Information Technology Law

Seventh Edition

IAN J. LLOYD

Senior Research Fellow, ILAWS: The Institute for Law and the Web, Faculty of Business and Law, University of Southampton

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

Fourth Edition 2004
Fifth Edition 2008
Sixth Edition 2011

Impression: 1

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2014932447

ISBN 978–0–19–870232–0

Printed in Great Britain by
Ashford Colour Press Ltd, Gosport, Hampshire

1

Privacy, technology, and surveillance

Introduction

In 2004 Richard Thomas, then the Information Commissioner for the United Kingdom,[1] warned against the dangers of the country 'sleepwalking into a surveillance society'.[2] This theme was developed in a report published by his office in 2006 entitled *A Surveillance Society*.[3] In the foreword to the report he went further claiming that 'we are in fact waking up to a surveillance society that is already all around us'. The massive publicity generated by the recent revelations concerning data monitoring programmes such as Prism and Tampora which are conducted by the NSA in the United States (with assistance from the British agency GCHQ) and GCHQ's own operation Upstream,[4] provides further evidence in support of the Commissioner's argument.

Smoke and mirrors—from echelon to prism

> Imagine a global spying network that can eavesdrop on every single phone call, fax or e-mail, anywhere on the planet.
>
> It sounds like science fiction, but it's true.
>
> <http://news.bbc.co.uk/1/hi/503224.stm>

The summer and autumn of 2013 saw a plethora of media postings concerning revelations about the US government's systems for obtaining access to communications data. The passage quoted above would seem to fit well into these but actually comes from 1999 and relates to the disclosure of a massive surveillance operation, known as project ECHELON which allegedly allowed the US security agencies (and also those from the UK and a number of other countries) to monitor the content of all email traffic over the Internet. For anyone interested, the footnote below provides a link to a report on ECHELON produced by a European Parliamentary Committee.[5] In the world of espionage and national security, little seems to change. There are always more questions than answers.

[1] The status and role of the Information Commissioner will be discussed more extensively in subsequent chapters. Essentially, the Commissioner is charged with enforcement of the United Kingdom's data protection (and freedom of information) legislation. Again, this will be considered more fully in later chapters.

[2] <http://news.bbc.co.uk/1/hi/uk_politics/6260153.stm>.

[3] <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>.

[4] For an extensive collection of materials relating to these programmes see <http://www.theguardian.com/world/the-nsa-files>.

[5] <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN>.

In early summer 2013 we learned much about two surveillance programmes apparently operated by the United States' NSA and the Federal Bureau of Investigation (FBI). Under the first, the authorities have apparently been granted a secret court order requiring the major US telecommunications company Verizon (which offers fixed-line and mobile telecommunications services as well as broadband Internet access) to transmit on an ongoing basis a wide range of data concerning its users' communications to the NSA and the FBI.[6] In the UK (and the EU more generally) we are not strangers to the notion that communications providers should be required to retain communications data and, under specified circumstances and procedures, transfer it to law enforcement agencies (and indeed to a range of public authorities). The transfer of communications data is authorised under the Regulation of Investigatory Powers Act 2000 and is supervised by the Interception Commissioner. In his most recent report published in July 2012 he indicated that, during the reporting year, public authorities as a whole submitted 494,078 requests for communications data.[7] The intelligence agencies, police forces, and other law enforcement agencies are still the principal users of communications data. It is important to recognise that public authorities often make many requests for communications data in the course of a single investigation, so the total figure does not indicate the number of individuals or addresses targeted. Those numbers are not readily available, but would be much smaller.

This may seem a substantial figure but to put it into some perspective, Verizon have nearly 145 million customers, data on all of whom is required to be submitted on an ongoing basis to the NSA and FBI. It is not known whether other United States communications companies (in particular AT&T which is similar in size to Verizon) have been served with similar court orders but there are suggestions that these networks have been very willing to cooperate with law enforcement.[8] In theory the requirement to obtain a court order is stricter than the UK procedure which requires only approval by a senior member of staff within the public authority. The fact that proceedings are secret and the fact that the US Verizon order became known only through a leak does not inspire confidence.

The second element of US practice that was exposed by the whistleblower Edward Snowden, concerned NSA access to content-related data held by a range of Internet-related companies such as Google, Apple and Facebook. This data is clearly much more sensitive than the communications data discussed above. As with all aspects of the story there is uncertainty over even basic issues. The claim is that the NSA enjoyed direct access to servers. This has been vehemently denied by a number of the companies involved. A Google statement asserted that:

> Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a back door for the government to access private user data.[9]

Google publishes on a regular basis a so-called 'Transparency Report'.[10] This provides data on the number of requests it receives from governments around the world for access to data on the browsing history of individuals. This does not, however, give details of how many requests from the US authorities relate to national security concerns. A number

[6] <http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order>.

[7] <http://www.intelligencecommissioners.com/docs/0496.pdf>.

[8] <http://online.wsj.com/article_email/SB10001424127887324049504578543800240266368-lMyQjAxMTAzMDEwMzExNDMyWj.html>.

[9] <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

[10] <http://www.google.com/transparencyreport/>

of other Internet companies have produced similar statistics although, again, with very limited data about the proportion of national security requests.[11] At the time of writing, Google and a number of other communications providers are seeking permission from the US authorities to publish more data about the extent of national security-related requests for data.

In the United Kingdom, a draft Communications Data Bill (subsequently dropped following objections from the Deputy Prime Minister) was published in 2012. It was subjected to scrutiny by a joint Parliamentary Committee. In giving evidence to the committee the Home Secretary was asked to comment on the uses made of communications data. Her response was:

> As I say, I do not make any comment about individuals in relation to the security service, or any of the other security and intelligence agencies. It would not be appropriate for me to do so. Everybody who is working on this Bill is doing so because this Government believes that it is important that the police and the other agencies are able to continue to have the powers that they have today to do as we have discussed earlier, which is to save lives, in a new technological environment. I understand that the police estimate they get 30,000 urgent requests for communications data per year, and they estimate that they save lives in 25% to 40% of those cases. I think that matters to the public.[12]

Very large numbers but ones that sit rather uncomfortably with another statistic that a 'mere' 640 murders were committed in the UK during 2012.[13] It does seem hard to credit that between 7,500 to 12,000 lives are saved annually in the United Kingdom because of access to communications data.

