6 Personal data rights

6.1 Data protection and freedom of information

Because IT massively increases the range of data that are recorded somewhere or other, and makes data much easier to move about and access than when paper-based records were all we had, society has found it appropriate to develop new laws relating individuals and information. On the one hand, the law is trying to assure people a degree of privacy by controlling access to data concerning themselves: *data protection*. On the other hand, it is giving individuals new rights to see information held by public bodies: *freedom of information*.

Data protection legislation is motivated by the worry that IT is turning the world into what David Brin has called a "transparent society", where no-one any longer has a side of their life which is private.[34] We never chose to abandon privacy – it is happening as an unforeseen side-effect of technology developments which have been adopted for other reasons; and a wholly transparent society might prove hard for many decent people to bear.

The link between IT and freedom of information legislation is less direct. The fundamental motive is that public bodies are there to serve the public, so the public should have a right to see the details of what its servants are doing. Without IT, though, it might have been impractical to require organizations to answer questions on any and every detail of their work at any time. Now, IT is making it more practical, so the law is requiring it.

Both of these areas of law come under the heading of "regulation": they impact chiefly on organizations rather than on individuals, and the issues they create for organizations are more about knowing exactly what is required and finding ways to comply than about willingness to obey the law. Nevertheless, it is certainly possible for an individual to offend against the Data Protection Act, and someone convicted of doing so will get a criminal record.

Both areas are supervised by an officer called the Information Commissioner, who promotes compliance with these new laws, instigates legal action against those who breach them, and maintains a register of users of personal data. An Information Tribunal hears appeals from the Commissioner's rulings.

We shall first consider freedom of information, and then move on to the more complex topic of data protection.

6.2 The Freedom of Information Act

The *Freedom of Information Act 2000* came into force from 2005 onwards; it is a purely national measure rather than a response to an EU directive.[35] In summary, it says that individuals are entitled to request and promptly receive any information held by "public authorities" (a term which includes national and local government bodies, but also nationalized industries, the National Health Service, and many other organizations) unless the information in question is exempt. There is a long list of exempt information categories. For instance, one individual cannot demand information relating to another individual – apart from being a commonsense proviso, if it were not there this law would directly conflict with the Data Protection Act to be discussed later; no-one can demand information whose release would prejudice national security; and so on and so forth.

The availability of this new right is clearly of interest to many individuals. For present purposes, though, we are more interested in its consequences for the bodies which are obliged to supply information. The impact is significant. During the first twelve months when the Act was in force, there were over 100,000 freedom-of-information applications, including about 70,000 to local authorities. A little arithmetic suggests that the average council must have dealt with several requests per week. Fielding a request will not necessarily involve merely releasing an immediately-available item of information. It may require applicant and respondent organization to co-operate with one another to establish what relevant data are held by the latter and how to track them down within the complex archives accumulated by any organization. There is an obligation on the respondent organization to give "reasonable advice and assistance" to the applicant, who cannot be expected to be familiar (for instance) with the computational or database infrastructures of the organization, or to know whether a particular category of information is held by the organization at all.

Data which an organization is obliged to locate and hand over are not even necessarily limited to material currently present in an electronic file system. An early issue which came before the Information Tribunal (*Harper* v. *Information Commissioner* (2005)) related to material that was previously on a system but had been deleted. To the ordinary user, the information is gone, but there are forensic-computing techniques which can often retrieve deleted files. The Tribunal decided that, depending on the technical possibilities, the organization might be obliged to do that.

6.3 Limiting the burden

Various provisos are designed to keep the burden on organizations within bounds. At least one of these, however – namely that an organization is not required to provide information which is already "reasonably accessible to the applicant" – seems in practice to be weaker than it sounds. One might think that if a public body makes a large one-off effort to put all its non-exempt information on the Web (and updates anything that changes), it could then meet its freedom-of-information obligations simply by publishing the URL of its website. But that will not be enough. Scottish freedom of information legislation matches the English law in most respects (though it is formally separate, being contained in the *Freedom of Information (Scotland) Act 2002*). In 2005 the Scottish Information Commissioner considered whether presence of an item of information somewhere on an organization's website meant that the item counts as already "reasonably accessible"; he decided that this does not follow (*Mr L and the Lothian and Borders Safety Camera Partnership*, decision no. 001/2005). The information must be accessible *to the particular applicant*, and the Commissioner noted that only 45 per cent of adult Scots were making personal use of the internet. Furthermore many people, even with internet access, might find it difficult to track particular items down within a large, complex website without professional help.

Other burden-limiting provisos may be more significant. An organization need not respond to repeated or vexatious requests, so a disgruntled council-tax payer cannot use the Freedom of Information Act to get his own back by pestering his council with silly applications. And some sensible requests would take far more time (and therefore expense) to answer than others, so there is no obligation to provide an answer if the estimated cost of doing so exceeds an "appropriate limit". For a local authority, the appropriate limit equates to three man-days' work. (Unless the *average* time per request is very much less than that, the figures on numbers of requests quoted earlier mean that an average council must be maintaining a full-time post just to field freedom of information applications.)

