mean that surveillance has become increasingly invasive.[18]

These technical changes have rendered tape-recorded surveillance an obsolete technology, and the term CCTV is now for the most part a misleading label. Modern surveillance systems are no longer 'closed-circuit', and increasing numbers of surveillance systems use networked, digital cameras rather than CCTV. The continued use of the term is an indicator of a general lack of awareness of the nature of contemporary surveillance, and disguises the kinds of purposes, dangers and possibilities of current technologies.

Many modern surveillance systems can instead be thought of as 'public webcams' and they will generally be referred to as such in this report. Although most surveillance cameras do not broadcast to the Web, and are therefore not webcams as such, the way that they function makes them very similar to webcams. For example, they can be - and often are - linked as a network covering a wide space; their footage can be streamed to the Internet or TV; the footage is stored digitally and it can be searched using image searching technologies. These webcams are *public* in that they capture images from public spaces, including images of members of the public. They change private or anonymous behaviour into publicly available images, and they can potentially transmit for public consumption anything captured digitally.

Just as public awareness of how public webcams exist and change public spaces is lagging, so law and custom has been slow to respond. The ubiquity and power of public webcams calls for greater attention to the impact of digitisation on privacy in the public realm, and an end to complacency associated with outdated perceptions that belong in the CCTV era.

6.1.2. How effective is camera surveillance?

Crime prevention is the primary justification for public webcams, but they are often used for other purposes such as monitoring traffic flows. Most recently, measures to combat terrorism have revealed the extent of public webcam capabilities. In other words, public webcams are justified by reference to public utility, most often expressed as security, with economic efficiency as a secondary or subsidiary aim. Social benefits are valued more highly than the rights of individuals.

Two main questions arise from claims about the utility of public webcams: whether the limitations on the rights of individuals entailed in surveillance are sufficiently offset by the expected social benefits; and whether public webcams in fact produce those expected benefits. These questions figure in a number of studies on the use of crime prevention systems (all of which use CCTV as a generic term camera surveillance).

Research on public attitudes to 'Open-Street CCTV' in Glasgow shows that the benefits that individuals experience from increased surveillance may not be that great:

> …when actual, as opposed to prospective, feelings of safety are compared over time, there is no improvement after installation of CCTV cameras. Further, respondents believe that CCTV is better than the police at detecting crime, but that police patrolling are more effective than CCTV in making people feel safer. One way of interpreting this is to suggest that Glaswegians, along with many sociologists, prefer 'natural' to 'electronic' surveillance.[19]

Moreover, the limitations on citizens' rights are not evenly distributed, with negative effects falling in predictable and unfair ways on certain sections of the community. Norris and Armstrong, highlighting the increasing amount of evidence that CCTV operators engage in racial and socio-economic profiling, argue that the selection of targets by CCTV operators can be discriminatory towards males, particularly black males.[20] The 'gaze of the cameras', they found, 'do not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant, or through appearance and demeanor are singled out by operators as unrespectable'.[21] It is therefore debatable whether the benefits of surveillance outweigh its negative effects.

Furthermore, it is far from clear that surveillance brings these intended benefits at all. Research for the Home Office on the impact of CCTV revealed that while there were a number of studies showing successes, there were many that showed failures. The success stories, including CCTV in car parks, tended to include cases where CCTV was introduced alongside other measures.[22]

Taken together, the available studies fail to provide evidence that surveillance brings significant benefits, or that any benefits it brings outweigh the limitations it imposes on individual rights. Hence, this brings into sharp relief the dilemmas associated with the question - what is surveillance for? How can the encroachment on personal freedoms which is the supposed price for greater safety and feelings of security be justified, when it seems that surveillance does not deliver? These are questions that need further scrutiny. The worst way to deal with them is to ignore them on the basis that it seems obvious that increased surveillance will mean decreased crime or on the basis that increased surveillance is inevitable or unstoppable. An open debate on the acceptability and usefulness of surveillance is necessary.

6.2. Surveillance in our Pockets

6.2.1. Mobile phones

As long as it is switched on, a person's mobile phone can reveal where they are, within a range of 150-400 metres in urban areas. There are useful applications for this, for example, missing persons or criminals at large can be traced and found by following their mobile phones; and breakdown companies can use a mobile phone signal to locate stranded motorists.

But the technology can also pose a threat. Ben Goldacre (*The Guardian* Wednesday February 1, 2006) exposed the sinister side of the technology that allows mobile phones to be tracked - ostensibly intended for tracking stock and staff movements. He writes "For the past week I've been tracking my girlfriend through her mobile phone. I can see exactly where she is, at any time of day or night… as long as her phone is on." He did this by registering for a web-based service which allows a given mobile phone to be located. In order to register a phone, the person needs the phone number, and initially, text messages are sent to that phone to show it has been registered to the service, and warn the

user that someone is able to locate them. However, after that initial stage (about five minutes after registering the phone), no more messages are sent, and when a request is sent to locate the phone, the location is shown on the website without it affecting the phone at all. This allows a person to track the owner of the phone without the owner's knowledge, as long as they have access to the phone for just five minutes. Goldacre writes: "Your mobile phone company could make money from selling information about your location to the companies that offer this service. If you have any reason to suspect that your phone might have been out of your sight, even for five minutes, and there is anyone who might want to track you: call your phone company and ask it to find out if there is a trace on your phone. Anybody could be watching you. It could be me."

There are obvious ways of mitigating some of the threats inherent in such services. It can be demanded that providers of such services take measures to ensure the security of the person being located. For example, it would be safer if the phone being tracked received multiple text messages over an extended period of time, or if text messages were sent every time the phone was located. This case shows how what is a morally neutral or potentially beneficial technology can be exploited for less acceptable purposes. It is essential that the providers of such a service are persuaded to ensure that it is developed in a safe way.

Another important issue that this raises is that of public awareness of the capacities of technology. More people are becoming aware that their location can be pinpointed as long as they have their mobile phone switched on, but how many people are aware that this capability for tracking mobile phones has led to the development of personal phone tracking services described above? Surveillance by mobile phone is potentially far less worrying than surveillance by public webcam, as it is voluntary to the extent that one can always turn a mobile phone off. However, this is a choice that a person can make only so long as they are aware that the phone in their pocket can make them a subject of surveillance.

6.2.2. Travel cards

Transport for London's Oyster card scheme has been met with concern and criticism from privacy campaigners. The technology used in an Oyster card is described in chapter 3 - the card uses an RFID chip that stores information, which is read by a reader at a ticket barrier or on a bus when placed on or at a short distance from it. Users of public transport either pre-load the card with cash credit which is used to pay for individual journeys, or the card allows unlimited access to transport within stipulated time and zone limits, equivalent to using the card as a season ticket.

Although the information relevant to allowing access to the transport system is held on the individual card, when the card is touched against a reader information concerning the transaction is saved by the reader, and sent to a central database. This creates a record of the use of a particular card, ie the journeys it was used to make. 'Pay-as-you-go' Oyster cards can be bought without registering them in the name of a particular user; however, in order to buy a season ticket of a month or longer, registration is mandatory. Registration is generally encouraged, so that credit on lost or stolen cards can be reimbursed. Therefore most Oyster cards are linked to a named individual, meaning that the central database contains records of the movements of particular, identifiable individuals. These movements are also easily revealed - simply taking a card to a machine allows access to a record of recent usage.

Information about the journeys made with Oyster cards has been used by the police as a surveillance tool, with the number of requests made by police for Oyster card data increasing. It has been alleged that Oyster card data are used by private investigators to track the movements of spouses suspected of infidelity. Therefore, the Oyster card is not only a means of accessing public transport, but is also a surveillance tool. Although Oyster cards are owned and used voluntarily, the opportunity to opt out of this form of surveillance is taken at a cost. The price differential between journeys paid for by cash and by Oyster card mean that trying to avoid using one is financially punishing, and the options for obtaining and using an unregistered card are limited.