Public and private surveillance

There is no doubt that communications data can be a valuable investigative tool for crime detection. In evidence before the Committee the Director General of the Serious and Organised Crime Agency indicated that it was used in 'around 95%' of their investigations. It is very common for information about Internet activity to be led in criminal cases. What we are seeing increasingly—especially as telecommunications networks and services are located squarely in the private sector—is that distinctions between public and private surveillance are becoming blurred. Surveillance systems such as Prism could not operate without the involvement and cooperation, whether voluntary or under legal compulsion, of private companies.

In 2012, the *Daily Telegraph* reported on a murder trial in which the female victim had vanished from her home with her body being found several weeks later. At the trial of the accused, a Dutch engineer named Tabak, prosecution evidence was led on the following lines:

> Lyndsey Farmery, an internet use analyst who assisted police with the investigation, took the jury through Tabak's online activity in the days after killing 25-year-old Miss Yeates.
>
> Web records from work and personal laptops show he researched the Wikipedia page for murder and maximum sentence for manslaughter, she said.
>
> While regularly checking the Avon and Somerset police website and a local news site, the Dutch engineer was also checking body decomposition rates.

[11] <http://www.guardian.co.uk/technology/2013/jun/17/apple-reveals-us-surveillance-requests>.

[12] <http://www.parliament.uk/documents/joint-committees/communications-data/Oral%20Evidence%20Volume.pdf>.

[13] <http://www.citizensreportuk.org/reports/murders-fatal-violence-uk.html>.

> Days after killing Miss Yeates at her Clifton flat on December 17, Tabak watched a time-lapse video of a body decomposing, Bristol Crown Court heard.
>
> Tabak—who denies murder but admits manslaughter—also went on Google to look up the definition of sexual assault.[14]

At another level of communication data, a freedom of information request in 2012 revealed that the Metropolitan Police had made 22,000 requests over a four-year period for access to data held by London Transport relating to journeys made using its system of Oyster cards.[15] The data can be used to place a suspect (or a card registered in the suspect's name) in the vicinity of an offence at the appropriate time. In another example of the use of electronic data, a magistrate was convicted of theft.[16] A woman had lost a Rolex watch in a Tesco supermarket. Two years later the watch was handed in to a jeweller's for repair. Its serial number was checked against a list of missing watches and this led to the arrest of the magistrate who had handed it in for repair. His defence that he had bought the watch as a present for his wife in a second-hand shop (whose location he could not remember) was undermined when data relating to use of his Tesco Clubcard placed him in the supermarket at the time the watch went missing.

As the above examples show, communications and location data can constitute crucial evidence in criminal investigations. In the Tesco example, there is an issue as to why the loyalty card data was still available in such detail two years after the event. The Data Protection Act requires that data be retained for no longer than is necessary for the purpose for which it was acquired. It is difficult to see what justification there might be for a supermarket to keep marketing data at this level of detail for two years.

In any matters relating to criminal investigations and even more to issues of national security, there has to be a balance between the legitimate need for secrecy and public accountability. The key issue is perhaps proportionality. We live very large parts of our existence online. OFCOM data indicates that the average UK consumer now sends fifty texts per week—a figure that has more than doubled in four years—with over 150 billion text messages sent in 2011.[17] Almost another ninety minutes per week is spent accessing social-networking sites and email, or using a mobile to access the Internet, while for the first time ever fewer phone calls are being made on both fixed and mobile phones.

We have well-established laws requiring respect for our physical property. Search warrants are required to be issued before law enforcement agencies can enter our houses and it is perhaps time that our virtual houses received similar protection. Another recent tool which has been extremely useful for law enforcement agencies is DNA evidence. There is certainly controversy concerning the circumstances under which DNA is collected and retained but there does not appear to be a strong body of opinion in favour of universal DNA profiling. Effectively, however, that is what appears to be happening with communications data in the United States. UK practice is more restrained but we do need a more evidence-based debate. I mentioned above data relating to the number of requests for access to Oyster card data. There is no data that I have been able to find relating to the number of times it has been used in the course of criminal prosecutions. In the wake of the Prism revelations in the United States, some cases were cited as evidence of the value

[14] <http://www.telegraph.co.uk/news/uknews/crime/8836161/Vincent-Tabak-researched-unsolved-murders-after-killing-Joanna-Yeates.html>.

[15] <http://www.theregister.co.uk/2012/02/10/metropolitan_police_asks_for_tfl_data/>.

[16] <http://www.telegraph.co.uk/news/uknews/1482200/Magistrate-fined-for-keeping-lost-Rolex.html>.

[17] <http://media.ofcom.org.uk/2012/07/18/uk-is-now-texting-more-than-talking/>.

of communications data in preventing terrorist offences but other sources have cast doubt on this, suggesting that other and older forms of intelligence gathering deserve the credit.[18]

To finish this introductory section on a lighter note, but one that does perhaps make the point about proportionality, I recall an intellectual exercise intended to identify the best way to reduce casualties in road accidents. We can all think of suggestions, invariably involving additional or improved safety features in cars. The winning suggestion was rather different. Prohibit seat belts and air bags. Instead make it mandatory to have a sharp spike fitted on the steering wheel pointing directly at the driver's heart. I'm sure it would cut the number of accidents but…[19]

Forms of surveillance

In 1971, Alan Westin in his seminal work, *Information Technology in a Democracy*,[20] identified three forms of surveillance that might be conducted by public authorities:

- physical
- psychological
- data.