6.4 Implications for the private sector

Private-sector firms have no duty to respond to freedom of information applications; they are not public bodies, supported by public money. Private companies normally want to preserve confidentiality about their internal affairs, releasing only carefully selected information which will help to maintain, or at least not undermine, their market position.

However, public-sector and private-sector organizations have many dealings with one another. For instance, public bodies often invite commercial firms to tender for contracts. So important questions arise about what a public body is required to do in response to a freedom of information application which relates to the commercial activities of a private-sector organization. For instance, would a public body have to give one firm details of bids received for a contract from competing firms, so that the applicant could use this knowledge to pitch its own bid just right to win the contract?

A law which required that would seriously damage the workings of the market economy, and the Freedom of Information Act does not go that far. It provides "qualified exemption" for applications relating to "trade secrets, and information the disclosure of which would…be likely to damage commercial interests". The word "qualified" means that this is not a blanket exemption, as the ones already mentioned for personal data or data relating to national security are. Instead, for commercially-sensitive data the body receiving the application must consider case by case whether the public interest in maintaining the exemption (for the sake of a healthy economy) outweighs the public interest in transparency. It is the public body which makes this decision. It is encouraged to consult the commercial organization, where appropriate, but it is not required to do so; and if the commercial firm does not like the public body's decision, it has no right to complain to the Commissioner or appeal to the Tribunal.

In a crude example like the scenario just sketched, where a private company says to a public body in effect "before we tender for your contract, show us the bids you have received from our competitors", the public body would certainly invoke the qualified exemption in order to refuse the application, and the Information Commissioner would uphold the refusal.

But cases in real life are often not so simple. Thus, take the first freedom of information appeal taken to the Information Tribunal by a journalist: *John Connor Press Associates* v. *Information Commissioner*, decided in 2006.

Matt Davis is a Brighton journalist and MD of John Connor; he asked the National Maritime Museum how much it paid for a work of art it commissioned for a new series. The Museum invoked the qualified exemption in order to decline to give the information out immediately, saying that Davis must wait until after the conclusion of negotiations on the next contract in the series; it gave him the data requested six months after his application. Davis complained to the Information Commissioner, who decided in favour of the Museum. Davis then appealed to the Tribunal.

(There is no suggestion in this case that Davis or his firm had a direct interest in these contracts; anyone can make a freedom of information application, one does not have to establish a "need to know". And although the actual documents supplied by the responding organization will often be subject to copyright, the organization is not allowed to impose any duty of confidentiality on the applicant with respect to the *information contained* in the documents – hence giving the information to the applicant amounts to publishing it for all to see.)

The Tribunal decided for Davis against the Commissioner's ruling. It held that the two art commissions were for separate projects, so releasing details about the first contract, once it was concluded, could not damage the interests of the Museum.

The rationale here perhaps depends on specific facts about the two commissions. To an outsider unfamiliar with the specifics, the Tribunal decision looks surprising. Negotiating a contract is a delicate process, rather like playing poker; one might have supposed that the Museum would be best placed to judge whether it was safe to release details (particularly when it sought only to delay releasing them, not to refuse altogether). Although the Freedom of Information Act does not straightforwardly require disclosure of commercially confidential information, the boundary round commercially-exempt information is evidently being drawn quite tightly.

6.5 Government recalcitrance

While the freedom of information exemption for commercially sensitive information is proving fairly narrow, it is noticeable on the other hand that the British Government (the body which chose to introduce the Act) is aggressive in claiming exemptions for its own data.

For instance, there is currently a political controversy about the proposed introduction of a nationwide system of identity cards. Many people object to this on several separate grounds. It is seen as a threat to civil liberty; it is arguably not likely to achieve its alleged purpose of reducing the terrorist threat; and large-scale and innovative government IT projects have a dismal history of expensive failure.

Against that background, the Office of Government Commerce refused a freedom-of-information application in 2006 for information about the outcome of Gateway Reviews of the identity card project.[36] The identity card project looks just the kind of thing which motivated the introduction of the Act: it is publicly funded, and many members of the public have a lively and legitimate interest in it. Furthermore, the OGC made no claim that releasing the Gateway Reviews would harm any commercial interests. The Information Commissioner struck down the refusal and required the OGC to release the information. But the government appealed that ruling; in 2008 it managed to win its appeal, by resorting to obscure legal manoeuvres which shocked some commentators.

Thus it is not altogether clear that the practical results of the Freedom of Information Act are shaping up to correspond closely with the motives cited for introducing it. It is an area that business needs to keep an eye on. It cannot assume that because business is not subject to freedom of information applications, it will not be affected by them.

