Privacy, Anonymity and the Internet

Ian Lloyd*

Readers are reminded that this work is protected by copyright. While they are free to use the ideas expressed in it, they may not copy, distribute or publish the work or part of it, in any form, printed, electronic or otherwise, except for reasonable quoting, clearly indicating the source. Readers are permitted to make copies, electronically or printed, for personal and classroom use.

Introduction

Scott McNealy, chairman of SUN, one of the leading Internet companies, famously commented of the online world and its likely development. ‘You have zero privacy already. Get over it.’ We might compare this with the sentiment expressed in a well known cartoon created by Peter Steiner and originally published in the ‘New Yorker’ magazine.

How can a person have zero privacy and yet operate in an environment where no-one knows who or what he, she or it is? Trying to reconcile seemingly incompatible expectations is nothing new for the law and it is suggested that both views have elements of validity. In this particular context, the approaches highlight, it is submitted, a crucial distinction between
notions of privacy and of anonymity. The legal dimension of the latter concept has hitherto been relatively little explored yet, it is suggested, may furnish a sturdier basis for the protection of individual rights and freedoms for the majority of the population than what is sometimes stigmatised as, perhaps correctly, more elitist concept of privacy.

The relationship between privacy and anonymity is complex perhaps akin to that between conjoined siblings. Both share common, and frequently vital, organs but also have capacity for independent action. Robert Doisneau’s iconic photograph of a couple kissing in a Parisian street provides an excellent example of an apparently private and spontaneous moment being brought into the public arena but with the anonymity of the participants preserved – for a while. In reality the photograph was staged with the photographer later commenting that "I would have never dared to photograph people like that. Lovers kissing in the street, those couples are rarely legitimate."¹

Although the concept of privacy is extremely broad in its scope, what might be regarded as the classical aspect of the right is the wish to prevent others knowing both who we are and what we are doing. For the vast majority of the population, unless we are enjoying or enduring a Warholian fifteen minutes of fame, our actions, at least when linked to our identity are of little concern to anyone other than close family and friends. I cannot expect to kiss my wife in a public place without others seeing us, but unless behaviour is particularly outrageous, nobody will really notice or care who we are. Inevitably, almost everyone has to live large parts of our life in a public environment and here notions of privacy can have

* Professor of Information Technology Law, University of Strathclyde.
limited impact although the ongoing case of Murray v. Big Pictures\(^2\) provides an interesting example of the complex relationship between privacy and public spaces. Here the Court of Appeal held (over-ruling the High Court which dismissed proceedings on the basis that the claimant had not established a case to answer) that an action might lie for breach of Article 8 rights in a case where a photographer surreptitiously and using a long-lensed camera, deliberately photographed the famous novelist JK Rowling and her husband and infant son walking along a public street with a view to selling these images for publication. The scenario is an interesting one and one which the emergence of web sites such as Facebook and Youtube may exacerbate in that they give anyone with a camera a possible publication outlet.\(^3\) As with many aspects, what the Internet (and computer technology more generally) does is to offer expanded possibilities for the loss of anonymity. From the chance possibility that an acquaintance may be passing in real time, we move to a situation when a moment in time is captured, if not for ever, at least for an indeterminate length of time and the prospect of anonymity recedes.

Privacy, Anonymity and the Internet

Not too many years ago one of the first tasks for anyone arriving at a holiday destination was to send postcards to friends and family expressing (more or less sincerely) the wish that ‘you were here’. Today, the first action for many is to seek out the local Internet café or make use of the texting facility on a mobile phone.

Postcards are known to be a highly insecure form of communication given that their contents can easily be read by any curious member of the postal service or indeed by any other members of the household to which they are addressed. Probably for this reason, it would be an unwise person who allowed their contents to rise above the banal. Similar problems were associated with the earliest form of electronic communication – the electric telegraph – and led to a significant market in code books allowing users to conceal their messages from prying eyes. One of the pitfalls of modern emails, as many can testify, is that it is easy to compose a message in the belief that it will be seen only by the intended recipient only to discover that the technology produces different effects. Examples are plentiful of ‘reply to all’ functions being used when the intention was to respond only to an individual sender.\(^4\) Beyond such accidents it is the case that every action in the world of electronic communications leaves semi-permanent traces. Any electronic communication has to make its way through the equipment of a range of intermediaries each of which will collect and retain significant items of data. The European Union’s Data Retention Directive,\(^5\) which was adopted in the aftermath of the Madrid and London bombings, requires a range of electronic service providers to retain a wide range of items of data for considerable periods of time. For telephone calls data has to be retained relating to the name and recorded address of the calling and called parties. For mobile phones the data extends to details about the location of both calling and called parties as well as to the particular phones used. Effectively, when we carry our mobile, we disclose extensive details about our movements. The Directive provides also for the retention of