Physical surveillance, as the name suggests, involves the act of watching or listening to the actions of an individual. Such surveillance, even making use of technology, has tended to be an expensive undertaking capable of being applied only to a limited number of individuals. In investigations subsequent to the 7 July 2005 bombings in London, it emerged that at least one of the bombers had come to the notice of the security services but had not been placed under surveillance. An intelligence source was reported as suggesting that MI5 considered that at the time of the London bombings in 2005, there were in the region of 800 Al Qaeda suspects, a figure which subsequently rose by a further 200. Whilst the security services tried to keep as many people under surveillance as possible, this was an extremely labour-intensive process, with the source suggesting that keeping a person under surveillance for twenty-four hours a day would require a team of between twenty and forty watchers. At the lower estimate, this would require MI5 to have 20,000 operatives. At the time in question, the total staff to cover all aspects of its work was in the region of 2,000.[21] Obviously—and as illustrated by the failure to monitor the actual bombers more closely—only a small proportion of identified suspects could be subjected to physical surveillance.

Examples of *psychological surveillance* include forms of interrogation or the use of personality tests, as favoured by some employers. Once again, logistical and cost constraints have served to limit the use of these techniques. The end-product of any form of surveillance is data or information.

[18] <http://www.guardian.co.uk/world/2013/jun/12/nsa-surveillance-data-terror-attack>.

[19] Also in the field of automotive safety, the European Commission has proposed that from 2015 all new cars should be installed with technology enabling them to contact the emergency services automatically in the event that sensors detect that the vehicle has been involved in an accident. It is estimated (on what basis is not clear) that the system, known as 112 eCall, could save 2,500 lives a year by enabling faster response to accidents. See <http://ec.europa.eu/commission_2010-2014/kallas/headlines/news/2013/06/ecall_en.htm>.

[20] Unir Microfilms Int., 1971.

[21] <http://thescotsman.scotsman.com/londonbombings/MI5-spied-on-only-one.5282797.jp>. The Intelligence and Security Committee made the same point in their report on the bombings (available from <http://www.cabinetoffice.gov.uk/publications/reports/intelligence/isc_7july_report.pdf>) although the precise numbers cited above were omitted for reasons of national security.

With both physical and psychological surveillance, an active role is played by the watcher. *Data surveillance* involves a different, more passive approach. Every action by an individual reveals something about the person. Very few actions do not involve individuals in giving out a measure of information about themselves. This may occur directly, for example, in filling out a form, or indirectly, as when goods or services are purchased. The essence of data surveillance lies in the collection and retention of these items of information.

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. Developments in data processing suggest that the distinction between informational and physical privacy is becoming more and more flimsy. The reach of systems of physical surveillance has been increased enormously by the involvement of the computer to digitise and process the information received.

Today, the critical distinction between forms of surveillance is perhaps between direct and targeted surveillance of particular individuals and the more general, all pervasive surveillance which permeates all our lives without being specifically directed at any particular purpose. As George Orwell wrote in his famous novel, *1984*:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time, but at any rate they could plug in your wire whenever they wanted to. You have to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

This certainly has echoes of much of the debate about current surveillance. When we are directly and personally the subject of scrutiny, there may well be the sense that our privacy is being infringed—and this chapter will continue to consider the extent to which rights of privacy are accepted and protected in the United Kingdom. In other cases, the issue is perhaps more that we are losing the ability to transact anonymously. A famous cartoon by Peter Steiner and first published in the *New York Times* depicts two dogs sitting in front of a computer screen with one captioned as telling the other 'in Cyberspace, no-one knows you're a dog'. The key word here is 'knows'. As will be discussed in later sections of this book, one of the difficulties created for users of social-networking sites (and indeed the Internet generally) is the difficulty in determining whether another person's online persona matches their real-life existence. A forty-year-old paedophile can easily and convincingly masquerade as a sixteen-year-old boy or girl. That is one danger, but for present purposes we might focus on another. Nobody may 'know' who you are, but if the information generated by your actions fits the profile of a dog, you may find yourself treated as one. Many Internet sites make much of their income through selling advertising space linked to particular search requests. Browse the Internet looking at hotels in a particular city and you will almost inevitably find banner adverts relating to those searches appearing when you view other sites such as online newspapers

Living in the surveillance society

In an information-based society, extensive details concerning the most trivial actions undertaken are recorded. In the context of e-commerce, an online bookshop will know, at least once customers have bought goods and accepted the presence of cookies on their

computers, the title of every book which is examined and the nature of catalogue searches made. This can be linked to name and address details.

Perhaps the most noticeable and extensive surveillance tool is the closed-circuit television camera (CCTV). It is a rare high street or even shop which does not have one or more cameras. The estimate is frequently cited that there are in the region of 14.2 million CCTVs in the United Kingdom. With a population approaching 60 million, that equates to roughly one camera for every fourteen inhabitants of the country. Two million motorists are fined each year as a result of being caught by speed cameras. In general, it is estimated that the average person can expect to be 'caught' on camera around 300 times a day.[22]

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. Around 10 million number plates are recorded each day with a total of some 7 billion records stored[23] and compared against records maintained by the Driver and Vehicle Licensing Agency and motor insurance companies to identify vehicles which are not taxed or insured. The system also links with police databases to flag the appearance of any vehicle recorded as being of interest to the police.[24]

Even in the physical environment, trials are being conducted with image-recognition systems linked to CCTV cameras,[25] which can monitor the movements of specific individuals. One of the most extensive systems has been installed in the London Borough of Newham.[26] Here it has been reported that images from 150 cameras are compared against a database of around 100 known offenders maintained by the Council. If a targeted individual is identified by the system, the police are automatically informed. The system, known as 'Mandrake', is claimed to be sufficiently sophisticated to defeat attempts to conceal identity by such tactics as wearing glasses or make-up or even growing a beard. An accuracy rate of 75 per cent is claimed for the system,[27] although other sources have cast doubt on this figure.[28] The downside, of course, is that 25 per cent of those recorded on the system are innocent people who will be viewed with suspicion because of a false identification. In more recent developments, it has been reported that CCTV systems are being tested which use advanced monitoring techniques to assess the movements and actions of individuals within their range, with the aim of identifying behavioural patterns which might be regarded as suspicious. An example might be of a person who remains on an underground station platform for a considerable period of time, allowing a number of trains to arrive and depart without attempting to board it.[29]

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 has published an application from Microsoft for a system which will monitor an employee's

[22] <http://news.bbc.co.uk/1/hi/uk/6108496.stm>. [23] <http://www.npia.police.uk/en/10505.htm>.