6.6 Attitudes to privacy

Turning to the data protection legislation: as said earlier, the motivation for data protection laws is the idea that people want to keep some areas of their lives private, and are entitled to do so.

Before entering into details of the legislation, it is worth remarking that there seem to be large differences between individuals with respect to how much they care about privacy. A striking difference between generations at present is that older people find it hard to understand the willingness (indeed eagerness) of young people to expose their personal lives on social networking sites like Facebook and YouTube. Those of us who were young forty years ago enjoyed partying, but we knew that our follies would be forgotten in a few days. We wonder whether today's youth will live to cringe at the idea that their private lives are recorded in graphic detail for perpetuity – or whether technology has produced a generation that genuinely does not set a high value on privacy and never will.

The issue is not only about young people. Shoppers of all ages have proved happy to sign up for electronic loyalty cards such as Tesco's Clubcard, which allow the shop to build up a database of personal information enabling them to target their marketing at individual customers, in exchange for a tiny price discount. It may be that people are content to go along with this only because most of them have no idea how much detail they are revealing. (Tesco links its Clubcard data to data from the census and from other sources to build up much fuller profiles of its customers than they might imagine.) This will surely become better understood with time; David Manasian believes that "privacy is likely to become one of the most contentious and troublesome issues in western politics".[37] If so, data protection laws are destined to become increasingly crucial.

6.7 Is there a right to privacy in Britain?

Since there is unclarity about how far the population actually cares about privacy, before looking at the IT-related legislation on this topic, we ought to consider how far the law protects privacy in general, independently of computing technology.

Historically, English law recognised no right to privacy, and the nation did not appear to see this as an issue – perhaps people felt able to protect their privacy without needing to resort to law. The first hint of a legal right to privacy in Britain came after the Second World War, when the UK signed up to the European Convention on Human Rights, which came into force in 1953; signatory nations were expected to change their laws where needed to guarantee the rights specified in the Convention, and one of these is:

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

But, for many decades, this article (and indeed the Convention in general) had little practical impact on British law. The Convention had largely been drafted by Britons, with a view to expressing basic standards that had recently been and were still being flouted by Nazi and Communist régimes respectively, but which the British had been enjoying for a long time past. There was no appetite for treating the Convention as a trigger for modifications to our laws.

That changed in 1998, when rather than amending any individual laws that might not have harmonized perfectly with the Convention, the Convention was written bodily into English law as the *Human Rights Act*. But since the articles of the Convention are expressed in far more general terms than ordinary English laws, it remained to be seen how the article about privacy (and the other articles) would be interpreted in practice.

In the case of the privacy article, an important case was *Copland* v. *United Kingdom*, heard by the European Court of Human Rights in 2007.

Lynette Copland was personal assistant to the Principal of Carmarthenshire College, where she was suspected of misusing college telephones and computers for private calls and e-mails; the college put in place a system for monitoring her usage, and she complained that this was an invasion of her privacy. (Why the college cared about e-mails is unclear, since they cost nothing; perhaps its real worry was about spending working time on private activities. In any event, the monitoring did not lead to any disciplinary proceedings.) Defending UK law before the European Court, the British Government pointed out that although Lynette Copland's calls were logged, their contents were not intercepted, hence there was no failure to respect her private life or correspondence. But the European Court found that the logged details are themselves part of what the Convention guarantees privacy for. Lynette Copland was awarded damages.

To many British onlookers, it came as a shock to learn that an employee might be entitled to privacy even with respect to alleged abuse of the employer's phone bill. However, in other European countries there would be nothing surprising there. Similar cases, including some where the employees were indeed cheating their employers, had been decided in the employees' favour years earlier.

Conversely, in the USA it is by now routine for organizations to monitor their employees' activities more intrusively than this, and there is no suggestion there that this might be legally problematic. Apparently there is at present a large gulf between American and European positions on privacy rights. As is often the case nowadays, Britain finds itself in an awkward intermediate position, with American-type instincts but European-type law.

So far as I know, *Copland* has not led to new legislation in Britain, though organizations have taken to being explicit with their staff about policies on monitoring communications. (One factor in the judgement by the European Court of Human Rights was that the College had not warned Lynette Copland that her calls might be monitored. In the past, it was usual for British employers to log staff phone calls without discussing the fact that they did so.)

In 2008, though, the *Mosley* v. *News of the World* case was seen as introducing a legal right to privacy in the UK "by the back door".

Max Mosley is president of the Fédération Internationale de l'Automobile, the governing body for motor racing and pressure group representing car-users' interests. The *News of the World* ran a story revealing that he enjoys sado-masochistic "orgies". Mosley sued the newspaper under the Human Rights Act, citing the privacy article; the newspaper defended itself by citing another article in the same document protecting freedom of expression.