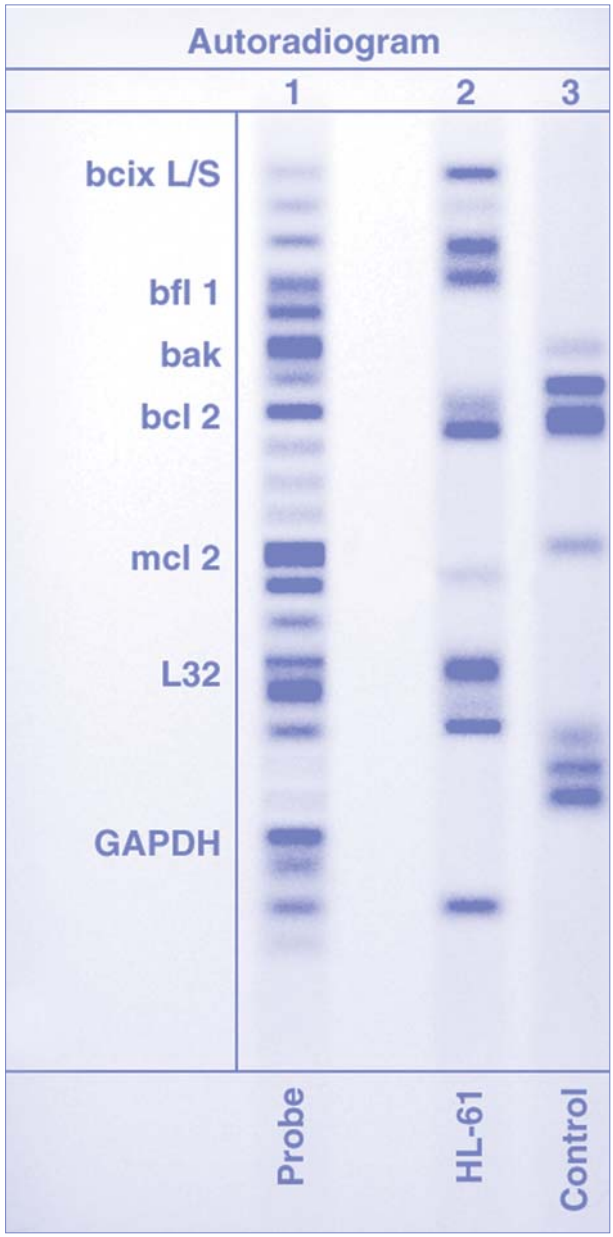
6.2.3. Loyalty cards

Nearly every supermarket, many department stores, chemists, petrol stations and other retail outlets now offer loyalty cards. The schemes are so established and ubiquitous that there is no need for detailed discussion of them here. What is worth considering, however, is how the data created by the use of loyalty cards are, or could be, used. Most people register loyalty cards in their own name, meaning that it is possible for records of the purchases of identifiable individuals to be created and stored. Some schemes, such as the Nectar card in the UK, are run in collaboration with a number of stores and services, so that such a record could provide quite a full picture of a person's activities.

If records of people's food shopping and therefore eating habits are created and retained, could such data be accessed and used by health insurance companies to raise premiums? Or by healthcare providers requiring unhealthy eaters to pay the costs of treating diet-related diseases? What happens if these data are subject to profiling - what effect will this have on the user of the card? (See section 8.3 for a discussion of profiling). If loyalty cards are not used anonymously, privacy in terms of the confidentiality or anonymity of one's actions is compromised. These schemes are voluntary - but do people enter into them with an understanding of the potential repercussions? Of course, one does not have to use a loyalty card for a record of payments to be created. Simply paying for goods with debit or credit cards also creates a rich trail of information about purchases, which could potentially be mined and profiled. Using a bank card is, again, voluntary but many people may not realise the data trail that their use leaves behind.

6.3. Conclusions

This chapter has demonstrated that the vast majority of UK residents are under surveillance everyday, whether that surveillance is entirely imposed on them, or is to some extent voluntary. The next chapter will discuss how to curb this surveillance and how to limit the effects that it has on individuals' privacy.



7. Technology to Protect Privacy

Having discussed threats to privacy in the chapter above, this chapter will discuss designing technologies that do not threaten but, as far as possible, protect privacy. The chapter is in two parts: the first concerns principles that need to be borne in mind when designing technologies to be consistent with privacy; the second gives suggestions of novel ideas for designing privacy protecting technologies.

Just as it is not possible to design a technology that is unbreakable, there is no way to design a technology so that a person's privacy is perfectly protected in all circumstances. A sense of proportionality is needed, fitting solutions to needs and to realistic threats. It is not possible to guard against all conceivable ways of invading privacy but it is possible to 'design out' unnecessary compromises of privacy.

7.1. Concepts of privacy protection

7.1.1. Authentication and identification

Modern societies increasingly use computer-based systems and electronic technologies to deliver services to allow access to restricted areas, to process payments and to authenticate a wide range of other rights. However, the audit trails from these transactions reveal details of the users' lives that they may wish to remain private. The loss of privacy is very much greater if separate audit trails are correlated, exposing exactly who is doing what, and building up a multi-dimensional picture of individuals.

Some of the problems associated with this loss of privacy stem from a general tendency to confuse authentication and identification. To make the notions clear: authentication is a process that results in a person being accepted as authorised to, or having the right to, engage in or perform some activity; identification is the process that results in a person's identity being revealed. Too often, it is assumed that identification is a necessary preliminary to authentication, but in fact identification is only one form of authentication which is not appropriate in all contexts.

A key principle for protecting privacy is therefore the clear separation of authentication (do you have the right to perform this action?) from identification (who are you?). An example could be a cigarette machine, which could legitimately require a user to show that they are over the minimum legal age, but which should not be asking for a name.

Fortunately, many rights to services can be provided anonymously. Examples are the pay-as-you-go mobile telephone and pay-as-you-go Oyster travel cards - which maintain the anonymity of the rights holder as long as they are not registered to a specified user. Since phones and travel cards can be issued and used anonymously, thus cancelling their potential to be used as means of surveillance, this option should be left open to users. In the case of Oyster cards in particular, the options for using them without having to register should be broadened.

In principle, this strategy can be used wherever the associated right only depends on payment. For example, it could be extended to plans for road-user charging. Suggestions for charging drivers for road use have including installing RFID tags into car number plates that can be read by sensors, thus recording the journeys to be charged. If these RFID tags are linked to a specific number plate registered to a specific driver, then this could threaten the privacy of the driver. However, if the RFID tag were in an anonymously owned card, kept in a car and topped up with cash by the driver, then a driver could be charged for road use without making a record of that person's journeys. This could be enforced by using toll gates that do not allow access to a car without sufficient credit on the driver's card. Of course, this system may not be preferable for all drivers, but those who may want to keep their identity to themselves should have the choice.[23]

There is no technical barrier to the development of a 'rights card' which could deliver data that authenticated an individual as the holder of the card, and authorised to perform some specific action (eg buying age-barred goods; entering a secure building; making a bus journey; leaving the UK and re-entering) without divulging the identity of the holder. Chapter 3 describes the kinds of tokens that could be used to this end. Such tokens could be kept

independent, so that it would be very difficult to correlate the records of bus journeys with the records of entering a building or purchasing goods, for example. If deemed necessary, the tokens could even include the holder's identity, encrypted with a public key, so that legitimate law-enforcement agencies could, *in extremis*, access the records and identify specific individuals.

Since it is not always necessary to know the identity of an individual in order to authenticate their rights, good policy-making should distinguish the authentication of a rights-holder from the identification of a specific individual, and justify the latter on a case-by-case basis.

7.1.2. Multiple identities and layers of identity

In some cases authentication involves identifying an individual. Whilst authenticating a person's right to take a tube journey does not require identification, ascertaining that someone is authorised to take out a bank loan in a given name will involve identifying them, in order to prevent fraud or money laundering. However, identification of an individual is a complex matter, as a wide variety of information about a person can be used to identify them. This section looks at how understanding the complexity of identity is essential to safeguarding privacy.

Some rights attach to roles rather than to individuals, and most individuals have many roles: for example they may be someone's employee, someone's parent, a hospital patient, a member of several professional bodies, the holder of a free bus pass, a receiver of state benefits or a victim of a crime. In principle, it is possible to keep these roles separate and there may be legitimate reasons for doing so. For example, the roles may reveal one or more of the following, which some people may have legitimate reasons to conceal:

> Age; HIV status; addiction; physical or mental illness; religion / politics; past traumas (e.g. rape); race / ethnic origins; previous gender; sexual orientation; disability; society membership; job (or lack of job); criminal record; past activities; past identity and present address.

Particular reasons for needing to conceal these details include such issues as:

> Escaping abusive relationships; avoiding stalkers; witness protection; concealing pre-takeover company investigations; protection of celebrities; avoiding identity theft; statutory requirements: e.g. to protect the identities of children in court cases or following adoption.

These concerns highlight the need for mechanisms that make the correlation of different roles difficult; the use of multiple 'identities' or guises is one possibility. For example many women have multiple 'identities' - using their original name professionally and their married name socially, even having two names on their passport. Although these names relate to one and the same person, it is possible to know and be able to identify a person through their professional name, without ever knowing their marital name. For example, someone may work with Ms Jones and be able to point out Ms Jones in a meeting when asked, without knowing that her marital name is Mrs Smith or being able to point out Mrs Smith in a crowd when asked. Ms Jones/Mrs Smith may prefer to have these multiple 'guises', so that she can keep her work and home life separate.

What this example shows is that identity is based to a large extent on relationships with other people or organisations. Ms Jones's professional identity is constituted by her relationship with her employer, colleagues and business contacts and Mrs Smith's social identity is constituted of family relationships and social relationships with friends, as well as an official relationship with the registry of births, deaths and marriage. The same person will also have a number of other identities of the sort described above, based on her relationship to her GP and the NHS more widely, relationship to a professional body,to banks and so on.

In order to ensure that people can keep aspects of their identity compartmentalised legitimately, it is important to recognise that identity is not a simple thing. Identifying information can be more or less detailed, and what counts as identifying information depends to a large extent on context. Name and date of birth might be considered to be the basic identifying information that singles out one individual from another. However, in many situations more information is needed. In a clinical setting, medical records are essential to one's identity as a physical being with certain ailments, allergies and susceptibilities, and these are needed along with a name and date of birth to identify someone - especially when it comes to authenticating access to prescription drugs. When applying for a mortgage,

credit history becomes an important part of one's identity as a 'financial' being, one who has entered into and possibly reneged on various financial agreements in the past, and this is required, along with a name and address, in order to authorise a loan.

Hence, what is in one context simply anecdotal personal history is in another essential information about who a person is, the rights they have, and the services they need. The fact that identity is layered or compartmentalised in this way must be recognised. Demands for identifying information should be restricted to what is necessary in any given context. That is, individuals should be allowed to give only the essential identifying information about themselves in any given situation, and should have the right to withhold other superfluous information that they might wish to keep private in that context. People should also have the right to keep multiple roles or guises distinct, so that it is not obvious to a third party (particularly a malicious third party) that these different identities are identities of the same individual. Having such a fragmented identity could be a major defence against serious identity fraud, because it becomes much harder for a third party to access all of the information needed to impersonate someone.