\(^2\) [2008] EWCA Civ 446.
\(^3\) Camcorder devices are now being marketed which are specifically designed to facilitate uploading images to sites such as YouTube or MySpace.
\(^4\) As an example of the manner in which emails can circulate, it took the author two Google searches and one intermediate link to find the full text of one such email. Total time less than 30 seconds to find that what was apparently meant as a personal email is available to any Internet user.
extensive data about Internet access and usage. These provisions have not yet been implemented in the United Kingdom although reports of the contents of a Communications Bill likely to be introduced into the next Parliamentary session suggest this will not be the case for much longer.

It is a feature of the data retention Directive that, on grounds of protection of individual privacy, its provisions do not extend to the contents of telephone calls, text or email messages6 but in many respects this is small comfort. Most telephone conversations are rather mundane and it would perhaps be a foolish terrorist or criminal who would discuss plans openly. The topic of encryption has many aspects but simple techniques may be just as effective as the most sophisticated technological encryption software. A phrase such as ‘Can you deliver the parcel on September 15?’ might be a routine message to a delivery firm or an instruction to detonate a bomb. Although national security agencies reportedly maintain massive automated capabilities to intercept communications traffic, for example the Echelon system operated by Australia, Canada, New Zealand, the United Kingdom and, principally, the United States, these can have limited effectiveness against techniques such as that described above.7 Indeed it has been suggested that only a naive terrorist would use a technical system of encryption at least for transmitting messages.8 Relatively few email messages are encrypted and the presence of such a message might attract more attention than a seemingly innocuous phrase.

Whilst targeted and covert interception of communications undoubtedly remains a valuable tool for law enforcement agencies, much activity focuses not on the contents of communications but on the issue what communications device has contacted another device. It is common practice for law enforcement agencies to try to build up a picture of the range of contacts relating to a particular suspect or group of suspects. This has perhaps been taken to its furthest limits in the United States where the Patriot Act confers extensive rights upon law enforcement agencies to seek data from communications providers. It has been reported that it is common for requests to be made looking for data relating to two generations of calls made and received, i.e.

---

6 Article 1(2).
7 Recent publicity concerning the monitoring by British Intelligence of mobile phone calls made by suspected Irish Republican terrorists makes reference to terms such as ‘the brick’s in the wall’ as indicating, albeit with the benefit of tragic hindsight, that a bomb had been placed and was primed to explode. See e.g. http://news.bbc.co.uk/1/hi/uk/7613407.stm.
8 Matters may well be different in respect of data held on a computer and numerous case have been reported of investigations of suspected crimes being hindered by the fact that data is held in encrypted format. The Regulation of Investigatory Powers Act 2000 establishes a new offence of refusing to hand over to investigators details of encryption keys but the penalties are relatively minor and the offence does not appear to have been tested against a defence that the details have been ‘forgotten’.
This is of course, a very simplified diagram and B or C could well be a large organisation making and receiving thousands of calls a day. At a ‘mere’ two generations of calls we can soon run into massive numbers. In a more general context, it has been estimated that anyone in the world is within 6 levels of relationship with any other person, i.e. a message from any person to any other person with only the most rudimentary identifying details needs to be passed through no more than 6 intermediaries to reach its destination. The validity of such calculations has been questioned but there is no doubt that millions of people may have their communication records included in the course of any enquiries relating to a very few points of initial interest. In many ways the figures are mind boggling and it may fairly be stated that but for the ever increasing processing power of computers, surveillance on such a scale would be well nigh impossible in a democratic society.