Since the two principles are stated in broad, general terms which are more or less mutually contradictory, in the past British courts might have been expected to resolve the contradiction in line with past British legal norms, and Mosley would have lost. To many commentators' surprise, the judge in *Mosley* v. *News of the World* found for Mosley, saying that he "had a reasonable expectation of privacy in relation to sexual activities (albeit unconventional) carried on between consenting adults on private property." He awarded the significant sum of £60,000 in damages.

This is the most striking of a series of recent cases in which judges have been developing a legal right to privacy as an example of "judicial activism", creating precedents without any new legislation. So by now it is probably misleading to say that UK law does not recognise a right to privacy.

6.8 The history of data protection

Although the foregoing explains the social background within which data protection laws have been emerging, these specifically IT-related laws create constraints which go far beyond merely extending general privacy rights to the digital domain.

As computing grew in importance, laws about processing personal data were at first introduced separately in separate European countries. Britain was relatively late to bring in such a law. In the 1970s, it was seen as a commercial advantage for Britain to lack such legislation while other European countries had it: firms wanting to process data within Europe would prefer a country where there was less legal interference.

In the 1980s the balance of advantage swung the other way, as countries with strong data protection began to forbid export of personal data to laxer régimes. Rather than lose business, the UK introduced the *Data Protection Act 1984*. That Act has since been superseded by the *Data Protection Act 1998*, implementing the EU *Data Protection Directive*. References, below, to the "Data Protection Act" will refer to the 1998 Act.

This brief history helps to explain why current British data protection law is the way it is. Any such law must strike a balance between two interests. The stronger the law, the better it is for individuals who value their privacy – but the more difficulty the law will create for businesses (and the other organizations to which it applies). Britain has consistently given the interests of business a high priority.

Britain was able to do that with the 1998 Act, because the European Directive allowed some flexibility for countries to make different choices when transposing it into their national law. The UK Government was open about the fact that it aimed to produce an Act that was as weak as possible, consistent with meeting the requirements of the Directive. Data protection is an area of IT law where there remain quite large differences between EU member states, although each legal régime is a response to the same Directive. Presumably, some European societies value protection for individuals so highly that they (or at least their governments) are willing to pay a cost in terms of greater burdens on business.

6.9 The Data Protection Act in outline

Although the British Act is weaker than its counterparts elsewhere, it is still a tough law. It creates very real problems for business – large enough problems to justify extended coverage here.

The Data Protection Act 1998 is problematic for a number of different reasons:

- it is both very *complicated*, and in parts quite *vague*
- it is often hard for an organization to know precisely *what its obligations are*
- when the obligations are clear, they are sometimes *difficult to achieve*
- some things forbidden by the Act are things that a reputable business might well have wanted to do, and which many people might see as *not objectionable*.

To English lawyers, the Act is a strange piece of legislation – one lawyer used the word "unprecedented".[38] This is partly because it takes various passages of wording over from the EU Directive, which was drawn up by people used to Continental-style rather than Common Law legal traditions; so the statute often uses such general language that judges are forced to surmise what the legislators were trying to say (something that, as we saw in chapter 2, was tabooed in the English tradition).

Within a short textbook it is not possible to give a full account of the Act, but here are its main points:

- it relates to data about *identifiable persons* ("data subjects")
- an organization[39] may gather, hold, process, or pass on personal data only with the subject's *active consent*
  - however, there are *special circumstances* in which this prohibition does not apply
  - there are *exemptions* for activities such as journalism and policing (both of which would presumably be well-nigh impossible if they were not exempted)
- certain categories of personal data are classed as *sensitive data*, for which the rules are stricter
- personal data may be used only for the *original purpose*(*s*) for which it was gathered, and retained *no longer than necessary*
- an organization handling personal data must *notify* the Information Commissioner about what it is doing
- personal data must be processed *fairly*
- a data subject is entitled to *see what data* an organization holds on him, and can *object* to what the organization is doing with his data; the Act specially caters for objections to
  - use for *direct marketing*
  - *automatic processing*
- personal data must be *stored safely*, and may not be moved *out of the EU* into laxer jurisdictions.

Each of these points will be enlarged on below. But first, to illustrate how tough the European data protection régime can be, let us consider the now-famous *Bodil Lindqvist* case, heard in Sweden in 2003.

6.10 The *Bodil Lindqvist* case

Bodil Lindqvist did voluntary work for her church in the village of Alseda, organizing adult confirmation classes. For the benefit of confirmation candidates, from her home PC she put up a chatty website with information about herself and her colleagues, including phone numbers, and mentioning that one of them was working part-time because she had injured her foot. Mrs Lindqvist did not check with her colleagues before putting the site up, or notify the Swedish information commissioner (probably it never crossed her mind that what she was doing might be controversial), but one of the colleagues objected. Mrs Lindqvist took the site down, and turned herself in to the local police.