7.1.3. Digital Identities

Many of a person's multiple identities correspond to digital identities. These are the identities that are used to identify a person to the providers of online goods and services that they use. For example, the information that the bank has about a person who uses Internet banking, the information that allows them to access their bank account and the information about that bank account, is a digital identity. Relationships are central to digital identities too; they are created by the links between an individual and providers of services, people they interact with on the Internet and so on.

Separation of digital identities is key to keeping them protected - especially from the sort of identity fraud described in section 4.1.4. Encryption technology should make it mathematically implausible to deduce further personal information about someone from one digital persona (say, their webmail logon details). If this can be achieved, collating enough personal information to enact identity fraud should be impossible. It should also be possible to disable or delete one digital identity without affecting others. For example, if important details about an individual's banking identity are stolen, that online account could be closed, rendering void any identifying information that allows access to the bank account and destroying that particular relationship with the online banking service. A new identity can be created instead perhaps with another bank, but this should all happen without rendering any other digital or 'real world' identity insecure.

Disconnection technologies can be used to separate authentication from identification and to keep distinct multiple 'identities' - both digital and 'real world' identities. Selective encryption can be used to partition access to particular classes of data, and thereby keep multiple 'identities' separate, and even make it impossible to access the data without the agreement of the data subject. Encryption technology should in effect make it mathematically implausible to deduce one identity from another. This requires privacy protection at a fundamental level, developing online services so that identity information about users can be disconnected in this manner. Privacy has to be engineered into the system at the most fundamental level, allowing anonymity or at least pseudonymity of users (the ability of users to have a different pseudonym for different services) at the level of the infrastructure.

7.1.4. The Context of authentication

It is essential to ensure that the means of identification is fit for the purposes of identification and the context in which it takes place. For reasons described in section 4.2.3, biometrics should not be used as means of authentication in unsupervised settings. The amount of authenticating information should depend on how secure a transaction needs to be - it is a great deal more important for a person to be able to prove their authorisation to take out a mortgage than to buy music on an online store. No means of authentication is failure-proof, but it is wise to fit the degree of certainty with the degree of security needed.

It is important to recognise that there is no single solution for all authentication processes. It is also important not to rely on one single solution in any given context. Problems will arise if devices or systems rely on one single means of authentication - eg, biometrics. It is essential that there are different methods of authenticating someone or proving their identity so a failure in one method does not cripple the whole system, or lock an unfortunate individual out of it. It is a matter of good engineering - designing relevant solutions and incorporating redundancy into them.

7.2. Designing for privacy

In many areas of design, end users are protected from the consequences of their own or others' behaviour. For example, car crime has been reduced because designers have been encouraged to take crime prevention seriously in the design of car locking systems. The designers of IT systems should be encouraged to take a similar approach to end-users' privacy. This section contains some suggestions of ways to design for privacy.

7.2.1. Privacy in Web 2.0

One example where the need to design for privacy is particularly important is for novel on-line services where users may not appreciate the implications of their actions (discussed in section 4.1.4). Personal data can be posted on blogs (made easier by the popularity of generic blogging sites which allow individuals to quickly set up their own sites), or on networking sites such as myspace. A teenager posting personal information on such sites may have very little grasp of the range of people who can access the information or the length of time it may be available. Personal diary entries and pictures could easily be read by future employers vetting job candidates via Internet searches of their names (and aliases, if they are not kept as very careful secrets).

Although these sites should include clear warnings about the potential ramifications of making personal information publicly available on the Internet, some protection should also be built into their design. For example postings to websites might be automatically destroyed after a certain period of time, unless the end user confirmed they wished to have the material retained. Postings to certain services could have an automatic delay before the material was made available to ensure a 'cooling-off' period between posting and publication.

Research could be pursued into the possibility of using Digital Rights Management (DRM) technology to protect personal information.[24] DRM technology is used primarily for music sold over the Internet. The music files that are downloaded have software attached to them which puts limitations on the use that can be made of those files - for example, limiting the number of times that the files can be copied, limiting the number of devices that the files can be copied to or limiting the amount of time that the file can be stored for. Applying this technology to information posted on the Web could allow information to be posted for limited amounts of time, or could allow information to be publicly available on the Web but not copied by others - meaning that the author of the information had control over the amount of time for which it was available, and could also rule out the possibility of the information being altered. Thus it could be used to protect the authors of blogs and the users of social networking sites.

7.2.2. Rights protection on personal information

The use of DRM technology could be extended to far more sensitive information than that which is posted onto websites. Whilst books and music are protected by such technology, safeguarding the copyright and ownership rights of authors or publisher, personal information about individuals has no such protection. Personal information exists in the databases of a wide number of local and national government departments and agencies and in the databases of commercial organisations and marketing companies. This information has no such protection and the subject of the data is not treated as owning that data in any sense and has no real control over it. If personal data were protected by DRM technology, an individual could set controls over who was able to access data about them and could take steps to ensure that data are not shared with organisations who they would not wish to access their data. Moreover, individuals' data would be protected from illicit use and copying by employees of companies using that data for fraud - or selling it onto other individuals who would use it for fraud. Making it difficult to copy or save data in an unauthorised way would be an effective means of protecting against some of the database failures discussed in 4.1.2.

DRM technology is by no means perfect, and current versions would not apply straightforwardly to personal data. It is also the case that it would not stop 'low tech' misuses of data - such as manually copying data from a screen and putting it in new, unprotected documents. However, the technology would still offer some protection and would deter or at least slow down the criminal who wished to steal personal data. There is a good deal of potential in it as a disconnection technology and its applicability to personal data should be fully explored.

However this technology might develop, it is unlikely to be a solution that individuals would be able to implement themselves. However, trusted, third-party organisations could exist with the purpose of guarding individuals' data and setting the appropriate permissions on those data. No individual would be able to reject all access to their data, of course - if a person is a suspect in a crime for example, police would need access to data which reveals their identity - but there should be the possibility to restrict sharing and copying of data within agreed parameters.

7.2.3. e-Passports

It was suggested in section 4.2.1 that one way of ensuring the security of e-Passports was to encrypt the data in the chip, and hope that the encryption does not fail. Another possibility is to forego RFID chips that can be read remotely for more secure methods of checking and verifying passports. One possibility is in the form of a technology being developed by Ingenia Technology called 'Laser Surface Authentication' (LSA) (see www.ingeniatechnology.com).[25] This involves identifying documents, including passports, by means of their unique individual surface qualities. Paper documents and plastics such as credit cards have unique microscopic surface qualities that arise from the arrangement of paper fibres or the way that the plastic has set. These qualities cannot be controlled and cannot be copied, and they are unique in every case - rather like human fingerprints. Ingenia have devised a way of scanning documents to reveal these surface properties, which they refer to as the 'LSA fingerprint'. The system they have created is 'read-only', the document is passive, it is simply scanned and a record of its surface features is recorded. This record will be put on a database alongside an appropriate description - say the details of the passport owner in the case of the passport. If the document is read again this description will be picked out.

This technology has been shown to be highly accurate - the surface qualities at the microscopic level are so unique that a false match is highly unlikely. The upshot is that this system can be used to detect counterfeit passports - passports not previously scanned will have no match on the database. It can also be used to show if a passport is tampered with - if the photo or name is changed this can be revealed on scanning the passport.

This technology could provide a secure way of verifying passports. It would be more secure than an RFID that could be read over a distance. It could also offer privacy gains, as the amount of information on the database available to the person scanning a passport can be controlled - it could be limited to just a name or a photo or even just the assurance that the passport is a genuine passport issued by the appropriate country. This technology could be used for ID cards. Instead of ID cards having chips on them or information printed on their surface, they could be linked to databases in the same way. Provided the database is secure, then individuals' privacy and security is protected. Alternatively, more advanced privacy schemes are possible where the LSA fingerprint is used as an encryption key for locally held personal information. Traditional technologies such as 2D barcodes can be used to carry the information on the card itself. This offers the same immutability of data as would occur if it was held on a central database, combined with the inability to make identical copies.

This of course is not the only option for a technology to base passports and ID cards on, but it is an example of a novel approach to the problem which does not make use of existing technologies with known vulnerabilities - such as RFID chips. Novel approaches like this should be explored to find the best, most-privacy enhancing solutions, for ID cards and passport systems.

7.2.4. ID Cards

Means of verifying ID and the uses to which ID cards can be put could also benefit from novel approaches. If the UK is to introduce ID cards it would be valuable to explore the kinds of form they could have and the benefits that they could offer to their holders.

For example, recent developments in technology (see chapter 3) mean that the token used to hold or to gain access to personal information need not be a card but could be any object that a person always carries with them - a phone, watch or piece of jewellery. If a person must carry a device that holds such significant information, it may be more secure to conceal the identity of that device rather than to have a card which clearly serves that purpose and could be a target for fraudsters. In designing ID cards there is no reason to adhere to the model of an oblong piece of plastic with a photograph and other information printed on it. An ID token could take many forms.

ID tokens could also perform functions of personal benefit to their holders. An ID token could be used as a 'key' allowing access to a PC, so that an individual's PC could only be logged into when the ID token was in close proximity - say the distance that a watch might normally be from a laptop or PC. This would mean that a person's PC would be more secure, by being inaccessible to other users. This could not only benefit its owner - but the subjects of any data held on that PC - a significant advantage given the high profile examples of laptops holding sensitive information being stolen in recent years.