**No Anonymity on the Internet?**

It is a rare form of activity today that cannot, and in many, many cases is not, carried out within an electronic environment. One of the major policy initiatives of the 1997 Labour government was the determination to make all forms of government service available electronically. To an extent, greater perhaps than with many other government targets this has been successful and much current attention is being directed at what is generally referred to as data sharing. Historically, and frequently disastrously, different Government departments have commissioned their own bespoke software systems. Assuming they worked, these would generally be incompatible with systems commissioned by other departments. The current trend is for more use to be made of standard software packages and to facilitate data sharing across departments. This can have positive aspects from an individual’s standpoint. One of the frustrating aspects of dealing with different government departments has traditionally
been the need to give the same items of information over and over again. In the context of one
review of government practice, the example was put forward of

   a family who had a total of 44 contacts with government over 180 days trying to make
   the necessary arrangements after a family member died in a road accident.9

Allowing departments to share data, it was suggested would simplify the task of individuals in
such a situation. Put in terms of minimising the strains on grieving relatives it is difficult to
object to data sharing, but this is perhaps a case of the exception becoming the rule. It is one
of the basic precepts of data protection law that data supplied for one purpose should not be
used for another purpose. Recent years have seen extensive actions by Government in relation
to the practice of data sharing. The Serious Crimes Act of 2007 authorises very extensive
transfers of personal data to specified anti-fraud organisations, The Act also makes provision
for extensive data matching exercises to be conducted by the Audit Commission.

For many, typically but by no means exclusively, of a younger age, online life is becoming an
integral component of their personal life. Social networking sites have acquired massive
penetration. It is a rare media event today that does not seek to access and make us of
information presented on social networking sites with references to postings on such sites. It
is also relatively common for employers or potential employers to conduct searches seeking
information about individual’s social networking activities. Accounts (and photographs) of
alcohol fuelled nights out may sit uneasily alongside a carefully crafted CV and soberly
dressed interview candidate. Given that the decision to participate in a social networking site
is entirely optional and the dissemination options and possibilities made as clear as is ever the
case on the Internet, it is difficult to argue that such activities constitute any form of
infringement of privacy except perhaps on the basis that individuals may well be unaware of
the fact that their spontaneous actions may leave permanent trails in cyberspace. Perhaps
rather than talking in terms of privacy, the message should be that by making information
available in such a public forum and linking it to a name, individuals are giving up their
anonymity. The Information Commissioner's office has produced guidance aimed specifically
at young persons concerning the risks associated with such on-line activities. Much the same
could be said of a wide range of on-line activities. Millions of people have signed up for store
loyalty cards either unaware or uncaring that they are giving away information identifying
them and their purchases. Perhaps most potentially intrusive is the Nectar card which links
across a range of suppliers both on the High Street and in the field of on-line retailing where
more than 200 outlets, including such well known names as Amazon and E-Bay, participate
in the scheme. Although it is claimed that only limited data is collated centrally such coverage
means that virtually every purchase an individual makes could be linked by a single
identifying number.

Every action on line leaves traces, often more extensive than is likely to be the case in the real
world. A visit to an on-line bookstore, for example might be anallogised to entering a high
street store only to have an employee watching and recording every book picked up and
examined.10 The use of cookies allows continuing linkage between a site and a particular
computer. Surveillance devices in the workplace allow employers to monitor the activities
and efficiency of individuals. At a potentially extreme level, the United States Patent Office
have published an application from Microsoft for a system which will monitor an employee’s
heart rate, body temperature, blood pressure and movement. It is claimed that the system will

---

9 http://www.number10.gov.uk/Page10759.
10 Such tactics (carried our surreptitiously) are sometimes practised by high street stores for research purposes.
automatically detect signs of stress or illness. At a rather simpler but perhaps more threatening level, evidence is mounting regarding the scale of surveillance currently conducted by employers regarding the on-line activities of employees. One recent case concerns the dismissal by Marks and Spencer of an employee who allegedly leaked details of plans to reduce redundancy payments. His representatives have suggested that:

the company monitored every single keystroke made by staff on computers and kept the information for six years. She also claimed that supposedly anonymous replies to staff surveys were tracked.\textsuperscript{11}

It is only fair to note than the company have denied these claims. At a technical level, however, there is little doubt that such behaviour would be feasible. Most of us use Internet search engines on a daily basis. Indeed the term to ‘Google’ has become a widely accepted verb. There has been ongoing debate between Google and European data protection authorities concerning the length of time for which data relating to searches is retained in a format which permits identification of at least the computer from which the request originated. Until 2007, such data was retained for 2 years before being anonymised. Following discussions it has recently been announced that data will be rendered anonymous after nine months, a period which is still longer than the 6 months sought by the European Union’s Article 29 Working Party on Data Protection.\textsuperscript{12} Extensive records will also be maintained by Internet Service Providers (a term which may well include employers.)