[24] Details of the system and its possible uses are given in a document, 'ANPR Strategy for the Police Service 2005–8', produced by the Association of Chief Police Officers and available from <http://www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc>.

[25] As was reported in *The Independent*, 12 January 2004, more than 4 million CCTV cameras are in use in the United Kingdom. At a ratio of one camera to fifteen people, this, it is claimed, makes the United Kingdom the 'most-watched nation in the world'.

[26] <http://www.bbc.co.uk/londonlive/news/july/cctv_170701.shtml>.

[27] *Daily Mail*, 15 October 1998.

[28] *The Guardian* has published claims that the system had never identified a suspected individual. See <http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html>.

[29] <http://rinf.com/alt-news/contributions/mick-meaney/20-of-uk-cctv-could-judge-your-behaviour-within-3-years/614/>.

heart rate, body temperature, blood pressure, and movement. It is claimed that the system will automatically detect signs of stress or illness. Even the Internet and World Wide Web (WWW), which are often touted as the last refuge of individualism, might equally accurately be described as a surveillance system par excellence. An individual browsing the Web leaves electronic trails wherever he or she passes. A software program can transmit a tracer known as a 'cookie'[30] from a website to the user's computer. Cookies can take a variety of forms and may retain details relating to the user's actions, either for the duration of a visit to a site or for a specified and potentially unlimited period of time.[31]

In terms of goods themselves, the ubiquitous barcode which facilitates identification of the product and its price at the checkout may be replaced by radio frequency identification tags (RFID). These are essentially a form of microchip capable of transmitting information, both prior to and after the point of sale. This would, for example, enable the movement of the object to be tracked, both in the store and also externally. One possibility which has been canvassed is that future generations of banknotes will have RFID tags embedded in them in order to enable movements of cash to be tracked with a view to countering money laundering. In respect of motor cars, the European Commission has launched a programme designed to specify standards for electronic vehicle identification (EVI). The programme, it is stated, aims to develop:

> an *electronic, unique identifier for motor vehicles*, which would enable a wealth of applications, many of them of crucial importance for the public authorities to combat congestion, unsafe traffic behaviour and vehicle crime on the European roads. It is clear that such an identifier as well as the communication means to remotely read it should be standardised and *interoperable* all over Europe.[32]

In the United Kingdom, it has been reported in a similar context that plans are being drawn up to fit all cars with a microchip which will monitor driving behaviour and automatically report a range of traffic offences, including speeding, road-tax evasion, and illegal parking.[33]

Examples of thickening information threads and trails are legion. Barely ten years ago, the only records compiled by United Kingdom telephone companies regarding telephone usage concerned the number of units of charge (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 do 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. Recent research conducted on behalf of BT illustrates well the issues involved. It is reported that 15,000 calls an hour are made from work phones to sex or chat telephone lines.[34] With mobile phones, even more data is recorded, with location data enabling the movements of the phone to be tracked with ever greater precision. Again, the widespread use of cash-dispensing machines allows the withdrawals of bank customers to be tracked on a real-time basis, both nationally and internationally.

[30] For information about the nature of these devices see <http://www.cookiecentral.com/faq.htm>.

[31] A Report on Privacy on the Internet has been prepared for the European Commission Working Party on Data Protection and gives some interesting insights into the topic. The report is available from <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf>.

[32] <http://www.publications.parliament.uk/pa/cm200304/cmselect/cmtran/319/319we45.htm> (emphasis in original).

[33] *Sunday Times*, 24 August 2003.

[34] Cited on Ceefax (an electronic information service broadcast by the BBC), 21 July 2003.

Surveillance and the law

Concern at these privacy implications of information technology was expressed by Lord Hoffmann when delivering his judgment in the House of Lords in the case of *R v Brown*:

> My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and the telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of a person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.[35]

The potential dangers were further considered by Lord Browne-Wilkinson VC in *Marcel v Metropolitan Police Commissioner*.[36] Documents belonging to the plaintiff had been seized by the police in the course of a criminal investigation. Civil proceedings were also current in respect of the same incidents, and a subpoena was served on behalf of one of the parties to this litigation seeking disclosure of some of these documents. Holding that the subpoena should be set aside, the judge expressed concern that:

> if the information obtained by the police, the Inland Revenue, the social security offices, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state.[37]

As indicated in the above passage, an appropriate balance between privacy—classically expressed in terms of the right to be left alone—and surveillance—representing the wish to discover information about another—is difficult to define. Although initially appearing as opposites, privacy and surveillance are linked almost as if they were conjoined twins.

A wide range of surveys of public opinion evidence show strong support for the protection of privacy. Although many of these derive from the United States, in the United Kingdom, the Information Commissioner has commissioned annual surveys of public opinion. In the annual report for 2000, the then Commissioner noted:

> Respondents were read a list of issues and asked to say how important they think each is. The proportion who thought that protecting peoples' rights to personal privacy was very important increased but not significantly from 73% to 75%. In terms of people's hierarchy of priorities the issue remains extremely important. Again only Crime Prevention and Improving Standards of Education are thought to be more important issues by the public.

Subsequent surveys have adopted a different formulation, more closely linked to the Information Commissioner's remit, by asking for respondents' views concerning the importance of protecting personal information. The answers, however, have remained fairly constant. Table 1.1 contains the results from the 2010 survey.[38]

[35] [1996] 1 All ER 545 at 555–6. [36] [1992] Ch 225.