7.2.5. Anonymous surveillance?

The main aims of camera surveillance are to deter potential crimes, to detect and stop crimes when they occur and to identify and capture the perpetrators of crimes that have already occurred. In order for such aims to be satisfied, it is supposed necessary that ordinary law-abiding citizens will have to endure surveillance. If it were possible for surveillance systems to be developed in such a way that limited this collateral intrusion on privacy, the use of surveillance technology may be more acceptable.

One way of attaining this end would be to devise systems that only stepped into action when a suspected crime was taking place. Instead of having operatives scanning hours of mundane footage, feed from the cameras could be examined by an automated system, which alerted the operative when suspicious activities were detected. This would mean that ordinary activities would be effectively ignored, and certainly not scrutinised by an operative.

Algorithmic processing of images by computers for this purpose has so far been less than successful but research should be focussed on how to improve it. A successful automated surveillance system could have a number of benefits. If a system is developed that can successfully target only suspicious behaviour, the law-abiding citizen can be confident that their behaviour is not under scrutiny. Furthermore, research shows that stereotypes seem to affect the way that CCTV operators monitor footage, meaning that surveillance systems have a more negative effect on those who tend to receive poorer treatment in other areas of life. Automated surveillance systems could instead be programmed on the basis of fact rather than prejudice. The algorithms used for identifying suspicious behaviour could be open-source and open to public review to avoid prejudices creeping into the system. Anonymous surveillance could therefore offer a much fairer and therefore more effective means of watching over public spaces.

Research into this technology should be encouraged and intensified, as should study into the way people behave in public spaces, in order to characterise and distinguish between suspicious and acceptable behaviour more accurately. Although doing this may be very difficult, exploring the possibility would be valuable. If this can be done successfully, the targeted surveillance that would result would represent a less serious invasion of privacy than the blanket surveillance currently deployed, with its known shortcomings.[26]

7.2.6. Anonymous digital cash?

There have been a number of schemes already offering ways of paying by card without having an account in a particular name. Most of these have not been successful, but there is still value in researching the possibility of a successful scheme. Many people want to buy goods via the Internet, but doing so often requires using a debit or credit card with their associated wake of data about purchases made. Anonymous digital cash could offer a way around this. Of course, one will have to give away some identifying information to buy goods from online stores and have them delivered, but this option avoids a single, centralised record of everything one has ever bought.

It might be supposed that few people would want this sort of service - only people buying things that might be considered embarrassing or suspicious. However, as with all issues to do with privacy, having something to hide is not the only reason for desiring privacy. For many people, privacy is an end in itself, one that they have the right to enjoy without significant inconvenience.

Another issue is whether people would wish others to have privacy in this arena - for example, the concern might arise that anonymous digital cash was used by money launderers or terrorists seeking to hide their identity. Thus this technology represents another dilemma - should anonymous payment be allowed for those who wish to protect their privacy, or should it be strictly limited so that it is not available to criminals?

7.3. Conclusions and recommendations

The potential technological solutions to privacy issues discussed in this chapter are all intended as suggestions for solutions to privacy problems. Many of them are imperfect or are at an early stage of development. Therefore, none are being recommended outright, but all are discussed to show that there are many options for introducing identity management technologies in a way that does not threaten individuals' privacy or the security of their personal information. These suggestions are primarily here as a stimulus for discussion of, and research into, privacy enhancing technologies. These examples show that designing for privacy is possible and the recommendation of this report is that it is a possibility that must be pursued.

R5 Organisations should not seek to identify the individuals with whom they have dealings if all they require is authentication of rightful access to goods or services. Systems that allow automated access to a service such as public transport should be developed to use only the minimal authenticating information necessary. When organisations do desire identification, they should be required to justify why identification, rather than authentication, is needed. In such circumstances, a minimum of identifying information should be expected.

R6 Research into the effectiveness of camera surveillance is necessary, to judge whether its potential intrusion into people's privacy is outweighed by its benefits. Effort should be put into researching ways of monitoring public spaces that minimise the impact on privacy - for example, pursuing engineering research into developing effective means of automated surveillance which ignore law-abiding activities.

R7 Information technology services should be designed to maintain privacy. Research should be pursued into the possibility of 'designing for privacy' and a concern for privacy should be encouraged amongst practising engineers and engineering teachers. Possibilities include designing methods of payment for travel and other goods and services without revealing identity; and protecting electronic personal information by using similar methods to those used for protecting copyrighted electronic material.

Part Three: Trust

8. Technology, trust and equality

The previous chapter dealt with the way that surveillance technologies can affect aspects of individuals' privacy. This chapter examines how various ways of deploying surveillance technologies and managing data collection can affect our relationships with the government, the state, private companies, public bodies and with each other. It begins by looking at how certain ways of developing and implementing technologies can diminish trust and give rise to inequality and goes on to consider how surveillance and data collection can be carried out in a way that protects trust and diminishes inequality.

8.1. Trust and threats to trust

Trust enhances both the legitimacy of the democratic state and the ability of the government to carry out its responsibilities and its programme. Trust is double-edged, it is developed over time but can be lost quickly. This is reflected in continuing reference in both the media and academic literature to a general crisis in, or decline of, public trust.

Critiques of public policy with specific reference to privacy and surveillance often refer to these debates and ideas, with warnings on the possible detrimental effects on trust of any diminution of privacy, increases in and abuses of surveillance, and the failure of government to protect the privacy of its citizens. Less attention is paid to the dangers of government failing to act, and the impact that inaction can have on trust.

8.1.1. Understanding trust

There are sharp disagreements about the basic meaning of trust, as well as agreement that it can have different functions or roles. Barbara Misztal identifies seven types of trust: as faith; confidence; exchange; expectation; role performance; co-operation; and gift giving.[27] Technological change is accompanied by trust as expectation: the expectation that the state has a duty of care and that whatever government is in office will exercise its powers and deliver the means of protecting us from new dangers. In relation to privacy and surveillance, levels of trust are vulnerable if government appears unresponsive or is deemed too slow to react to the dangers posed by the use of those technologies. Trust has a rational basis, and is accorded only when institutions perform their roles satisfactorily. Institutions generate trust when they perform well and when they do not they are deemed untrustworthy and generate scepticism.[28]

Another important aspect of trust is trust as *interest promotion*. This is about investing trust in an institution because we know and agree with its aims, and believe that its agents will work in accordance with those aims.[29] If enough members of the public hold the view that the state is committed to a proper balance between the interests of its citizens in terms of security and privacy, and believe that agents of the state will work to uphold that balance, then the government of that state will enjoy a great deal of latitude in policy-making, and will be able to implement its policies and rely on public compliance for new laws and regulations.

8.1.2. Trust the state and judge the government?

It is with respect to trust as role performance that governments are most vulnerable. This form of trust is based on people's experiences, as the performance of institutions is monitored by the public and opinions and perceptions subsequently develop. While it might take years of effective governance to establish institutional trust, it can be wiped out very quickly, however fairly or unfairly, by high profile mistakes or accidents. Moreover, trust problems over a particular issue can translate into a mistrust of a whole government (which can be electorally punished), but leave trust in the state (in the police or National Health Service for example) unaffected (though state bodies such as the police or the NHS can lose public trust in some circumstances).

There are a number of incidents in which a government or series of governments have suffered loss of trust due to poor role performance, or perceived poor performance. Crucially to the interests of this report, a number of these relate to the introduction of new technologies. For example, the implementation of a new computer system in the Child Support Agency (CSA) was considered a disaster, with many vulnerable people failing to receive child support payments due to its inadequate functioning. The failures associated with the CSA have been brought up in criticisms of plans for

the NHS project 'Connecting for Health' which involves bringing modern computing systems to the NHS. They have also been raised in connection with the ID cards scheme and the associated National Identity Register (NIR).

Both past problems and recent difficulties mean that government is vulnerable when it comes to trust in their ability to implement a large IT project, or any other complex business change project. Of course, government is not alone in experiencing difficulties in implementing complex projects with a large IT component, but it is particularly vulnerable since its projects use public money and involve critical services such as the NHS.

Because governments are in a fragile position with respect to trust as role performance, properly differentiating between trust in a government that can be removed from office, trust that is placed in the state, and trust about specific policies and actions, is crucial. The state should remain the ultimate protector of citizen rights to privacy and should not garner new powers to invade the privacy or increase surveillance without strong justification and the explicit consent of citizens. The government of the day should only ever have temporary and revocable rights to affect or suspend rights, and their powers should be challengeable in the courts or by appeal to an ombudsman or similar agency.

This principle applies to citizens' data itself, such as that which may be held in the proposed NIR. Such a database should not be owned by a single government department, but should be available for use by all government departments, like the DNA database. Custodianship and control should reside with an independent body. Individuals are citizens of the state, not of the current administration, and their data should not belong to a division of that administration. (See also sections 7.2.2 and 8.2.1 on the need for trusted third parties who will safeguard personal data.)

New technologies that impact on privacy should be assessed accordingly. Some developments call for the clarification and extension of state protections. Others require direct actions by government, including, for example, exclusions, facilitation, laws, regulation and education. A third set of developments - governance measures across the public and private sectors - may require further analysis and information-gathering about the technology as well as details about public expectations and concerns.