Considerable publicity has recently been given to proposals to introduce a new system for targeting on line adverts to users dependent upon their browsing history. Some of the United Kingdom’s major ISPs, including BT and Virgin have signed up to a system known as Webwise developed by a company called Phorm although none have yet implemented the system. In part concerns relate to Phorm’s previous business activities which may be described as operating on the boundary of acceptable conduct in relation to the use of spy ware software- a practice which involves the use of cookies to monitor the operations carried out on a computer. If the scheme is what the developers claim, it might be seen as a rare case of a poacher turning gamekeeper

Effectively the system notes the URLs of the web sites visited by a user and then searches the sites compiling a list of key words. This can then be linked to the user in order to build up a profile which could be used by to target marketing. An advertiser specialising in offering travel services might, for example, want to target marketing at web users who have previously visited sites selling airline or train tickets.

At first sight the proposal seems a horrifying intrusion on privacy and indeed many commentators are of this opinion. Perhaps not surprisingly the developers of the system take a different view with their web site proclaiming that Webwise

revolutionises online advertising by setting a new, higher standard on privacy and anonymity. Designed with both user privacy and targeting effectiveness as equal priorities, the result is a technology that, for the first time, ISPs, their Internet user customers, and all participants in the online advertising ecosystem can trust.

Key to the system is the claim that it allocates a random number to each individual and that this is the only form of data which it keeps on the individual. A user will have a contract with an ISP for provision of Internet access. The ISP in turn enters into a contract with Webwise. The first time the user accesses the Internet after the Webwise contract is implemented a

\textsuperscript{11} http://www.guardian.co.uk/business/2008/sep/08/marksspencer.tradeunions.

\textsuperscript{12} Opinion 1/2008 on data protection issues related to search engines.
randomly generated number will be allocated and linked to a cookie placed on the user’s computer.

The Webwise hardware and software acts as a filter between the ISP’s equipment and web sites. When the user types a URL in his or her browser the Webwise system categorises the relevant web site, in a manner not too dissimilar to that used by traditional search engines, albeit perhaps more limited in scope. A visit to, for example, an airline booking site might be referenced against ‘airline’ ‘ticketing’ ‘reservations’ or similar terms. Over time, the system will build up a more and more detailed profile of the browsing habits of the user and this could be made available to advertisers so that the messages which appear on the user’s screen are tailored to the browsing habits identified. A user who regularly visits web sites connected with travel might receive adverts relating to offers on flights or hotel accommodation. A further feature claimed for the system is that it will maintain a list of sites associated with fraudulent activity and cause a warning to be displayed if a user attempts to navigate to such a site.

It is stressed in publicity that users can opt out from the system either on a permanent or a temporary basis. A number of ISPs have indicated that they will offer the system on an ‘opt in’ basis. It does not appear clear, however, how the opt-out system will work at a technical level and in particular whether their traffic will still be routed through the Webwise system.

Some support for the system has come from sources normally closely associated with unconditional support for individual privacy. The basis for the approval appears to lie in an acceptance that safeguards are such that there is a high degree of assurance that anonymity will be preserved. Others are less convinced and the issue of the systems compliance with the Data Protection Act is being considered by the Information Commissioner. Concerns have also been raised that the practice may contravene the provisions of the Regulation of Investigatory Powers Act 2000, not through recording information about individuals (as some form of consent will have been obtained for this) but in the subsequent trawling of the web sites visited to identify the key words used.

As in so many cases concerned with Internet based activities, the key issue is one of trust. A Privacy Examination report was commissioned by the developers of Webwise from the well established consultancy firm Ernst and Young. This expressed the view that the system complied with the developer’s claims regarding privacy protection but with the rider that:

Because of inherent limitations in control, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the Service or controls, or a deterioration in the degree of effectiveness of the controls.13

With continuing increases in processing power, it is becoming more and more difficult to be assured of anonymity. In 2006 AOL placed on the Internet data relating to search requests made by millions of its subscribers. The assumption was that as no names or other identifiers such as the IP address of the computer used to conduct a search, the individuals concerned would remain anonymous. Instead each user was allocated a randomly generated number. Although no names were published, in at least some cases it proved possible to identify

---

individuals following analysis of their search history. One case concerned a user allocated the identifying number 4417749. As was reported:

No.4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

Search by search, click by click, the identity of AOL user No.4417749 became easier to discern. There are queries for several people with the last name Arnold, for "landscapers in Lilburn," Georgia, and for "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her over the phone.14

The case may well be an isolated one, but there is no doubt that the issue of preserving anonymity is assuming increasing importance in the context of activities such as national censuses. The possibility to compare data across a diverse range of sources undoubtedly challenges, at least in a small number of cases, the anonymity previously promised by law in the conduct of censuses.