[37] [1992] Ch 225 at 240. This quotation is also of considerable relevance to the emerging practice of data matching, which is considered more fully later.

[38] <http://ico.org.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_individuals.ashx>.

Table 1.1 Concerns with issues of social importance

Concerned	2004	2005	2010
Preventing crime	85%	88%	93%
The National Health Service	78%	83%	92%
Equal rights for everyone	69%	81%	87%
Protecting people's personal information	70%	83%	92%
National security	71%	78%	85%
Improving standards in education	76%	84%	90%
Protecting freedom of speech	67%	80%	81%
Environmental issues	66%	74%	77%
Unemployment	50%	70%	90%
Access to information held by public authorities	48%	66%	75%

Whilst it would be an exceptional person who placed no value upon privacy, significant difficulties have to be overcome in the attempt to give the concept a concrete legal meaning. First, it is undoubtedly the case that different people and societies have widely varying interpretations as to which matters are private and which reasonably belong in the public arena. Millions of (mainly) younger people place details of their lives on social-networking websites such as 'MySpace'[39] or 'Facebook'.[40] In many cases, the level of detail exposed appears excessive to those of an older generation.[41] Celebrities may court and value a greater degree of attention than the average person would find tolerable although, as cases such as *Campbell v MGN*[42] and *Douglas v Hello!*[43] illustrate, even celebrities draw distinctions between public and private life. Those living in close-knit communities may accept that their every action will be known to and commented upon by others. City-dwellers may expect much more in the way of freedom from observation but this may carry with it the spectre of the lack of interest and concern.

At a societal level, the United Kingdom is noted for attaching great value to privacy in respect of dealings with the tax system. In Sweden, by way of contrast, information about tax returns is a matter of public record. This is reported to have produced problems for the authorities at the time when the pop group Abba was at the height of its fame. Many thousands of fans discovered that they could readily and cheaply obtain copies of their idols' tax returns (which included a photograph). Dealing with the demand for copies is claimed to have brought the system close to meltdown. Even in the age of freedom of information legislation, it is difficult to envisage such a scenario being acceptable to the average British citizen. As perhaps an anecdote, however, whilst traditional forms of publication of financial information caused little stir, the emergence of a website, 'Ratsit.se', pushed even Swedish notions of openness to their limits when it started publishing financial details obtained from the national tax authority on its website, from where they could be accessed by anyone free of charge. The service proved popular, with about 50,000 searches being made each day. Many, it appears, were made by individuals curious to know details about their friends and neighbours. Whilst most might have hesitated to make a personal visit or request to the tax authorities for the data, the anonymity associated with web searches proved attractive. Numerous complaints were made to the Swedish data protection authorities. The tax authorities indicated to the website owners that, whilst Swedish

[39] <http://www.myspace.com/>. [40] <http://www.facebook.com/>.
[41] See e.g. <http://nymag.com/news/features/27341/>. [42] [2005] UKHL 61.
[43] [2007] UKHL 21.

freedom of information law obliged them to supply tax data, it did not require that it be supplied in electronic form. Provision of the data in paper form would have involved a massive effort to convert documents into electronic formats. Faced with this prospect, the site was reorganised. From June 2007, access could be obtained only upon payment of a fee and, in line with the principles applying in respect of Swedish credit reference agencies, the subject would be informed of the fact that a request had been made and of the identity of the requesting party.

Whilst surveillance is often seen as involving the surreptitious and unwelcome collection of personal data, this is not always the case. Although individuals may claim to value privacy, they frequently appear to do little to protect themselves. Hundreds of thousands of individuals have applied for supermarket 'loyalty cards'. Such cards provide an invaluable point of linkage between details of individual transactions and the more generic stock management computer systems which have long been a feature of retail life. The seller now knows not only what has been bought but also who has bought it, when, in conjunction with what other products, and what form of payment has been tendered. Analysis of the information will reveal much about the individual's habits and lifestyle which may be used as the basis for direct marketing, targeted at the individual customer.[44] Again, many thousands of individuals respond to lifestyle questionnaires which may be delivered either as a mailshot or accompanying a magazine. In return for the chance to win what are often low-value prizes, respondents freely disclose all manner of items of personal information.

Privacy issues

The classical legal definition of privacy is attributed to a United States judge, Judge Cooley, who opined that it consists of 'the right to be let alone'. A considerable number of other definitions have been formulated over the years. A number of these were cited in the *Report of the Committee on Privacy*.[45] The essential component, at least for the purposes of the present book, may be stated in terms that an individual has the right to control the extent to which personal information is disseminated to other people.

This notion, which is often referred to as involving 'informational privacy', has two main components. The first concerns the right to live life free from the attentions of others, effectively to avoid being watched. This is perhaps the essence of privacy as a human condition or state. Once a third party has information, the second element comes into play, with the individual seeking to control the use to which that information is put and, in particular, its range of dissemination.

The post-Second World War expansion of rights to privacy

Notions of a right to privacy have formed a feature of many domestic laws for decades and even centuries. Generally, however, rights to privacy would be rooted in a number of other legal concepts. In the United States, for example, the right of privacy has been seen as emerging from a range of constitutionally guaranteed protections. As was stated by Mr Justice Douglas in the case of *Griswold v Connecticut*:

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition

[44] For an excellent collection of links to materials on this topic see <http://www.nocards.org/>.

[45] (1972) Cmnd 5012.

> against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'[46]

This expansive basis for the right to privacy has resulted in the doctrine being held applicable to an extensive range of situations, including forming the basis of the seminal Supreme Court ruling in the case of *Roe v Wade*,[47] which established a constitutional right to abortion.

In the aftermath of the Second World War, the concept of human rights began to be recognised at an international level. In 1948, the General Assembly of the United Nations adopted the Universal Declaration of Human Rights. This proclaimed in Article 12 that:

> 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.