8.1.3. Electronic identity - threats to trust

Just as trust in the state is essential for democracy, trust in information systems and technologies is essential for e-government and e-commerce. But novel technologies and processes, such as those involved in e-government and e-commerce, have a fragile status with respect to trust, largely because members of the public do not understand the processes in which they are to place their trust. One of the most important and challenging issues with electronic identities is enhancing users' understanding of what is involved. Users are accustomed to signing papers physically, handling credit and bank cards, and being asked for forms of identity in stores. In the electronic environment, users are not always aware when they are releasing information about themselves, or how much they are releasing. Asked for identity details online, there is a tendency for citizens to over-release: this is probably because online forms offer no flexibility over what information is needed - a form cannot be submitted without providing all of the requested information. Users need to understand what they are doing when using electronic forms of identification, otherwise mistakes may occur which will later negatively affect their trust and further participation in electronic delivery systems.

A closely related problem is usability. If users are overly taxed by the management or handling of electronic identification, they may well revert to conventional methods. Any introduction of electronic methods should be accompanied with campaigns to raise awareness and encourage understanding of how electronic identification functions.

Trust can be further compromised by the modes of failure associated with identity technology - such as biometric identifiers that may be used in identity cards (see sections 4.1.3 and 4.2.3 on biometrics). In essence, a biometric is comparable to a PIN which can never be changed; hence, if it is ever compromised, it is compromised forever (a person cannot get a new set of fingerprints, as they could a new credit card and PIN). Individuals could be subject to masquerade, identity fraud and identity denial, not only by other people, but also by the state. This could potentially be identity fraud of a far more serious nature than is currently prevalent, and the threat of this could seriously compromise trust in the system. Hence it is essential that failure modes are fully explored before the implementation of technology such as biometric identity cards, in order to foresee the problems which might arise, and how they can be dealt with. Chapter 4 above explores some of the ways that surveillance and data collection technologies could fail and suggests some ways of dealing with these failures, but much more research on this topic is necessary.

8.2. Protecting personal data

8.2.1. Liability for data maintenance

Who should be responsible for data kept about citizens: individuals themselves or the state? In the report published by the Council for Science and Technology entitled *Better use of personal information: opportunities and risks*,[30] it was suggested that it should be the individual's responsibility to ensure that information collected about them was accurate. This is based on the idea that the individual should 'own' data about themselves and should have control over it. Although this suggestion seems to empower the individual, one might worry about those individuals ill-equipped to monitor their own data, who might not fully appreciate the significance of errors.

Should the responsibility for accuracy and security of personal data reside with government? Although the government has the responsibility for constructing the legal and policy framework for the governance of privacy and surveillance, the implementation of that policy, the enforcement of regulations, the monitoring of compliance, education of the public, development of enforcement capabilities, and reporting functions belong in a separate agency. As an independent supervisory authority reporting directly to the UK parliament, the Information Commissioner's Office (ICO) satisfies this governance requirement, but needs to have adequate powers to effectively and efficiently fulfil its aims.[31] As discussed in the chapter 5, the ICO lacks the formal investigative powers deployed by the Equal Opportunities Commission and the Commission for Racial Equality since 1975 and 1976 respectively, and available to the Disability Rights Commission since 2000. The ICO needs an equivalent power to carry out formal investigations for any purpose connected with the performance of its statutory duties.

Another possibility is that companies take on the role of trusted custodians of personal data, if there is to be increasing usage of large-scale datasets and profiling techniques. They would manage and protect personal data just as banks are entrusted with people's money. These companies could have the role of protecting personal data against misuse and error, by ensuring it is correct, and that it is only passed on to acceptable organisations. However, this would disadvantage classes of people who could not afford such a service and who would therefore remain vulnerable. An alternative model would be for organisations which require data to pay a company for the data, in exchange for an assurance that the data they receive are up to date and have been passed on to them with the subjects' consent. Such operations could be beneficial to both data users and subjects of data.

There should be research into business models which could deliver this service effectively. What is clear is that there should be a trusted third party with responsibility for safeguarding personal data. Whether that would be a public or private body is a matter for debate.

8.2.2. Liability for misuse

Personal data can be made vulnerable as a result of non-malicious mistakes as well as by identity fraud. For example, that made by the hotel in Brighton which abandoned a large number of confidential registration cards in a skip, leaving them open to theft and abuse by criminals. Although such actions are accidental, they are nevertheless negligent, and the organisations responsible for rendering people's data insecure should put their mistakes right. Such companies should be forced to recompense their clients if they make their personal data vulnerable - perhaps by having to write and apologise to each, offering compensation for the inconvenience of cancelling and replacing cards. Such penalties are used in California, serving to make onerous demands on those companies who are not careful with clients' data. The threat of having to go through such processes if customers' or associates' data are compromised should encourage organisations to be better custodians.

8.2.3. A digital charter?

The fact that so much personal information is stored and processed electronically means that there is need to clarify a person's rights and expectations concerning their personal information. The move to e-government and e-health causes worry, as individuals become concerned that personal information will be shared without their knowledge and that there might be errors in their personal information. It would be valuable to have a digital charter that would outline how personal information, stored electronically, should be shared; the rights that individuals have to access and check those data; and their rights to opt-out from e-government or e-health schemes should they have significant concerns. Devising and enforcing such a charter could have a significant effect on levels of trust.

It is certainly important that individuals are made more aware of how their data are used and are given greater control over it. Access to personal data should be made easier - for example by automatically providing free copies of credit reports annually.

8.3. Profiling and equality

8.3.1. Profiling - scourge or saviour?

This report has shown that many new technological developments involve more accumulation of and access to personal data. They create the possibility of, indeed depend upon, everyday behaviour and normal transactions being recorded and then made available first to the business and administrative entities behind them and ultimately, and should the need arise, to law enforcement agencies of every description. What will happen to those data and how are they used?

The answer to both questions is that data will be accumulated in large databases and then it will be 'mined' for its value: commercial, administrative, medical or judicial. Whilst in the past behaviour was only passively observed, the data that are easily available today can be used to reveal individual preferences and modes of acting in everyday life. Any credit or debit card purchases leave behind a wake of data that is collected, stored and aggregated into databases for mining, and possibly linked with data from other databases, such as electoral registers or credit reference sources. The data are then searched to create profiles, or prototypes, which are used to classify individuals into categories or groups. This allows the massive numbers of individuals that are handled by businesses and administrations in modern systems to be dealt with in a semi-customised manner.[32]

Group profiles have emerged from modern data-driven approaches to marketing, and are a prototype of an abstract person whose pattern of behaviour may never be exactly matched by any flesh-and-blood individual. The key is the category to which individuals may be assigned for the purpose of simplifying further information processing tasks. Groups that may be profiled include car drivers who may be special insurance risks, employees who may be particularly productive, bank customers who may be money launderers or terrorists and so on. The problem is that the categorisation is rarely perfect and individuals may perform in a manner that puts them into one of the groups without real justification. Citizens may coincidentally use a bank account in a manner that resembles the way criminals do, with unexpectedly large amounts being withdrawn at unusual times. As a result, they may find themselves classified in a group profile with undesirable knock-on effects. Such profiling:

> …could possibly be used against individuals without their knowledge, thus shaping their access to facilities, goods and services, also potentially restricting their movement and invading personal space. In fact, this would regulate their access to and participation in, the European Information Society.[33]

Although the algorithms behind such profiles may be created with some input from human experts (so called 'directed bottom-up analysis'), competitive pressures mean that these profiles will increasingly be created 'on the fly' by the computer programs themselves, with no involvement by human actors. Instead of a person there to check that the profile being created makes sense in practical terms and that it is fair, there may just be a program turning out profiles that seem logical to the computer but are nonsense in practical terms. This will produce many false positives (cases included in the category that do not deserve to be there) as we know from the way that credit card fraud checks work at the moment. How will citizens, clients, patients and so on know that they have been unfairly included or excluded until it is too late? Citizens may find themselves stigmatised as criminals or bad creditors without being able to defend themselves and without a sure route to recourse, simply because their data traces match a pre-existing group profile.

As well as group profiling, there is also individual or personalised profiling. A personalised profile is a set of correlated data that identifies a single person - it might be biometric data or behavioural data that is uniquely associated with an individual, such as keystroke data (it may even be the RFID tags in the particular garments you own, as suggested in section 3.1.3 of this report). The use of personalised profiling in commercial contexts has already begun. The danger here is that service providers will only offer one particular service or product because that is what they are deemed to prefer:

> When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? … profiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed.[34]

Profiles are a useful means for service providers to provide an apparently customised service to their consumers, allowing the handling of business on an enormous scale while still seeming to be tailoring offers to the particular individual. Indeed, profiles may reduce the growing information overload that assails the users of modern technology. But at a price: the choices that a free individual may want to make in a given context may not be available, the choice having already been made by some computer program.

It is important that customers are informed when decisions about them are made by wholly automated means. This is because, as explained in the previous chapter, the DPA accords people the right to appeal decisions made by such means. Moreover, since the outcome of that profiling can have an upsetting or humiliating effect on an individual - such as being refused credit - it is important that the subjects of profiling are aware that decisions about them are made on the basis of contestable profiling and do not necessarily reveal the 'truth' about their trustworthiness or credit worthiness.