The Swedish public prosecutor took Mrs Lindqvist to court under the Swedish counterpart of the Data Protection Act; Mrs Lindqvist lost the case, and appealed. The appeal court referred various questions about the European Directive to the European Court of Justice for authoritative rulings. On the basis of those rulings (to be discussed in a moment), Mrs Lindqvist's conviction was upheld. She was fined 4000 Swedish crowns (about £300 at the then exchange rate) – and, perhaps more important for Mrs Lindqvist, she acquired a criminal record.

If a clearly decent private citizen faces this treatment under data protection law, then (to quote a group of American lawyers) "business organizations may assume that the ECJ condones highly aggressive prosecution of alleged privacy violations under the provision of the Data Protection Directive".[40]

The EU Directive includes an exemption for "personal or domestic activities": one will not be convicted for keeping a private address book with friends' and family contact details, for instance. Mrs Lindqvist's defence argued that her voluntary work should come under that exemption, but the ECJ rejected this argument. As for her argument that the prosecution was incompatible with the guarantee of free speech in the European Convention on Human Rights, the Court simply refused to acknowledge any contradiction.

The Swedish appeal court asked the ECJ whether typing and posting a Web page that included mentions of identifiable people counted as "processing personal data". The ECJ answer was yes: to do anything with such information constitutes "processing".

The court of first instance[41] had treated the offence as aggravated by the mention of the injured foot: medical information comes under the heading of "sensitive data". The ECJ confirmed that that was correct. (Lloyd, p. 43, asks whether a public comment that an athlete could not compete in some event because of injury would therefore fall foul of the law; he suggests perhaps not, but it is unclear what the relevant difference is.)

The one respect in which the ECJ interpreted the Directive more leniently than the Swedish court of first instance was with respect to exporting data outside the EU. It ruled that simply placing data on a European website which is globally accessible does not count as data export. However, this seems to have been largely because the site was not arranged in the expectation that non-Europeans would visit it, and there was no evidence that any had done so. In a business context the situation might be very different. David Scheer reports that when the US-based company General Motors decided to update its electronic telephone directory, allowing staff working for GM in any country to look up the work numbers of colleagues elsewhere, they had to "spen[d] about six months amassing piles of legal documentation and other paperwork" to make this legal for European GM sites:

> Not even GM's U.S. headquarters could know the phone numbers, if the company didn't take some measures first… The rules are so broad that global companies assign dozens, and in some cases hundreds, of employees to deal with them….[42]

Returning to the Lindqvist case: this was of course resolved under Swedish law, and although English judges commonly treat decisions in other Common Law jurisdictions (e.g. North America, Ireland, Australia) as persuasive precedents, Continental decisions normally play no role in English courts – Continental law is not a precedent-based system. However, if one considers that the Swedish law was introduced in response to a Directive applicable also in Britain, and interpreted by a Court of Justice whose rulings are equally binding on our courts, it becomes difficult to regard Lindqvist as simply irrelevant in Britain.

For the lawyer Stewart Room "There can be no doubt that [the facts in Lindqvist] would not have resulted in prosecution under the Data Protection Act."[43] Indeed, recent British decisions have made our interpretation of the EU Directive less rather than more like the interpretations applying in some Continental countries, as we shall see shortly. But this may be an unstable situation. Even if the UK is happy with a lax privacy régime, it will not necessarily be allowed to retain it indefinitely.

6.11 The Data Protection Act in more detail

Let us now look in a little more detail at the main points of the Data Protection Act, listed earlier.

Identifiable persons

Data controlled by the Act are any data which either directly identify a living person, or enable a living person to be identified; and that includes not just factual data about a person, but also anyone else's opinion about the person or intentions towards the person. The data need not include the person's name, if other information allows an individual to be identified. Ian Lloyd quotes the example of the disease haemophilia, which is inherited by all sons of a haemophiliac mother, so that data identifying a deceased woman as a haemophiliac counts under the Act as (sensitive) personal data about any sons she had who are now alive.

Personal data are not limited to text files, but cover e.g. CCTV images, recordings of people speaking to automated call-centre systems, and so forth. Under the French version of the law, a cookie is likely to count as personal data about the individual on whose machine it is placed.

This sounds, then, as though any file whatever which briefly mentions an identifiable person, in whatever context, will be hit. The leading British case here is *Durant* v. *Financial Services Authority* (2003).

Durant found himself in a dispute with Barclays Bank, which came under the supervision of the Financial Services Authority. Durant invoked the Data Protection Act to ask the FSA for copies of all personal data which it held on him. The FSA gave Durant some material, with information about third parties blanked out, but refused to show him other files that contained his name, on the ground that they did not count as "personal data" about Durant. Durant claimed that he was entitled to any file that mentioned him.

