Law for Computing Students

Geoffrey Sampson

Geoffrey Sampson

Law for Computing Students

Law for Computing Students

ISBN 978-87-7681-471-7

Contents

Acknowledgements

I should like to express my gratitude to Robin Fry and Charlotte Shakespeare, both of Beachcroft LLP, for advice during the writing of this book. They bear no responsibility for any shortcomings in the finished text.

1. Introduction

1.1 The purpose of this book

So why do computing students need to know anything about law, beyond – just like anyone else – how to keep themselves out of trouble with the police?

Well, most students who take a degree in computing (computer science, information systems, "informatics", or similar) aim to find a computing-related job in a company or a public-sector organization. And that job will not involve just sitting in a back room hacking code. Jobs like that mostly disappeared with the twentieth century, and those that remain have largely been offshored to countries like India. Jobs for British computing graduates in the 21st century involve using technical knowledge to help a business to flourish; they are about business savvy as much as about bits and bytes. (This includes public-sector jobs; public-sector organizations do not make profits, but they run "businesses" as commercial companies do.) A crucial factor for successful business is an understanding of the broad legal framework within which business operates; computing graduates need to be aware in particular of how law impinges on information technology.

Readers need not take my word for this. In Britain, the body which lays down standards for our profession under royal charter is the British Computer Society. One function of the BCS is accrediting computing degrees: the Society scrutinizes curricula and delivery of teaching, and confirms (or declines to confirm!) that particular qualifications from particular institutions are acceptable by national standards. The BCS lays special stress on the need for computing degrees to balance technical content with substantial elements of what it calls "LSEPI" – legal, social, ethical, and professional issues. This book is about the L of LSEPI.

It is true that, up to now, a BCS-accredited qualification has not been an indispensable requirement for working in our profession. Computing is not yet like, say, medicine or architecture: no-one is allowed to practise as a doctor or an architect without a qualification recognised by the appropriate professional body, but as yet there are no legal restrictions on entry to the IT profession. However, that is because our subject is still new; the situation is unlikely to last. Already in 2006 the British government made the first moves towards introducing statutory controls on entry to jobs in computer security, and it seems probable that this trend will spread to other areas of the profession. Some university computing departments may still be teaching the subject in exclusively techie terms – the first generation of computing teachers tended to come from backgrounds in maths or engineering, so the techie stuff is what they care about. But degrees which do not have an "LSEPI" dimension yet will find that they need to develop one.

In any case, the real issue is not about some arbitrary requirement by a professional organization; it is about what employers want. Ian Campbell, chairman of the Corporate IT Forum and Chief Information Officer at British Energy, spells the point out clearly:

> the future will be IT lite, with technology departments staffed by smaller numbers of people, with higher levels of commercial awareness and lower levels of technical expertise … they will be business people first and their core skill set will be commercial rather than technological.[1]

Awareness of the legal framework within which an IT-based business operates is one of those core skills.

Some familiarity with information technology law is a necessary part of 21st-century computing education, then. That does not mean that people in computing jobs need to have every clause of every computing-related statute at their fingertips, or that this book will be offering that level of detail. (It would be many times longer than it is, if it tried to do that.) When a business confronts a specific legal problem, it takes advice from a professional lawyer, just as we do in our private lives if we find ourselves in some legal difficulty. (Sensible people in their private lives try to avoid the need for lawyers as far as possible, but a business, even if it is respectable and well-run, will commonly encounter quite a few situations calling for legal advice and perhaps for actual litigation.)

What the rest of the graduate-level people in a business need, who are not trained lawyers, is a broad grasp of the general nature of the legal environment in which the business (together with its trading partners and its competitors) is operating. In private life, the average person does not need detailed knowledge of the law of contract, but he certainly needs to understand that his signature on a document may create a binding commitment. What this book aims to give computing students is that kind of broad level of understanding of the law applicable to IT. When the book discusses individual laws, the focus will be on their overall thrust; there will be no attempt to list every special case and exception. It is more important to show the reader *whereabouts in an IT-based business legal problems are likely to arise*, than to identify the exact nature of potential problems and problem solutions.

(Let me stress that someone facing a specific legal problem should not attempt to use this book as a substitute for taking professional advice. The book is not intended for that purpose, and not suitable for it.)

Even a longer textbook could not provide a detailed statement of IT law which graduates could rely on after they find jobs, because law changes. IT law is changing particularly fast. This is part of what the student needs to learn: not just elements of what the law happens to be at a particular moment, but a sense of the extent to which it is fluid, the directions in which it is tending to evolve, and the nature of the pressures influencing this area of legal development. This book will discuss these latter issues, as well as the state of the law as it stands at the time of writing (namely 2009).

One of the central things which computing students need to understand about law is how unclear it often is. This may come as a shock, because in technical areas of computing everything is precise. Within a given computer language, a sequence of characters either is a valid line of code or it is not. There is no room for debate; if the compiler accepts the line, it is valid, and if not, not. The student's only task is to learn to write valid code and avoid writing the other kind. Law is not like that (it cannot be, unfortunately). Quite often we shall find that even legal experts cannot say for certain what the legal implications are of some entirely realistic computing-related business scenario. Understanding that the law is often vague is an important part of understanding the law.

1.2 Geographical perspective

Another way in which law contrasts with standard computing topics is that computing technicalities are the same everywhere, but law varies from country to country. In this book we shall be concerned with IT law as it affects business in England and Wales. This will frequently require us to look at laws of other countries. British businesses often depend heavily on trade with the USA, and many British firms are subsidiaries of American parent companies; consequently, some American laws impact on business life in Britain. Also, thanks to UK membership of the European Union, much new law, including IT-related legislation, originates in Europe rather than being purely "home-brewed". There will be many references in this book to these legal influences from outside, but to make sense of them we need to adopt some particular geographical perspective. Our perspective will be that of IT professionals based in England and Wales.