8.3.2. Dilemmas of profiling

The use, or potential uses of profiling give rise to a sharp dilemma. Should airports use basic profiling to identify people who pose a greater security risk and put them under extra scrutiny? Should police use profiling in attempts to stop terrorists and criminals? There seems a *prima facie* argument for such profiling - namely that more time can be spent putting the people who fit the profile under extra scrutiny, and less can be spent on those who lie far outside it. Stereotypes do exist, and people may feel that it is a waste of resources to screen people who are nothing like the stereotype.

However, this tactic risks treating all people who fit a certain profile as potential terrorists or criminals. It is redolent of racism, ageism, sexism and discrimination against particular religions or denominations. It is very hard to accept that profiling along such lines should go on in a free, open and tolerant society. In addition, profiling in this manner may be counterproductive, since focus on one perceived threat may result in overlooking other threats. It may also generate distrust of the authorities that use such profiling methods - just as police bias towards certain ethnic minorities in making stop and search investigations can undermine trust in the police. While profiling might seem justifiable, its consequences undermine any justification for profiling methods.

8.4. Reciprocity

8.4.1. Reciprocity and trust

Reciprocity is increasingly recognised as an important component of public trust, on which the legitimacy and effectiveness of public institutions depend. As the code of ethics for the American Public Health Association states:

> The effectiveness of institutions depends heavily on the public's trust. Factors that contribute to trust in an institution include the following actions on the part of the institution: communication; truth telling; transparency (ie, not concealing information); accountability; reliability; and reciprocity. One critical form of reciprocity and communication is listening to as well as speaking with the community.[35]

What this means in terms of practical steps that government can take is that it is important to encourage or even require public involvement in public debate, and in the construction and delivery of policy. It is particularly important that in relation to privacy, anonymity, identity management, privacy enhancement technologies and surveillance practices, reciprocal arrangements are devised that enable, empower, and facilitate the continuing involvement of citizens. Public engagement in policy formation will be key to the acceptability of identity management and privacy policy.

This approach to reciprocity and trust would not mean an extension of rights or require the instantiation of new rights. It simply means using existing rights of participation to ensure closer connections between the collectors and users of data and the individuals supplying the data, for example by giving people the right to ask relevant questions of the collector or user. This kind of reciprocity does more than protect so-called negative rights not to be interfered with, or transgressed against. It presumes that, as citizens, we have positive rights to co-operatively engage with others, and leads directly to benefits for all participating parties.

8.4.2. Reciprocity and public webcams

In the case of surveillance and public webcams, reciprocity can be achieved by giving people access to webcam footage so that, by seeing where the webcam operators choose to fix their extended gaze, the watched can watch the watchers. A truly public webcam would bring existing users - the observers, collectors, interpreters and users of such data - into the same, accountable realm as those being observed. It would make people aware that surveillance cameras are quite different to out-moded CCTV technology, giving them a greater understanding of the kind of surveillance they are under.

At present, surveillance systems are closed to those being observed. Public webcam images need not be private, but could be available to all who would use public spaces chosen for surveillance. As discussed in the previous chapter, 'natural' forms of surveillance are preferred by the public, and therefore an effective surveillance system needs to be more like the natural surveillance created when an area is monitored by community members, or known figures such as local police officers. Allowing members of a community access to the cameras that watch over it may be a way of achieving a modern analogue of the village green.

The benefits of this would be significant. A major benefit of surveillance cameras is the peace of mind they offer. Knowing that an area is being watched over can reduce the fear of crime. The benefit might be greater if one could see for oneself that there were no worrying activities - or if there were, one could avoid and report them. Benign uses would abound. It could, for example, offer access to views of local traffic conditions, and permit reciprocal checks on the social behaviour of other drivers. The sense of paranoia that a surveillance camera can create in even a perfectly law-abiding citizen might be mitigated if one knew for certain exactly what it could see. Surveillance is at its most threatening when the citizen is unaware of it, and may be less threatening if one knows exactly when and where one is being watched.

But the greatest value of this sort of 'community webcam' would be its power to prevent a Big Brother state. The authorities in *Nineteen Eighty-Four* held absolute power, keeping the citizen a helpless subject of surveillance. The East German Stasi recruited informants secretly and derived some of their power from no one knowing who was being watched or by whom. In contrast, making surveillance cameras accessible to the community would ensure *reciprocity*, the sharing of power between the watchers and the watched. Community members could object if they felt particular cameras were unnecessary or unnecessarily intrusive. This would limit the potential for voyeuristic or prejudicial misuse of surveillance. Sharing footage from public webcams would result in shared ownership of the system and shared benefits and could create a modern version of community surveillance.

Such a scheme has already been established in Shoreditch, East London. Residents in a specified area are able to access a 'community safety channel' showing images from surveillance cameras in the area. Any suspicious behaviour seen on the channel can be immediately reported to the police via the TV set. Reported in *the Guardian* ('Residents given access to live CCTV footage', Matt Weaver, The Guardian Wednesday January 11, 2006), a spokesman for the Shoreditch Trust said:

> Everybody talks glowingly of the days, in the 1940s and 50s, when neighbours looked out for one another. This is about using technology to allow everyone to look out for each other. This is not about some anonymous Big Brother figure looking down on you, the entire community will have access to this technology…It addresses not just the reality of crime but the fear of crime, which can be just as debilitating as crime itself. It is something that residents find reassuring.

Access to the surveillance footage is controlled in a number of ways. Images from the cameras will be broadcast in 30-second stints, on a loop. Residents will not be able to direct the coverage or record it.

8.4.3. Implementing a public webcam

Such a system might be thought to be a greater intrusion on privacy than the one we have at present. The group Liberty has already expressed concern that the system will infringe on peoples' privacy. There is also the risk that such a public webcam would be misused. Therefore, it would have to be designed and implemented in a way that prevented it from being misused by neighbourhood 'spies' or stalkers, opportunist thieves, or oppressive parents or spouses.

Several options are available for this. Like the footage available to residents in Shoreditch, it should not be within the power of the individual to control the cameras, by directing them or zooming in on particular areas. However,

community members should be able to complain about and thereby alter the positioning of a camera, if they believe the camera is watching over an area where it is not needed, or is excessively intrusive. The images to which the public have access could be limited to those taken from some height, so that whilst an overview of an area is available, revealing whether there are people around, their general behaviour and so on, it is not possible to 'spy' on exactly what one's neighbour or teenage offspring is up to. If these options are still deemed to be too intrusive, a more limited system would allow the community to access intermittent stills taken from the cameras. This would show where the cameras are positioned, without allowing them to be used to watch one's neighbours for extended periods of time.

All such options should be explored. If cameras constantly watch over a community, that community needs to know the extent to which their privacy is limited, and should have a right to question that. Of course, this right has to be made available without further limitation of that privacy, so deep consideration is needed about how that is to be done. Schemes such as that run by the Shoreditch Trust should be closely examined to see whether and where they have succeeded and failed, and lessons should be put into practice.

8.5. Conclusions and recommendations

This chapter has shown the need to address the relationship between individuals and both state-run and private organisations, and the treatment of individuals by both types of organisation. Individual citizens are the subjects of profiling, the subjects of surveillance, the subjects of data in large databases, the victims of identity fraud and so on. This chapter has argued that individuals need greater rights. They need to know when their treatment is due to profiling, so that they can dispute the profiling and the treatment. They need to be clear on who is accountable for protection of their data, and how they are protected if their data are used fraudulently. Generally, they need to have a clear role in reciprocal relationships between themselves and the state or the companies they deal with. One means of achieving reciprocity has been discussed at length above: allowing people access to the video footage routinely taken of them. As this chapter shows, a great deal of thought needs to be put into how public transparency - such as through reciprocity - can be achieved whilst protecting the privacy and security of individuals. But considerations along these lines are necessary, as are creative approaches to establishing reciprocity in other areas of life.

Finally, individuals need to be aware of their rights and responsibilities when it comes to the processing of their personal data. Education is key to enabling people to protect themselves against fraud, stand up for themselves in the face of profiling, and protect data that they can and wish to keep private. Alongside education there needs to be ease of access to the processes that allow people to protect themselves.

R8 There is need for clarity on the rights and expectations that individuals have over their personal information. A digital charter outlining an individual's rights and expectations over how their data are managed, shared and protected would deliver that clarity. Access by individuals to their personal data should also be made easier; for example, by automatically providing free copies of credit reports annually.

There should be debate on how personal data are protected - how it can be ensured that the data are accurate, secure and private. Companies, or other trusted, third-party organisations, could have the role of data banks - trusted guardians of personal data. Research into innovative business models for such companies should be encouraged.

R9 Commercial organisations that select their customers or vary their offers to individuals on the basis of profiling should be required, on request, to divulge to the data subjects that profiling has been used. Profiling will always be used to differentiate between customers, but unfair or excessively discriminating profiling systems should not be permitted

R10 Data collection and use systems should be designed so that there is reciprocity between data subjects and owners of the system. This includes transparency about the kinds of data collected and the uses intended for it; and data subjects having the right to receive clear explanations and justifications for data requests. In the case of camera surveillance, there should be debate on and research into ways to allow the public some level of access to the images captured by surveillance cameras.

9. Glossary

Algorithmic trading: A trading system that uses mathematical models for making transaction decisions in financial markets.

Anonymous/personalised data: Personalised data are data from which the identity of the data subject can be inferred, either from the data themselves, or in conjunction with other easily accessible data. The identity of the data subject cannot be inferred from anonymous data.

Authentication: Verifying that a person, computer, software program or other agent has the right or authority to buy goods, access a service or perform a specific task. To be distinguished from identification, which is only a species of authentication.

BCS: British Computer Society.