Although influential, the Universal Declaration has no binding legal force. Such a legal instrument was not long delayed. In 1949, the Council of Europe was established by international treaty. Its stated goals include the negotiation of agreements with the aim of securing 'the maintenance and further realisation of human rights and fundamental freedoms'.[48] One of the first actions undertaken within the Council was the negotiation of the Convention for the 'Protection of Fundamental Rights and Fundamental Freedoms' (European Convention on Human Rights, hereafter, 'the Convention'). The Convention was opened for signature in November 1950 and entered into force in September 1953. As its Preamble states, the signatory states reaffirmed:

> their profound belief in those fundamental freedoms which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the human rights upon which they depend…

Of the many rights conferred by the Convention, Article 8 is of particular relevance in the present context. This provides that:

1. Everyone has the right to respect for his private and family life, his home, and his correspondence.
2. 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.

Although the second paragraph of Article 8 is couched in terms relating to interference by public authority, the jurisprudence of the European Court of Human Rights has established that the obligation imposed upon Member States is to ensure that private and family life is protected by law against intrusions by any person or agency, whether within the public or the private sector. In the case of *Hatton v United Kingdom*,[49] the Court referred to the

[46] (1965) 381 United States 479 at 484.
[47] 410 United States 113.
[48] Statute of Council of Europe, Art. 1.
[49] (Application No. 36022/97) (2003) 15 BHRC 259.

existence of 'a positive duty on the State to take reasonable and appropriate measures to secure the applicants' rights under Article 8 § 1 of the Convention'.

The term, 'private life', is not defined further in the Convention. As with the United States concept of privacy, the term has been broadly interpreted by the European Court of Human Rights, which was established to supervise the state's compliance with the Convention's requirements. In one important respect, the Convention right goes beyond the United States notion of privacy. In the United States, a critical distinction exists between activities taking place on private property and those in public (or semi-public) places. The European notion of private life is less tied to physical objects, and may protect individuals in respect of their activities in the public arena. In the case of *Halford v United Kingdom*,[50] the European Court of Human Rights held that the protection of Article 8 extended to telephone conversations made by the applicant from her office phone. When her employers monitored the calls in the course of disciplinary proceedings against the applicant, the Court ruled that there had been a breach of Article 8.

The case of *Copland v United Kingdom*[51] is also of considerable significance. Here, the applicant was employed at a college in Wales. The college's Deputy Principal formed a suspicion about her relationship with another individual and believed that the applicant was misusing college facilities for personal purposes. Although there was no direct monitoring of the content of calls, the communications records of both outgoing and incoming telephone calls were analysed. Monitoring and analysis extended also to Internet usage in the form of the locations of the websites viewed, together with the dates and duration of browsing activities. Details of the addresses of email messages were subjected to a similar process.[52] Arguing that there had been no breach of the applicant's rights under Article 8, the United Kingdom government claimed that:

> Although there had been some monitoring of the applicant's telephone calls, e-mails and internet usage prior to November 1999, this did not extend to the interception of telephone calls or the analysis of the content of websites visited by her. The monitoring thus amounted to nothing more than the analysis of automatically generated information to determine whether College facilities had been used for personal purposes which, of itself, did not constitute a failure to respect private life or correspondence.[53]

This contention was rejected by the Court which, referring to its previous decision in *Halford*, held that email messages should be regarded in the same manner as telephone calls. Although in this case there was no monitoring of the content of either telephone calls or emails, the data recorded, it was held, constituted an 'integral element of the communications'.[54] In the absence of any warning having been given to the applicant of the possibility of monitoring, the conduct constituted a breach of Article 8.

In addition to expanding the scope of private life beyond the limits of private property, the jurisprudence of the European Court of Human Rights has shown that the enforcement of the right to respect for private life imposes positive obligations encompassing the grant of access to at least some forms of personal data. In the case of *Gaskin v United Kingdom*,[55] the complainant, whose childhood had been spent in the care of Liverpool City Council, sought access in adulthood to a wide range of social-work and medical records compiled

[50] 1997, 3 BHRC 31. [51] [2007] ECHR 62617/00.

[52] At the time that the activities occurred (around 1998–9), United Kingdom law made no provision regarding such conduct. The Telecommunications (Lawful Business Practice) Regulations 2000 made under the authority of the Regulation of Investigatory Powers Act 2000 would now apply to this form of activity.

[53] para. 32. [54] para. 43. [55] (1990) 12 EHRR 36.

during these years. At the time the request was made, the Data Protection Act 1984 provided a right of subject access only in respect of data held in electronic format. Although the Council took significant steps to assist the complainant—in particular by seeking the consent of all those responsible for creating records to their disclosure—access was denied, except where positive consent had been obtained.[56] Recognising that the grant of access to records containing personal data was an integral part of the requirements of Article 8, the Court held that the United Kingdom was in breach of its obligations by failing to establish an appropriate mechanism for determining the extent to which access should be granted.

As demonstrated in *Gaskin*,[57] although the breadth of Article 8 rights offers benefits for individuals, it also suffers from an inevitable lack of precision, especially in situations where conflict arises between competing claims. Building on the general principles, a trend emerged within Western Europe during the last third of the twentieth century for the introduction of data protection laws concerned specifically with the issues arising from the processing of personal data. One of the major concerns was that the capability of the computer to store, process, and disseminate information posed significant threats to the individual's ability to control the extent to which personal information was disseminated and the uses to which it might be put.

A linkage has frequently been drawn between the general right to privacy and the notion of informational privacy. This is clearly seen, both in the Council of Europe Convention on the Automated Processing of Personal Data and, more recently and extensively, in the text of the EC Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,[58] which makes no fewer than fourteen references to the noun 'privacy'. Article 1 of the Directive is explicit:

> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

The scope of these measures will be discussed in more detail in the following chapters.