Turning to the Dog

As the name suggests, social networking involves individuals in making contact with each other. Typically, we live our lives in a series of compartments and value the ability to at least influence the range of dissemination of personal information. In many respects we are all actors playing a range of different roles in our lives, son, brother, husband, father, teacher, friend, colleague, acquaintance. The list could go on, but in each relationship we both actively present some aspects of our character and passively attempt to keep others secret. Breaking down the compartmental walls may have consequences which cannot be predicted but our increasing involvement in cyberspaces raises many new issues.

At a positive level, electronic communications allow individuals to communicate in a way that can minimise the impact of any disability from which they may suffer. In a very real sense the Internet may promote goals of social inclusion. Actions may, of course be motivated by more malign considerations with the classic example being that of paedophiles who present a fictitious personality in the attempt to persuade children to agree to face to face meetings. Such tactics and techniques are not novel. In the mid 1990’s a much publicised case concerned a 32 year old man passing himself off as a 17 year old in order to attend school and obtain sufficient exam passes to be offered a place at medical school. This may have been a somewhat extreme case and there is no doubt that the Internet allows greater flexibility for users to choose the personality that they want to present to others. Instances have been reported of males presenting themselves (apparently very convincingly) as females in Internet fora. In a real sense there is privacy in electronic communications because we have great control over the image we present. Anonymity is a different matter. If an individual accesses the Internet from an Internet café in order to browse web sites, and pays cash for the privilege, there is the prospect of a good degree of anonymity. In almost every other situation our Internet usage will leave trails which can be traced to a particular computer and, at least by inference, from there to a particular individual. Such a prospect has come as a less than

welcome surprise to a considerable number of Internet users who have acted in the belief that they enjoyed anonymity or at least pseudonimity in the sense that their postings would have appeared under a chosen pseudonym rather than a real name.

Over the last few years, there has been increasing applications to the courts in the course of legal proceedings for the making of, so called, Norwich Pharmacal orders within an Internet context. These derive from the decision of the House of Lords in the case of *Norwich Pharmacal Co v. Commissioners of Customs and Excise*. This established the doctrine that a party to potential litigation could seek disclosure of information held by a third party which might identify others against whom a claim could be made if three conditions could be satisfied:

- A wrong had arguably been committed against the claimant by a third party whose identity was not known to the claimant;
- Identification of the third party must be necessary to allow proceedings to be instituted;
- The party against whom the action is brought must be in a position to identify the wrongdoer.

In a typical case, an ISP will be asked to identify users who may have committed copyright infringement or have engaged in conduct which is considered to be defamatory of a claimant. An agreed statement read out in court in the context of recent litigation describes well the issues and situations which may arise in such cases. The defendant, it was admitted, was

…responsible for the publication of a seriously defamatory, abusive and scurrilous anonymous website at www.dadsplace.co.uk, with an associated chat forum, newsletter and leaflets which have been called the "Dads Place Publications". Over a period of two years from April 2004 to about mid-July 2006, from behind their cloak of anonymity, Dads Place used their publications and in particular the Website to conduct a malicious, unpleasant and relentless campaign of libel and harassment …

Those responsible for the publication of the Dads Place Publications took careful steps to conceal their identities and it took many months of painstaking investigation to identify just some of those responsible for Dads Place and bring proceedings against them.

More authoritative judicial consideration was given to these issues in the case of *Sheffield Wednesday Football Club Ltd and Others v. Hargreaves*. The claimants here were parties connected with the management of less than triumphant English football club. The defendant operated a supporters’ web site which allowed for the posting of comments on matters concerned with the club. A number of comments (published pseudonymously) were considered to have been defamatory of the claimants who brought an action before the courts seeking an order that the web site owner identify the individuals responsible (users were required to register with the site owner before being allowed to post comments).

As is common in discussion groups devoted to participants’ enthusiasms, many of the postings complained of, although technically defamatory, were insulting rather than damaging. The judge described several of the comments as being “trivial” or amounting to no more than “saloon-bar moaning about the way in which the club is managed.” In these cases, the court declined to order the identification of the posters. In other instances, complaints

15 *Norwich Pharmacal Co v Commissioner of Customs and Excise* [1973] 2 AllER 943.
16 *Sheffield Wednesday Football Club Ltd and Others v Hargreaves* [2007] EWHC (QB) 2375.
centred on allegations of financial impropriety and in these cases it was held that disclosure should be made.