Bifi: Using the body as a medium for communication by sending signals through (for example) the skin.

Big Brother: State surveillance of all private and public activities, as described in *Nineteen Eighty-Four*, a novel by George Orwell (pen name of Eric Blair).

Biometric data/Biometric identifiers: Identification by means of biological characteristics, such as fingerprints, iris patterns, or facial geometry.

Blog/Blogging: The term 'blog' derives from 'weblog'. This is an online journal, in which the author expresses personal thoughts or opinions or reports personal events for public consumption.

Civil Society: Where citizens of a state live their lives. It is a realm that is independent of government. It is populated by individuals pursuing their interests and ends, non-state organisations such as families, businesses, churches, pressure groups, voluntary organisations and so on.

Connection/Disconnection/Process technologies: Respectively technologies for: linking systems and transmitting information between them (such as wireless networks) / preventing systems from being linked together or sharing information (such as firewalls, or encryption of data) / information processing to correlate or compare data, such as search engines.

Digital Signal Processing: The processing of a digital signal, often by converting an analogue signal into a digital signal that can more easily be analysed or manipulated.

Disruptive innovation: An innovation that causes a sudden or large change, primarily in society or in business activity.

DPA: Data Protection Act 1988.

DSL, Digital Subscriber Line: A technology that uses telephone lines to provide broadband connection to the Internet.

DTT, Digital Terrestrial Television: The provision of digital television signals through conventional transmitters and domestic aerials (e.g. in the UK, Freeview).

e-government/e-health:. The use of computing technology, especially Internet-based systems, to support access to government services or the provision of healthcare.

EDGE: A digital mobile phone technology which acts as an enhancement to 2G and 2.5G GPRS networks.

(Data) Encryption: The conversion of data into a coded form that makes it impractical for anyone to interpret it unless they possess the secret key, which unlocks the code.

End User Services: An electronic service that is delivered to individual citizens or employees.

Government: The authoritative decision-making arrangements of the state at central and local levels. Government has responsibility for legislation, policy-making and implementation through the state's administrative apparatus.

Governance: The exercise of power and authority in governing, which must include reference to state and non-state institutions and agencies, among whom some power is distributed and shared.

GPS, Global Positioning System: A network of satellites broadcasting precise timing signals by radio to GPS receivers, allowing them to accurately determine their location.

Grid computing: The interconnection of many computers through a high-bandwidth network, coupled with software that supports the co-ordinated use of the connected computers to work co-operatively on a single problem.

H.264: A digital video codec standard which achieves very high data compression.

HSM, Hardware Security Module: A plug-in card or external device for a computer that is used for the generation and physical protection of keys for use in encryption.

ICAO standard: Any standard published by the International Civil Aviation Authority.

ICO, Information Commissioner's Office: The agency established by Government to oversee the effective working of the Data Protection Act, Freedom of Information Act and related legislation.

ID/Identity: Who someone is. Identifying information is information which would allow someone to be recognised or tracked down.

IDM, Identity Management: Mechanisms for establishing who someone is and key facts about them, such that the facts can be retrieved and related to an individual in the future.

IM, Instant Messaging: Any technology that allows the transmission of text or picture messages across a network with very little average delay. Examples are the Short Message Service (SMS) on mobile phones, and Microsoft Messenger on Windows-based PCs.

Infrastructure: A collective term for the hardware and software that supports a range of services.

Interoperability: The ability of two or more systems to work together effectively without human intervention.

MMC, multi-media memory cards: Devices containing memory chips designed to hold images, audio and video.

MPEG4 Camcorders: Digital video cameras that store images using the MPEG-4 data compression standard.

NCC: National Consumer Council.

NFC, Near-Field Communications: A standard for communication between devices separated by distances of up to 20 centimetres. NFC refers to a specific set of protocols which can be more broadly classed as RFID. NFC operates at 13.56 MHz and can work with either of two communicating devices being active or passive.

P2P, Peer to Peer computing: Networking between computers of equal status. Contrasted with Client-Server computing, where the relationship is asymmetric.

Phishing: Sending fake emails that purport to be from a legitimate organisation, with the intention of tricking the recipient into revealing private data, especially account numbers and passwords.

PKI, Public Key Infrastructure: The technology that supports the exchange and use of asymmetric (public key) cryptography.

Platform: In computing, 'platform' refers to the computer hardware and operating systems which allow software to run.

Privacy: See section 2.3.1 for a discussion of the concept of privacy.

Quantum Cryptography: The use of the quantum properties of entangled subatomic particles (such as the spin of photons) to convey secret information in a way that can only be read by the intended recipient.

RFID, Radio Frequency Identification: The use of small circuits that can receive and transmit radio signals and that are cheap enough and small enough to be widely attached to goods for tracking purposes. RFID is a generic term for a range of more specific protocols.

(Data) Shredding: the use of encryption, followed by destruction of the secret key. By shredding, data becomes permanently unreadable even if it has been archived somewhere.

SIM, Subscriber Identity Module: The small smart card that makes a portable telephone or similar device personal to a particular subscriber.

Stakeholders: In general, stakeholders are those who are affected by a given policy, and are increasingly involved in the making of policy that is relevant to them. They include both groups and individuals.

State/Government: The state is the structural organisation of the political community, with a territory and a people under a single government, and formal institutions of representation, legislation, law, authority and administration. Whilst governments are elected and change regularly, the state persists.

Surveillance: Monitoring individuals' locations, behaviour or other personal data.

Sandboxes: A facility within a computer system that allows untrusted programs to be executed safely because the sandbox prevents interference with the rest of the system. This can be extended to the general idea of testing out new systems in restricted environments - for example, trying out identity management technologies in the relative safety of a 'virtual' world (eg, the 'world' of a multi-player online game) before using them in the 'real' world.

Token: A token is a physical object that connects a virtual identity (the information that is held about a person on various databases, or is associated with their use of online services) to a real identity. The token is connected to the real person by a biometric or a pin which the person uses to prove their identity and to thereby pay for an item or access personalised services. The chip on a chip and pin card is a good example.

Trojan Horse: In the computer software context, a 'Trojan Horse' is a malicious program disguised as, or hidden within, a legitimate piece of software.

TPM, Trusted Platform Module: Trusted Platform Module (TPM) refers to a published specification detailing a microcontroller that can store secured information, and is also used as a general name for implementations of it. Implementations consist of chips that will be built onto a PC or laptop's motherboard during manufacturing. A Trusted Platform Module offers facilities for the secure generation of cryptographic keys.

USB, Universal Serial Bus: A standard for interconnecting computer peripherals.

VoIP, Voice over Internet Protocol: A technology to allow voice telephony over the Internet.

WiFi: The technology underlying wireless local area networks.

Wimax, worldwide interoperability for microwave access: A standard for technologies which provide wireless broadband access as an alternative to cable and DSL.

XML, Extensible Markup Language: A standard defined by the World Wide Web Consortium exchanging structured documents and data over the Internet. XML has far greater descriptive power than Hypertext Mark-up Language (HTML).

ZigBee: A standard for low-power, short-distance wireless communications. It is comparable to Bluetooth, but intended to be cheaper to implement.

4G/5G: Future wireless telecommunications.

10. Bibliography

Bartle, R. (2005) 'Virtual Money in Virtual Worlds' in proc. of *Digital Money Forum*, Consult Hyperion, London, March 2005

Birch, D. (2005) 'Retail Electronic Payments Security: Trends and Implications for Mobile' in proc. of *Mobile Payments*, Informa

Birch, D. (2004) 'Who Are You? A simple question with many answers' in proc. of *Security and Privacy*, Vanguard

Briggs, B. (2003) 'Voice Biometrics: Just a Whisper' in *Health Data Management*, 2nd August.

Castells, M. (2002) 'Privacy and Liberty in Cyberspace' in *The Internet Galaxy*. p. 168-187, OUP, Oxford

Coghlan, A., Randerson, J. (2005): 'How far should prints be trusted?', *New Scientist*, September 17th 2005

Council for Science and Technology (2005) *Better use of personal information: opportunities and risks*,

Deisman, W. (2003) CCTV: *Literature Review and Bibliography*, Research and Evaluation Branch, Community, Contract and Aboriginal Policing Services Directorate, Royal Canadian Mounted Police, Ottawa

Ditton, J (2000) 'Crime and the City. Public Attitudes towards Open-Street CCTV in Glasgow' *British Journal of Criminology*, Vol. 40, No. 4

Dunn, J. (2005) 'Israeli Police Uncover Massive, Trojan Horse-Based Industrial Spy Ring' in *Techworld*, 31st May

Foresight. (2006) *Infectious Diseases: Preparing for the Future*, Office of Science and Innovation, London

Gatehouse, J. (2005) 'You are exposed' in *Macleans*, 21st November

Gill, M. and Spriggs, A. (2005) 'Assessing the impact of CCTV' *Home Office Research Study 292*, Home Office Research, Development and Statistics Directorate

Guest, T. (2005) 'Lost in cyberspace' in *The Telegraph Magazine*, 12th March, p. 28-35

Hildebrandt, M. and Backhouse, J. (eds) (2005) 7.2 'Descriptive Analysis And Inventory Of Profiling Practices', *FIDIS Future of Identity in the Information Society Project*

Hempel, L. and Töpfer, E. (2003), *On the Threshold to Urban Panopticum. Objectives and Results of the "Urbaneye" Project on the Employment of CCTV in Europe*, Discussion paper Nr. 06/03, ZTG-Themenschwerpunkt: Lebensqualität durch soziotechnische Systeme

Kahan, D. M. (2003) 'The Logic of Reciprocity: Trust, Collective Action and Law', 102, *Michigan Law Review*

Lace, S. (ed.) (2005) *The Glass Consumer*, Policy Press

Lessig, L. (1999) *Code and other laws of cyberspace*, New York, Basic Books

Levi, M and Wall, D. S. (2004), 'Technologies, Security, and Privacy in the Post 9/11 European Information Society', *Journal of Law and Society* 31 (2)

Liberty Alliance Project (March 2004) Whitepaper: *Benefits of Federated Identity to Government*

Mantix (2005) 'Big Brother or Guardian Angel?', published by Mantix

Mishler, W. and Rose, R. (2001) 'What Are the Origins of Political Trust? Testing Institutional and Cultural Theories in Post-Communist Societies', Comparative Political Studies, 34, 1, 30-62.