Surveillance-based legislation

Great and tragic events invariably carry a lasting legacy and aftershocks from the events of September 11, 2001 continue to reverberate around the globe. The perception, true or false, that the Internet and forms of electronic communications are linked with the spread of global terrorism has impacted significantly on governmental attitudes to many of the issues discussed in this chapter and, indeed, throughout the whole of the field of information technology law. Of particular relevance to the present discussion is the extent to which changes have been made—and are being made—to the delicate balance between personal privacy and the interests of the government and also, of course, of society at large, in preventing the commission of terrorist offences. Many of the legislative responses to the threat of global terrorism, especially those within the United Kingdom, have been enacted with great speed, driven by perceived necessity but also carrying with them the risk of creating a chasm between those whose primary interest is in law enforcement and individuals and

[56] In some cases, consent was refused but in a majority of cases, the original author either could not be traced or failed to respond to the request. Effectively, silence was regarded as constituting refusal.

[57] *Gaskin v United Kingdom* (1990) 12 EHRR 36.

[58] Directive 95/46/EC, OJ 1995 L 281/31 (the Data Protection Directive).

bodies concerned with the protection and promotion of individual rights and freedoms. Creative tension between different interest groups is inevitable and can produce benefits when there is a degree of acceptance that each group is acting in good faith. When creation turns to destruction, everyone loses and in many respects the present debate between civil libertarian lobbyists and governments has become sterile. Possible consequences are that individuals may lose some of the major elements of the protection introduced and developed over the past decades, whilst governments risk losing popular legitimacy if they are seen as being unconcerned with and threatening towards the rights of citizens.

Many significant legislative moves have been made in order to enhance the powers of law enforcement and national security agencies in the aftermath of September 11. Most of the aspects, such as increased powers of arrest and detention, are outside the scope of this book. For present purposes, the most important changes relate to increased rights of access to personal data.

The starting point of the analysis should be the EC Directive on Privacy and Electronic Communications.[59] As originally drafted, this Directive provides individuals with extensive guarantees of privacy in respect of data pertaining to their electronic communications. At a very late stage in the legislative process, however, and following the events of September 11, an amendment was accepted by the European Parliament permitting EU Member States to 'adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph'. The grounds referred to include the safeguarding of 'national security … defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system'. Even prior to the entry into force of the Directive, this power has been extensively used within the United Kingdom.

Initial legislative provisions date back to the Regulation of Investigatory Powers Act 2000, which empower a senior police officer to require a communications provider to disclose any communications data in its possession where this is considered necessary in the interests of national security, the prevention or detection of crime, or a number of other situations.[61] The term 'communications data' is defined broadly to include traffic and location data, although, as has been stated by the Home Office:

> It is important to identify what communications data does include but equally important to be clear about what it does *not* include. The term communications data in the Act does not include the content of any communication.[62]

The Regulation of Investigatory Powers Act 2000 did not require that providers retain data, although concerns had been expressed that mobile-phone operators were retaining customer records for a period of months and in some cases years.[63] The conformity of this practice with the requirements of the Data Protection Act 1998 that:

> Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes[64]

had been doubted. The passage of the Anti-Terrorism, Crime and Security Act 2001, which was rushed through Parliament in a matter of weeks, provided a legal basis for the retention of data. The Act conferred power on the Secretary of State to draw up a code of practice

[59] Directive 2002/58/EC, OJ 2002 L 201–37. [60] Art. 15. [61] s. 22.

[62] Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data (March 2003).

[63] See e.g. 'Liberties Fear over Mobile Phone Details', *The Guardian*, 27 October 2001, reporting that the mobile network, Virgin, has retained all data from the establishment of its network in 1999.

[64] Sch. 1, fifth data protection principle.

specifying periods of time during which communications providers would be required to retain communications data.[65] Although the Secretary of State was granted legislative power, it was envisaged that a voluntary code would be agreed between government and the communications industry. Negotiations did not produce agreement with industry, concerns centring in large part on the cost implications of retaining large amounts of data. The leading service provider, AOL, for example, has estimated that it would require 36,000 CDs in order to store one year's supply of communications data relating to its customers with set-up costs of £30 million and annual running costs of the same amount.

Initial proposals by the government for the establishment of a code of practice received heavy criticism, both in terms of the period of time within which data might require to be retained and the range of government agencies which might be granted access to this data. An initial draft code was withdrawn in July 2002 and a further draft was published in March 2003.[66] This restricted the range of agencies which might seek access to data but retains the requirement that data be retained for a period of twelve months.

Privacy and surveillance

One of the main ways in which privacy can be threatened is by the act of placing an individual under surveillance. Surveillance can take a variety of forms. Physical surveillance is as old-established as society. At an official level, it might involve placing individuals suspected of criminal conduct under surveillance. Whilst at the private level, reference can be made to the nosy neighbour looking at life through the corner of a set of lace curtains. In some instances, the success of surveillance may depend on its existence being unknown to its target. In other cases, the fact that conduct may be watched is itself used as an instrument for social control. As George Orwell described in his novel *1984*, the mere fact that people were aware that their activities might be subject to monitoring by the authorities would cause them to modify their behaviour, regardless of whether they were being watched or not.

There is no doubt that the world we inhabit today has changed and is changing at 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. The Internet and its use in academic life provides a very apposite example. There is no doubt that it provides teachers and students with access to a massively increased range of data. An author trying to track down a missing citation need often require only to submit a few words to a search engine such as 'Google' to be presented with the answer in seconds. More, however, does not always mean better. Excessive use of electronic resources will cause traditional research skills to atrophy, the availability of one hundred electronic articles saying the same thing adds little to the reader's understanding of a topic—even making the charitable assumption that the articles are accurate in what they say. The tendency is to seek to find the answer before one has understood the question.