The Court of Appeal sided with the FSA. It found that, to be covered by the Act, personal data must be "information that affects [the individual's] privacy", not just any material that includes a casual mention of an individual.

This represents a considerable loosening of obligations under the Act, relative to the interpretation that looked possible. One might feel that the interpretation in *Durant* is a more reasonable compromise between the rights of the individual, and the need of organizations to function efficiently. However, many legal observers believe that the *Durant* decision interpreted the Act more narrowly than the EU Directive requires. (This is a main reason why I noted above that the gap between British and Continental data protection régimes has been widening.) In 2004, the European Commission announced an investigation of the UK data protection régime, to see whether it adequately implements the Directive. (However, since 2005 this investigation appears to have gone quiet.)

6.11.1 Active consent

If personal data is processed, the body doing the processing must have the data subject's consent, and the Directive lays down that inferring consent from lack of objection is not enough: the subject must positively opt in. (This point has not yet been tested in British courts; some observers believe that British law may fudge the issue and allow "presumed consent".) Often, an organization will obtain data about individuals not from them but from a third party: in that case, the organization must inform the individuals that it holds the data.

(One common problem arises when a firm is bought up by another firm and the new owners want to contact the customers of the firm they have acquired. This counts as transferring personal data to a third party, and may be disallowed unless arrangements to secure consent are in place.)

There is a list of exemptions from the consent requirement. We have seen that journalists are allowed to keep files on people without their permission. Another kind of exemption would be for data needed by an employer for staff administration, such as running payroll or pensions software. But the exemptions are not open-ended. They cover only data which are strictly necessary for the purposes in question. Ian Lloyd offers the example of an employer which wants to include next-of-kin contact details in staff files, in case of emergencies at work. It sounds sensible; but Lloyd believes that these would probably not be exempt data (the next-of-kin's permission would be needed), because the staff member can do his or her job without the employer having this information.

6.11.2 Sensitive data

There is a presumption in favour of no processing whatever, without the explicit consent of the data subject, of information within a list of defined "sensitive" categories:

- race or ethnic origin
- political views
- religious or philosophical beliefs
- trades union membership
- health
- sex life

Even with respect to "sensitive data" there are exemptions, but these are defined extremely tightly.

One noteworthy point about the list of sensitive categories is that it evidently represents a political decision, rather than an objective listing of the kinds of information people most want to keep private. The Information Commissioner examined the latter issue in a 2006 survey.[44] It found that by far the most sensitive category of information is financial data, which is not on the Data Protection Act list – financial data scored more than twice as high as any category on that list other than health and sex life.

(There are probably large cultural differences in this respect between nations. I understand that, in Sweden, everyone's income tax returns are public – something that might lead to revolution in Britain!)

6.11.3 Use for original purposes and keep no longer than necessary

When an organization gathers personal data, it must say what it is going to use the data for, and erase the data when that task is complete.

It might often happen that an organization gathers data for one purpose, and then finds that the data could be used for another worthwhile purpose; that is not permitted. The new purpose might not be at all adverse to the interests of the data subjects. For instance, an insurance company will ask prospective clients for various background details so that it can advise on choosing a suitable policy. Having gathered such information from many clients, the company might then realize that statistics derived from that database could be used to devise new types of policy for which there is currently an unmet need. This could benefit some of the individuals (as well as the company), but it is forbidden under the Act.

In this example, which is fairly typical, one might think that there was an easy solution: the only data needed for the second purpose are statistical data, so the company could anonymize the data before using them for statistical analysis. However, in litigation which is not yet fully resolved, it is maintained that the act of anonymizing data *itself* counts as "processing personal data", hence is caught by the law.

A leading case relating to "keeping data no longer than necessary" is *Pal* v. *General Medical Council & ors* (2004). Dr Pal made a complaint to the General Medical Council relating to the treatment of some elderly patients. The complaint file was formally closed in 2000, but correspondence relating to Pal continued between the GMC and other parties; it involved a suggestion that Dr Pal's actions may not have been wholly rational. In 2004, these papers were still held by the GMC. Dr Pal said that they ought to have been destroyed when the complaint file was closed, and the court found in his favour.

Incidentally, the data in this case was documentation on paper; the Data Protection Act applies to paper as well as electronic information, provided that the paper files are organized in a way that makes them accessible via the name of the data subject. Readers of this textbook will be more concerned with the obligation to "weed" electronic files. But introducing routines for identifying and erasing information whenever required by this proviso of the Act will be no small task even in the electronic case.

6.11.4 Notification

Under the 1984 Act, one needed a licence in order to process personal data, but in view of the massive workload involved in issuing licences the 1998 Act replaced this with a requirement to notify the Information Commissioner about what one is doing with personal data. To process personal data without notification is a criminal offence.

Nevertheless, current figures suggest that only a fraction of the British organizations which are processing personal data are indeed notifying the Commissioner as required. (And if this aspect of the Act is being flouted, one naturally wonders how far the other constraints in the Act are being respected in practice.)