Misztal, B. (1996) *Trust in Modern Societies*: *The Search for the Bases of Social Order*, Polity Press, Cambridge MA

Norris, C. and Armstrong, G. (1999a) *The Maximum Surveillance Society*: *The Rise of CCTV*, Oxford: Berg Publishers

Norris, C. (1999b) 'The suspicious eye', *Criminal Justice Matters*, Vol. 33, Autumn 1999 p. 10-11

Norris, C. and Armstrong, G. (1998): 'The Unforgiving Eye: CCTV Surveillance in Public Spaces', Centre for Criminology and Criminal Justice, Hull University

Norris, C., Moran, J., and Armstrong, G. (eds.) (1996): *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Aldgate.

O'Neill, O. (2002), *A Question of Trust, The BBC Reith Lectures 2002*, Cambridge University Press

Perl, M. (2003): 'It's Not Always About the Money: Why the State Identity Theft Laws Fail To Adequately Address Criminal Record Identity Theft', *Journal of Criminal Law and Criminology*, Fall 2003

Shadbolt, N., Berners-Lee, T. and Hall, W. (2006) The Semantic Web Revisited. *IEEE Intelligent Systems* 21(3) pp. 96-101.

The Surveillance Studies Network, for the Information Commissioner (2006): A Report on the Surveillance Society

Warren, M. E. (1999) *Democracy and Trust*, Cambridge University Press, Cambridge

Move over, Big Brother in *The Economist*. 373(8404): p. 26-28 (4th Dec. 2004)

11. Acknowledgements

Working Group:

Professor Nigel Gilbert FREng AcSS (Chair)
University of Surrey

Professor Anne Anderson OBE
University of Dundee

Dr James Backhouse
London School of Economics and Political Science

Mr David Birch
Consult Hyperion

Professor Brian Collins
Cranfield University

Professor William Dutton
Oxford Internet Institute, University of Oxford

Mr John Edwards
Herbert Smith

Dr Ian Forbes AcSS
Fig one consultancy

Professor Wendy Hall CBE FREng
University of Southampton

Professor Andy Hopper CBE FREng FRS
University of Cambridge

Professor Cliff Jones FREng
University of Newcastle

Dr Martyn Thomas CBE
Martyn Thomas Associates Ltd

Secretary to the group:

Dr Natasha McCarthy

A call for evidence was published in February 2006 and evidence was received from the British Computer Society, the National Consumer Council, Mantix, Dr Chris Pounder of *Data Protection and Privacy Practice*, and Michael Page from Fujitsu Services. The working group is extremely grateful for these helpful contributions.

12. References

1 See the following news story: http://news.bbc.co.uk/1/hi/england/2805399.stm

2 Bartle, R. (2005)

3 Birch, D. (2005)

4 Briggs, B. (2003)

5 See Guest, T. 'Lost in cyberspace' *The Telegraph Magazine*. p. 28-35, 12th Mar. 2005.

6 Some of the material in this section was published in *The Guardian* as 'The age of sousveillance', David Birch, 14th July 2005

7 *Move over, Big Brother in The Economist*. 373(8404): p. 26-28 (4th Dec. 2004).

8 Castells, M. (2002).

9 "The ICAO suggested that the key needed to access the data on the chips should be comprised of, in the following order, the passport number, the holder's date of birth and the passport expiry date, all of which are contained on the printed page of the passport on a 'machine readable zone'."From 'Cracked it!', *The Guardian*, November 17th 2006

10 See http://news.bbc.co.uk/1/hi/health/5233604.stm]

11 The European Parliament has issued a Directive (Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of personal information) which encourages public sector bodies to make the information that they hold available in electronic form. The Directive has certain exceptions; for instance, for information covered by intellectual property rights.

12 See Shadbolt, N., Berners-Lee, T. and Hall, W. (2006) for a description of the Semantic Web

13 UK Cabinet Office (2002). Identity Fraud: a Study, London.

14 See the following presentation from the Digital ID Forum hosted by Consult Hyperion, November 2006. http://www.digitalidforum.com/PubWebFiles/DigID/7_2006/presentations/John_Dale_Ann_Jacklin.pdf

15 Most of the information in this section is taken from the Data Protection Factsheet, published by the Information Commissioner's Office.

16 See http://www.ico.gov.uk/

17 The comments here were strongly informed by discussions at the Memories for Life colloquium, hosted by the M4L Network at the British Library on December 12th 2006; particularly Jonathan Zittrain's presentation 'Ubiquitous Data and the Madness of Crowds' and comments by Andrew Charlesworth.

18 It is important to note that, in its guidance on the use of surveillance cameras, the Information Commissioner's Office stipulates that CCTV cameras with sound recording facilities should not be used to record the conversations of members of the public. CCTV Code of Practice, Information Commissioner's Office, July 2000.

19 Ditton (2000). Since 'natural' forms of surveillance are preferred by the public, and since electronic surveillance will grow rather than reduce, the question is whether such systems can find ways to replicate and include what people regard as 'natural'. Greater reciprocity, including the ability to see what is being seen by cameras pointed at members of the public, may be a way of achieving this. This issue is discussed further in section 8.4.2.

20 See Norris, C., and Armstrong, G. (1999a) pp.10-11.

21 Norris, C.and Armstrong, G. (1998), p. 8.

22 See Gill, M. and Spriggs, A. (2005)

23 The Royal Academy of Engineering has issued a statement on Road User Charging, available here: http://www.raeng.org.uk/policy/reports/pdf/road_user_charge/road_user_charging.pdf . This statement offers suggestions for protecting the privacy of road users whilst implementing an effective system for charging for road use.

24 This concept was discussed by Jerry Fishenden of Microsoft at the Digital Identity Forum in November 2006, as part of a panel discussionon ID cards. The presentation for this panel discussion can be found here: http://www.digitalidforum.com/PubWebFiles/DigID/7_2006/presentations/Expert_Panel2.pdf

25 Professor Russell Cowburn's presentation on this technology at the Digital Identity Forum, November 2006, can be found here: http://www.digitalidforum.com/PubWebFiles/DigID/7_2006/presentations/Russell_Cowburn.pdf

26 The Reason project, carried out by Kingston University, University of Reading and University College London, is one example of research in this area.

27 See Misztal, B., (1996), pp.12-32.

28 Mishler and Rose (2001), p 30-62.

29 Warren, M. E., (1999), p 349 (his italics).

30 Council for Science and Technology, November 2005

31 http://www.ico.gov.uk/eventual.aspx See also section 5.2 for a discussion of the role of the information commissioner.

32 M. Hildebrandt and J. Backhouse (eds) (2005), p.53

33 Levi, M and Wall, D.S., (2004)

34 Lessig, L. (1999) p. 154.

35 http://www.apha.org/codeofethics/ethics.htm

The Royal Academy of Engineering

As Britain's national academy for engineering, we bring together the country's most eminent engineers from all disciplines to promote excellence in the science, art and practice of engineering. Our strategic priorities are to enhance the UK's engineering capabilities, to celebrate excellence and inspire the next generation, and to lead debate by guiding informed thinking and influencing public policy.

The Academy's work programmes are driven by three strategic priorities, each of which provides a key contribution to a strong and vibrant engineering sector and to the health and wealth of society.

Enhancing national capabilities

As a priority, we encourage, support and facilitate links between academia and industry. Through targeted national and international programmes, we enhance – and reflect abroad – the UK's performance in the application of science, technology transfer, and the promotion and exploitation of innovation. We support high quality engineering research, encourage an interdisciplinary ethos, facilitate international exchange and provide a means of determining and disseminating best practice. In particular, our activities focus on complex and multidisciplinary areas of rapid development.

Recognising excellence and inspiring the next generation

Excellence breeds excellence. We celebrate engineering excellence and use it to inspire, support and challenge tomorrow's engineering leaders. We focus our initiatives to develop excellence and, through creative and collaborative activity, we demonstrate to the young, and those who influence them, the relevance of engineering to society.

Leading debate

Using the leadership and expertise of our Fellowship, we guide informed thinking, influence public policy making, provide a forum for the mutual exchange of ideas, and pursue effective engagement with society on matters within our competence. The Academy advocates progressive, forward-looking solutions based on impartial advice and quality foundations, and works to enhance appreciation of the positive role of engineering and its contribution to the economic strength of the nation.

The Royal Academy of Engineering promotes excellence in the science, art and practice of engineering.

Registered charity number 293074

The Royal Academy of Engineering
29 Great Peter Street, London, SW1P 3LW
Tel: 020 7227 0500 Fax: 020 7233 0054
www.raeng.org.uk