Similar issues arise in the wider world. Information is replacing knowledge and the change in terminology also indicates reliance on a more mechanistic- and statistical-based

[65] s. 102. [66] Available from <http://www.homeoffice.gov.uk/docs/consult.pdf>.

view of the world. An example can be seen in the increasing use of DNA technology for crime-detection purposes. In the United Kingdom, aided by a policy of taking and retaining samples from everyone charged and convicted of even the most minor offence, the national police DNA database now contains over 2 million entries. This tool, as with most forms of scientific evidence, is based upon calculations of probability. Recent high-profile cases in the United Kingdom have shown up some of the failings of such an approach and, in particular, that technology is only as effective as those using it. The consequences for those wrongly identified and convicted on the basis of the misunderstanding of statistics has been profound and tragic.

Although we may challenge the efficacy of some of the models, there is no doubt that the underlying principles of data protection matter more today than ever before. With developments in data processing and other forms of technology, there is the potential for every movement we make to be tracked and recorded. There is a well-established tradition of providing for necessary exceptions from the strict application of data protection principles in the context of national security and crime prevention and detection. These have been applied in the context of specific investigations and with the attempt made to secure a reasonable balance between the interests of the state and of individuals. With a move towards reliance upon databases, whether of DNA samples or other forms of information, there has been a significant shift in the nature of policing, from the attempt to find evidence linking an individual with an offence, to one where an individual is sought whose profile fits that of a suspected offender. In many cases, such an approach is justified but, as will be discussed in the final section of this chapter, the perceived and accepted need to defeat terrorism is leading to the removal of some data protection safeguards, with little being put in place to replace these. As with all aspects of design, unless components are included at an early stage, it is more difficult and expensive to incorporate them at a later stage.

Many of the recorded instances of the misuse of information have occurred, not as part of the original design, but as a by-product of the fact that the information is available. The story has been told of how the elaborate population registers maintained by the Dutch authorities prior to the Second World War (no doubt with the best possible motives) were used by the invading Germans to facilitate the deportation of thousands of people.[67] In this case, as in any similar case, it is clear that it was not the information per se that harmed individuals, but rather the use that was made of it. In this sense, information is a tool, but a very flexible tool; and whenever personal information is stored, the subject is to some extent 'a hostage to fortune'. Information which is freely supplied today, and which reflects no discredit in the existing social climate, may be looked upon very differently should circumstances change. It may, of course, be questioned how far any legal safeguards may be effective in the situation of an external invasion or unconstitutional usurpation of power. In discussions on this point in Sweden it has been suggested that:

> Under a threat of occupation there may be reason to remove or destroy computer installations and various registers in order to prevent the installations or important information

[67] F. W. Hondius, *Emerging Data Protection in Europe* (Amsterdam, 1975). See also Victor Mayer-Schünberger, *Delete: The Virtue of Forgetting in a Digital Age* (Princeton, 2009). This states fairly precise figures and comments:

> Because of the information contained in the comprehensive Registry, the Nazis were able to identify, deport and murder a much higher percentage (73 percent) of the Dutch Jewish population than in Belgium (40 percent) or France ((25 percent), or any other European nation.

Obviously, all sorts of factors would have affected the scale of Nazi atrocities in different countries but as so often, history is trying to warn us.

> from falling into enemy hands. An enemy may, for example, wish to acquire population registers and other records which can assist his war effort. There may be reason to revise the plans as to which data processing systems should be destroyed or removed in a war situation.[68]

Whilst such plans and procedures might appear to afford protection against the possibility of outside intervention, it must be recognised that, in the past, the use of personal information as a weapon against individuals has not been the exclusive province of totalitarian states. Again, during the Second World War, the United States government used information supposedly supplied in confidence during the Census to track down and intern citizens of Japanese ancestry.[69] More recently, it has been reported that the United States Selective Service system purchased a list of 167,000 names of boys who had responded to a promotion organised by a chain of ice-cream parlours offering a free ice cream on the occasion of their eighteenth birthday. This list of names, addresses, and dates of birth was used in order to track down those who had failed to register for military service.[70] Such practices illustrate, first, the ubiquitous nature of personal information and, second, that no clear dividing line can be drawn between public- and private-sector users, as information obtained within one sector may well be transferred to the other.

At a slightly less serious level, it was reported in the United Kingdom that information supplied in the course of the 1971 Census describing the previous occupations of respondents was passed on to health authorities, who used it to contact retired nurses with a view to discovering why they left the profession and to encourage them to consider returning to work.[71] Whilst it may be argued that no harm was caused to the individuals concerned by the use to which this information was put, it provides further evidence of the ubiquitous nature of information, and of the ease with which information supplied for one purpose can be put to another use.

Conclusions

Almost seventy years ago, the world was recovering from the trauma of global conflict. The negotiation of the Universal Declaration and the European Convention on Human Rights was regarded as a major legislative component of the road to recovery. The enhancement of individual rights was seen as the best response to the trauma of global terror. Today, the view appears to be that rights need to be restricted in order to defeat terror. Whilst it may, of course, be argued that a closer parallel is with the enactment of emergency legislation in time of war, the present situation is perhaps more akin to the image portrayed in George Orwell's novel *1984*, where a condition of perpetual and undeclared war existed between three power blocks, with shifting alliances and battles generally fought far from home but used as justification for repressive domestic policies.

Few issues in the field admit of easy answers. Any attempt to strike a balance between competing interests is difficult, especially in a fast-changing environment. Most would agree that law enforcement agencies should be provided with the best possible tools to enable them to perform their vital tasks. Data can constitute an extremely valuable investigative tool but the whole premise of data protection legislation over the decades has been

[68] *Transnational Data Report*, 1(5) (1978), p. 17.
[69] W. Petersen, *Japanese Americans* (New York, 1971).
[70] *Transnational Data Report*, 10(4) (1987), p. 25.
[71] D. Madgwick and T. Smythe, *The Invasion of Privacy* (London, 1974).

that the potential for misuse is considerable. At least within a United Kingdom context, the main problem is perhaps a lack of awareness. If data were nuclear particles or perhaps even genetically modified foodstuffs, people would be aware of and respectful of the dangers involved in their use and transportation. The danger today is that data flows are invisible and when society becomes aware of the potential for misuse, it may be too late to put this technological genie back in the bottle.