One relevant point here is that, to date, the UK Information Commissioner (unlike counterparts in other EU countries) has lacked the power of audit. Comparable supervisory bodies such as the Health and Safety Executive or the Financial Services Authority do not wait to be shown evidence that a particular organization is breaking their rules; they go into organizations to monitor compliance, without needing an invitation.

However, it has been questioned whether the EU Directive is adequately implemented if the Commissioner lacks this power, and in 2008 the Justice Secretary announced that the Commissioner will be given the power to audit public bodies in future. (The new power will not extend to private-sector organizations; in the present economic climate it is presumably felt desirable to avoid throwing extra burdens on business, though the minister denied that this was the main consideration.)

6.11.5 Processing must be fair

This proviso in the Act is a particularly clear case of the difference between Continental-style legislation and the English tradition. Fairness is a subjective concept. An ordinary English law would try to achieve fairness by deciding what objectively-defined activities would be fair, and requiring people to act in those ways – it would not leave it to judges to assess "fairness" for themselves.

Since the Data Protection Act is not that kind of law, the only way to know what it requires is to look at the precedents which have emerged so far. We shall examine two examples.

The first, *CCN Credit Systems Ltd* v. *Data Protection Registrar* (1990), was heard under the 1984 Act (but in the present context that is not important). Like other credit reference agencies, CCN was using data relating credit risks to addresses as input to its systems which decided whether individuals were good credit risks. This was normal practice in the industry; for one thing, it is easier to keep postal addresses straight than to link personal names reliably to their bearers – names are often shared by many individuals, and they are liable to occur in variant forms. But someone complained to the Data Protection Registrar (the earlier title for the officer now called the Information Commissioner) when he was refused credit because the previous householder at his address had a poor credit history. The Registrar required CCN to desist from this practice, and the court upheld the Registrar's veto.

The judgement made the "fairness" aspect particularly explicit. The judge said:

> We think it right to say that we accept that CCN did not intend to process data unfairly, and did not believe itself to be acting unfairly. But it is necessary to determine the question of fairness objectively, and in our view the case of unfairness has been made out.

This acknowledges that different people see fairness differently, while implying that the law will be imposing a relatively strong sense.

The second example of "unfairness" for the purposes of the Data Protection Act never came to court, because the organization involved, B4U.com, did not challenge the Information Commissioner's ruling. This matter related to commercial use of the electoral roll. In the 1990s it began to be common practice to use the electoral roll for purposes such as direct marketing; at that time copies of the roll could be bought by anyone for any use. From 2000 onwards the roll was produced in alternative editions; the complete version was used only in connexion with elections, while individuals could take themselves off the version available for commercial use. In 2006 B4U.com advertised a service allowing users to track down individuals they wanted to locate, drawing on the last publicly-available edition of the complete electoral roll.

The complete roll was obtained legally, and the use B4U.com made of it was legal when they obtained it. There has never been specific legislation controlling commercial use of old electoral rolls. But the Information Commissioner ruled that this use was "unfair". B4U.com did not challenge this, and closed its service down.

In both the CCN and B4U examples, readers may well be happy with the decision reached. But the "fairness" proviso of the Data Protection Act does not seem very satisfactory in terms of specifying a predictable boundary between what is fair and what is not.

6.11.6 Right to see and correct data

Every individual is entitled to see any personal data about him held by an organization, and to correct inaccuracies.

Provided an organization is permitted to hold a given category of data about you, you do not in general have a right to object to the data being processed. But you can forbid certain special kinds of processing. One is direct marketing; readers will be aware of this, from the various pieces of small print and tick-boxes that are nowadays routinely encountered when one fills in a retail order form. Processing for purposes of making automated decisions may need a little more glossing. Nowadays it is common practice for decisions on matters such as whether to issue a credit card to be made mechanically, based on the answers on the application form; experts say that automated decisions have a better track record of discriminating good from bad credit risks than decisions made by human credit controllers. But the framers of the Data Protection Act saw this kind of automatic decision-making as potentially harmful to individuals, so anyone is allowed to opt out of it.

6.11.7 Safe storage

Specifically, the Act requires that those holding personal data must, "[h]aving regard to the state of technological development and the cost of implementing any measures,…ensure a level of security appropriate to" the nature of the data and the harm that could result from its loss. This includes "ensur[ing] the reliability of any employees…who have access to the personal data."

The law recognizes that perfection may not be feasible, but it requires that whatever safeguards are reasonable, given the state of the art at the relevant time, must be taken. What counts as "reasonable" in this context will be for courts to decide – and standards that count as adequate will presumably change as technology advances.