As in so many respects, the challenge is to strike a balance between competing claims and the concept of pseudonymity, perhaps epitomised by the situation in Sheffield Wednesday may have a role to play in that actions may take under a shield of anonymity which may be withdrawn if there is evidence that it is being misused.

From Knowledge to Information, from Privacy to Anonymity

Especially as we move from village or close family communities to the more anonymous and impersonal lifestyles associated with much of modern life, traditional notions of privacy are perhaps of limited relevance to most persons. It is often a cause for concern that modern life confers too much privacy, to the extent that the weak vulnerable can suffer in isolation. The right to be left alone is surely of limited interest to the frail invalid who has little or no human contact for months at a time. Shopping in a hypermarket – even more shopping on line – involves minimal genuine human contact. In the Middle Ages the philosopher Francis Bacon referred to the fact that ‘knowledge is power’. Today it is commonplace to assert that ‘information is power’ and to recite the mantra that we live in an ‘information society’. The change in semantics is reflective of a massive change in society. Knowledge is essentially a human commodity with all the flaws and failings associated with imperfect beings. In the twentieth century a popular BBC comedy show, ‘Open All Hours’ featured Ronnie Barker as a small shop keeper in a stereotypical northern England close knit community. A running theme in the show concerned his efforts, invariably successful, to use his intimate knowledge of his regular customers to persuade them to purchase the goods he wished to sell rather than those which they had originally intended to buy. Today, of course, loyalty card data and analysis of transaction records allow stores to target marketing based on customer’s known buying habits. The effect may be the same but there will be little or no human knowledge of the particular individuals. Beyond use of data for marketing purposes, examples have also been reported of the use of data in connection with criminal investigations. In one case a magistrate was convicted of theft when he found and kept a Rolex watch in a supermarket. Critical evidence for the prosecution came from his loyalty card records which placed him in the supermarket at the same time as the watch was lost by its rightful owner. Illustrating the durability of such records, the facts only came to light more than 2 years after the event. The then Home Secretary David Blunkett sparked off considerable debate several years ago when in making a defence of the government’s proposals to introduce ID cards he suggested that individuals had more to fear from supermarket loyalty cards.

The increasing reliance on information as the basis for decisions and actions affecting individuals raises a large number of issues. In some respects and for some people the change may be welcomed. An application for a loan is unlikely to be influenced by any form of personal prejudice or animosity which the lender may feel against the applicant. The decision will almost certainly be taken on the basis of objective information recorded on a computer

---

17 For a report on the case see http://www.timesonline.co.uk/tol/news/uk/article507375.ece.
18 In an employment case discussed further below it has been suggested that Marks and Spencer have retained data relating to customers from 1986. A company spokesperson was quoted as saying that “The company was not able to answer a further allegation … that M&S kept data on its store card customers dating back to 1986. The spokeswoman said the company did keep data on customers but could not say how far back records were kept.
19 See http://news.bbc.co.uk/1/hi/uk/4020023.stm.
system (or on the even more impersonal system of credit scoring). Problems may, of course arise, if the information is inaccurate or if the applicant does not fit some model of an acceptable credit risk. A further factor associated with the use of computer networks is the extent to which information can be collated across a range of applications to develop detailed personal profiles.

Whilst ‘ordinary’ individuals may be unlikely to be the subject of direct and individually targeted surveillance, every action we take gives out some information about us. The term data surveillance (sometimes dataveillance) is commonly used to describe the situation whereby the information generated through our actions is collected and processed. With the ability to digitise any form of information, boundaries between the various forms of surveillance are disappearing with the application of information technology linking surveillance techniques into a near seamless web of surveillance. Much is written today about the number of CCTV cameras which populate the streets of the United Kingdom. By responsible estimates, there is one camera for every 14 people in the country and the average city dweller can expect to be captured on camera around 300 times a day. Traditionally, CCTV systems have relied upon images being viewed and assessed by human operators. In at least some instances this is no longer the case. A nationwide system of Automatic Number Plate Recognition cameras is being installed on the United Kingdom’s roads and is scheduled for completion in 2008 by which time about 50 million number plates will be recorded each day. The cameras will capture images of car number plates and compare these with records maintained by the Driving and Vehicle Licencing Agency and motor insurance companies to identify vehicles which are not taxed or insured. The system will also link with police data bases to flag the appearance of any vehicle recorded as being of interest to the police.

Even in the physical environment, trials are being conducted with image recognition systems linked to CCTV cameras which can monitor the movements of specific individuals. One of the most extensive systems has been installed in the London Borough of Newham. Here it has been reported that images from 150 cameras are compared:

… with a database of known criminals stored on computer at the council’s headquarters. Information is then passed to police.