Again a proviso in the Act which seems desirable from the individual's point of view has the drawback of unpredictability from the point of view of the organizations who must comply. To many readers, though, the most noteworthy point about this proviso is that the British Government, which was responsible for introducing the Data Protection Act, has become an industrial-scale violator of the safe storage obligation. The most notorious example was the loss in 2007 of two CDs containing extensive details about 25 million child benefit claimants; apart from that, over the year to April 2008 government officials were reported as losing details relating to more than 300,000 individuals a month, including confidential material such as banking details and criminal records. It is hard for laws to be effective if they contain an implicit rider "do as we say, not as we do".

(Public confidence was further eroded in January 2009 when a Treasury minister estimated that more than one in fourteen of the entries on the central taxpayer database contain errors.)

After a mislaid memory stick with usernames and passwords for twelve million users of the Gateway income-tax and state-benefit website was lost in a Staffordshire pub car-park in November 2008, forcing the site to be suspended, the Prime Minister asked the country to accept that losses of sensitive data were inevitable. If such mistakes are truly inevitable, how can anyone be punished for committing them?

6.11.8 Export control

Since electronic data can be moved across the world effortlessly and instantly, it would be pointless to control processing of personal data rigorously within the EU if holders of it could send it overseas for processing. So exporting data into unsatisfactory data protection régimes is forbidden.

Any EU member state is automatically deemed to have a satisfactory régime, and the European Commission has a working party that determines which non-EU countries are permissible destinations for export of personal data. At present Switzerland and Argentina are two countries whose data protection is judged adequate. Many other countries are not: these notably include the USA.

This creates practical difficulties for business. In order to get round the problem, the European Commission negotiated a so-called "Safe Harbour" agreement with the USA in 2000: it comprises a list of principles, going beyond the requirements of American law, which particular American firms can sign up to and thereby become permitted importers of personal data.

"Safe Harbour" has its own problems, though. The negotiations from which it emerged were acrimonious. American authorities have little sympathy with European data protection principles, seeing them as a protectionist economic device masquerading as a measure to benefit the citizen. And this must lead one to wonder how diligent, in practice, American companies that sign up to Safe Harbour will be about sticking to the letter of our laws.

On the other hand the European Parliament believes that the Safe Harbour safeguards may not be strong enough, and it may force the Commission to renegotiate the agreement.

Lastly, Safe Harbour achieves nothing unless American firms do sign up. So far they are not rushing to do so.

6.12 Is the law already outdated?

So much for the existing Data Protection Act and the EU Directive which it implements. Both are still fairly new, so there is a great deal of detail which will only be filled in as cases come before the courts.

However, we saw in earlier chapters that the speeds at which law and technology evolve are very different. One criticism now widely directed against the data protection legislation is that it is seriously out of date, and perhaps was already out of date when it came into force, because it ignores the internet. Lloyd comments (p. 59):

> the Directive and the Act are to a considerable extent surviving dinosaurs from the age when computers were mainly freestanding machines…with limited networking capabilities. The world has moved on….

Rowland and Macdonald (p. 381) discuss some of the problems in making holders of data responsible for what happens to data on the Web, where anyone can download and process the material:

> When [personal] information is placed on the web by an organisation or institution, how should that organisation's registration be framed? If the information is made available on an individual's home page, does that mean that the processing attracts an exemption on the grounds of personal and domestic use? In short, can legislation on data protection cope with this phenomenon? Even if the capability is there, does enforcement and supervision become such a gargantuan task that it becomes impossible, for all practical purposes, to locate and deal with contraventions?

These are serious questions. Some readers may like the idea of an unpoliceable internet, preferring a free-for-all where the law is impotent. But from a business point of view that attitude could be shortsighted. If the law throws up its hands and abandons the attempt to control the internet, individuals will withhold trust. Already, lack of trust online is frequently identified as a (perhaps the) chief barrier to the flourishing of electronic business.[45] Unless mankind finds ways to foster trust online, we shall not be able to reap the full benefits which the technology is capable of delivering; and law is normally a crucial part of the social infrastructure on which trust depends.

This makes it unlikely that data protection legislation will be abandoned. But it will surely have to change in dramatic and unforeseeable ways, to catch up with the technology. At present, the IT industry is starting to move away from a model in which organizations hold and process their own data towards a *cloud computing* model, in which much data and processing migrates via the internet to data centres that may be distributed across various jurisdictions. By 2008, some industry leaders were advocating "free-trade zones in cyberspace", where data could be processed under common rules (presumably developed by the industry, like the mediaeval Law Merchant, rather than by any particular terrestrial state).

In its current, national or EU-based form, the law creates large difficulties for organizations which must satisfy its requirements, and these difficulties will grow as the law is enforced more actively. For a computing student who plans to find a job using his degree within some public- or private-sector organization, this situation has a silver lining. Organizations will need to deploy IT skills in novel ways in order to comply with the legislation. That should be a new source of interesting work for my readers.