The markers say the system is sophisticated enough to take into account light conditions, whether the suspect is wearing glasses, makeup or earrings, the expression and even the ageing process.

Growing a beard or trying some other disguise will apparently not fool the camera because it can see through it.

If the system, known as Mandrake, recognises a crook, it sounds the alarm and displays a code number. A council operator, who never knows the identity of the suspect, then phones police, who have their own screens.

Images of around 60–100 convicted criminals are maintained on the system, which claims an accuracy rate of around 75%. The downside, of course, is that 25% of innocent people will be viewed with suspicion because of a false identification. In a more recent development it has been reported that:

A new CCTV system developed by ‘Agent Vi’ is being installed in some of the UK’s busiest stations, including Clapham Junction and Paddington Station.

The system uses advanced hi-tech monitoring technology to judge behaviour and it is expected that twenty percent all CCTV cameras in the UK will be connected to the system within the next three years.

The technology has been on trial at Liverpool Street station since 2003.

One of the main excuses being given for the use of these cameras is their promise to act as a deterrent against terrorism and to reduce vandalism, by detecting usual behaviour. The technology known as “Video Analytics” will also recognize how a train should look and then react by notifying authorities if the appearance changes.

There is no doubt that the world we inhabit today is changing with considerable speed. As well as being a commodity in its own right, data is the motor and fuel which drives the information society. A database with no data is a poor creature indeed and with the development of more and more sophisticated search engine technologies, the value of a database lies increasingly in the amount of data held rather than the thought which lies behind the selection and organisation of material. One of the aspects of recent government data losses which has surprised many people has been the amount of data which can be held on very simple storage devices. Details of some 30 million individuals involved with child benefits fitted onto 2 CDs. In a more recent case, details of almost 100,000 prisoners and prolific offenders was held on a memory stick. A simple memory stick costing perhaps no more than £1 is capable of holding the equivalent of 1,000 large books and only slightly more expensive devices could multiply that figure many times over. The child benefit case illustrates a particular danger arising from the effective removal of space constraints for data storage. It has become easier to keep data indefinitely than to engage in electronic spring cleaning and easier to copy all the data held rather than just those elements which are needed for a particular purpose.

Examples of thickening information threads and trails are legion. Barely 10 years ago, the only records compiled by United Kingdom telephone companies regarding telephone usage concerned the number of units (an amalgam of the time of day when a call is made, its duration and its identification as local, long distance or international). Today, it is near universal practice to present users with itemised bills. These may provide considerable assistance to the person (or company) responsible for paying the bill in monitoring and controlling usage but does also provide useful marketing information to the service provider as well as raising issues concerning the privacy of other persons who might make use of the facility. With mobile phones, even more data is recorded with location data enabling the movements of the phone to be tracked with ever greater precision. Much publicity has

---

24 The efficiency of the system has been challenged with ‘The Guardian’ claiming that the system had never identified a suspected individual. See http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html.
recently surrounded the arrest of a key suspect in the July bombings in London following the tracking of his movements from London to Rome by means of signals from his mobile phone.26

Conclusions

In recent years, the United Kingdom’s Information Commissioner has warned repeatedly of the danger that the country is ‘sleep walking into a surveillance society’. As indicated throughout this paper, technology is facilitating the gathering and retention of items of data which would previously have passed either unnoticed or been retained for a short period of time. Developments in networking and processing technologies enable the exchange of data across previously insurmountable barriers or in ways which would not have been practically feasible. At a very simple level, we might take the example of the telephone directory. A human faced with a telephone number and a directory could conceivably track down a name associated with the number but as the directory is indexed by reference to name the task would be a substantial one. Transfer directories to electronic format and the matter becomes relatively trivial.

Technological genies have always proved very resistant to being reinserted into bottles. We cannot reinvent history and the current reality is that significant amounts of data about our lives is being recorded, processed and used in ways which we may not know about. It is tempting to add the phrase ‘and cannot control’ to the previous sentence but this would be wrong. If the establishment of a surveillance society was inescapable, the words of the Information Commissioner would be futile. We do have choices although the practical effectiveness of these is dependent upon a more robust attitude towards the importance of anonymity on the part of law makers. It is tempting to stigmatise those who sign up to supermarket loyalty schemes as willingly selling their anonymity for a hypothetical can of beans in the form of money off vouchers. Matters become more serious with developments such as the proposed system of identity cards. Here there seem to be attempts by Government to link acquisition of the card to other forms of identifier such as a passport. The Identity and Passport Service’s website indicates that:

until 1 January 2010, people will be given an option to choose not to be issued with an ID card when they receive their passport, although their details will be entered on the National Identity Register (NIR). 27

It appears that from 2010, individuals may have to choose between foreign travel and declining to obtain a ‘voluntary’ identity card.

We can all be identified in myriad ways and in some respects that serves to at least limit the extent to which our anonymity might be compromised. Widespread use of a single identifier poses obvious dangers in terms of the ability to link data from a disparate range of sources.

It is important not to lose sight of the benefits which information technology generally and the Internet in particular has brought. Massive amounts of information are made available to everyone which previously would have been the preserve of a select few. Search technology, epitomised by the new verb ‘to Google’ has become an established feature of many person’s business and personal lives. E-commerce has brought about significant reductions in the cost of many items and frequent travellers will not mourn the disappearance of airline check in

queues (although in most cases delays have simply moved to other aspects of the airport experience). In many senses we do enjoy more privacy in the online environment than we do in the real world but what we do lack in almost every instance is anonymity. In some respects the dangers arising are greater. Kafka’s ‘The Trial’ expressed graphically the torments faced by a person faced with unspecified charges brought by people he did not know. What we may face tomorrow is almost a mirror image. We might be denied medical treatment when an analysis of our purchases indicates that we buy cigarettes. Because the ‘watchers’ do not know us, it may be difficult to explain that the purchases are for someone else – or made by another person who in an act of misguided kindness we allowed access to our credit card or our computer. To reverse our opening cartoon, if analysis of our behaviour suggests that we are a dog, we can expect to be treated like one.

It is virtually impossible to participate in modern society and demand complete anonymity any more than we can seek absolute privacy. What does need to be considered more carefully is the nature and extent of the consequences that may follow from a substantial diminution to our right and ability to conduct our affairs under conditions of anonymity. Silly, thoughtless and unkind actions are as much a part of the human condition as more admired qualities. If people cannot commit small sins, they may more easily be tempted to attempt more serious offences. We perhaps interfere with genetics at our peril.

Technology has a major part to play in law enforcement but it should not operate in isolation and a major concern about current United Kingdom policy is that policy changes are being introduced in an ad hoc and barely considered manner. A prime example, perhaps, is the DNA database maintained by police authorities. Already the largest of its kind in the world, it operates without any specific statutory authority or parliamentary oversight. Its existence marks a significant change in the nature of much policing activity. From seeking to identify an individual criminal the question today is often whose DNA profile matches material obtained at the scene of a crime?

But what is the solution? All the evidence is to the effect that the young and members of certain ethnic minorities are disproportionately represented on the database. Should we seek to include everyone? Just as privacy is sometimes considered to be an elitist concept favouring the rich and powerful and providing little benefit to the average person, so anonymity could be seen as excluding vulnerable minorities. Calls have been made from some eminent people, including senior judges, for everyone’s details to be included in the database. It is tempting to draw an analogy with fingerprint technology in the 19th century but the reality is that storage and processing capabilities at that time would have made a system of universal fingerprinting difficult if not completely impossible. Today at the technical level, universal DNA profiling is a simple task. If the political decision were to be taken, universal coverage would be a relatively simply technical matter.

What is needed, however, is a greater sense of trust and transparency. In 2000, the United Kingdom Parliament passed the Regulation of Investigatory Powers Act. Promoted at the time as a measure to update the law relating to surveillance to better tackle serious crime, recent evidence suggests that powers have been used, albeit in a small minority of cases, against suspected instances of dog fouling and littering. Certainly not commendable conduct but not, perhaps, justifying intrusive surveillance and providing an illustration of the phenomenon of ‘function creep’ whereby the boundaries of powers are steadily expanded.

Many questions and, unfortunately, few answers. No laws can guard against every accident or every eventuality. Many of the best documented instances of information misuse predate the computer age. Prior to the Second World War the Dutch government maintained elaborate
systems of population registers. Designed to assist efficient administration, details were held including name, address and religious affiliation. Not intrinsically objectionable until the Second World War erupted, Holland was occupied and the Nazis obtained a list of the name and address of every Jew in Holland. Whilst the motives of those who seek personal data today may be benign and even laudable, data can have a very long life and a change in circumstances may result in data supplied for one purpose being put to another. Especially at the stage of collecting data, the human being behind the data may well be a matter of little or no interest but if anonymity is lost the consequences may be profound.