England and Wales share a single system of law, which for historical reasons is called “English law”. The legal system of Northern Ireland is separate in terms of organization, and differs in some details of content; but none of those differences, to the best of my knowledge, affect matters discussed in this book.

Scotland is a rather different case. When Scotland and England were joined into one kingdom in 1707, Scotland kept its own legal system, which differed from English law not just in detail but in fundamentals. The two systems have grown together to a considerable extent over the subsequent 300 years, but they remain distinct, and new laws are often restricted to one or other side of the Scottish border. Thus, one English law that we shall need to look at in some detail in chapter 6 is the *Data Protection Act 1998*; that law does not apply in Scotland, which has its own data protection act with somewhat different provisions.

At the very general level at which this book is written, differences between Scottish and English law are few and not crucial. The bulk of material will apply equally to both countries. But where differences are visible even at this general level, the book will present the position that applies in England (and Wales and Northern Ireland) rather than in Scotland.

It is impossible to understand a particular area of law, information technology law or any other, without a general awareness of the overall legal system within which it is embedded. Accordingly, chapter 2 will outline some of the basics of our legal system. Subsequent chapters will then look in turn at various areas of law which are specially relevant to the profession of computing.

1.3 Further reading

In compiling this brief introductory survey of law for computing students, I have relied heavily on longer books which present the material in much greater authoritative detail. Some of these are intended chiefly for legal professionals, but computing students and others who are not law specialists will often find it enlightening to look at what they say about particular points.

For a general account of how English law works, see:

> Catherine Elliott and Frances Quinn, *English Legal System*, 9th edn, Pearson Longman, 2008.

The details of IT law are covered in the following textbooks, each of which has its own strengths and weaknesses:

> David Bainbridge, *Introduction to Information Technology Law*, 6th edn, Pearson Longman, 2008.[2]

> Ian J. Lloyd, *Information Technology Law*, 5th edn, Oxford University Press, 2008.

Chris Reed and John Angel, eds, *Computer Law: the Law and Regulation of Information Technology*, 6th edn, Oxford University Press, 2007.

Diane Rowland and Elizabeth Macdonald, *Information Technology Law*, 3rd edn, Cavendish Publishing, 2005.

A book addressed to IT managers concerned with the interactions between law and practical managerial problems is:

Jeremy Holt and Jeremy Newton, eds, *A Manager's Guide to IT Law*, British Computer Society, 2004.

The following title is designed to cover the syllabus of the ISEB foundation course "IT Law Essentials" (ISEB is the Information Systems Examination Board):

Jon Fell, ed., *IT Law: an ISEB Foundation*, British Computer Society, 2007.

Because the law is constantly evolving, books like these have to be kept up to date through frequent new editions; someone checking the law on a specific point should take care to use the latest edition. The editions listed above were the newest editions of the respective titles when this book was written.

Since this book relates mainly to law as it applies to IT-based businesses, it will sometimes be relevant to refer to passages in my textbook on e-business:

Geoffrey Sampson, *Electronic Business*, 2nd edn, British Computer Society, 2008.

Literature citations in this book which give author or editor alone, e.g. "Lloyd, p. 95", will refer to one of the items listed above. Publication details for other quoted works will be shown in footnotes.

2. The nature of English law

2.1 Different jurisdictions

The legal systems of different countries vary, not just in detail but sometimes in their basic nature. For historical reasons, the legal system of the USA is very similar to that of England and Wales, while the legal systems of the main Continental European countries, including most of our EU partners, are rather different from the English legal system.

When a business transaction takes place between organizations and/or people in different countries, in principle there is a question about *jurisdiction* – which country's laws apply to the transaction? That can be a real issue in one area of IT, namely e-commerce. When an individual uses the internet to buy something from a seller in another country, the buyer is unlikely to know what rights he has if the transaction goes wrong. But (contrary to what some readers perhaps expect), within the field of IT law as a whole jurisdiction questions do not loom large. When a business needs to think about legal issues, normally there will be no doubt about which country's law is relevant (though there may be plenty of doubt about what that body of law actually says about the matter in question). If firms make contracts across national boundaries, they will usually settle which legal system is to apply through an explicit clause in the contract.

I have discussed problems about jurisdiction for e-commerce in my *Electronic Business* textbook, but that issue is not significant enough to discuss further in this book. However, the legal consequences of Britain's EU membership mean that we shall certainly need to look at differences between English and Continental styles of law.

2.2 Is IT law special?

The phrase "information technology law" sounds as though, within the entire body of English law, there is a special subset of laws about computing and those are the only laws relevant to our profession. But it is not like that. What the phrase really means is "those parts of law in general which are often relevant to IT activities, or which have specially serious implications for IT activities". The particular laws in question usually will not have been introduced in response to IT in particular; they may be centuries old, but now computers have been invented it turns out that those laws have important consequences for the new technology.

Some new laws have been "purpose-built" in response to the rise of IT. The *Data Protection Act 1998*, already mentioned, is a good example. But "information technology law" is not concerned only (or even mainly) with those laws.

This is not to say that, from a legal point of view, information technology is just one more area of human life along with all the others that the law has to consider. IT does create special problems for law.

One problem is speed of change. The law has always needed to adapt to new developments in society and technology, but law changes slowly. With earlier innovative technologies, the law may have been just about able to keep up, but the pace at which IT is innovating and mutating is possibly unparallelled in history. There is a real question whether the mechanisms by which law evolves are equal to the challenge of a technology that has become central to much of human life, but which comes up with significant new developments on an almost weekly basis.

The issue is not only about changes in the law, but about the speed at which established legal procedures operate. For instance, we shall see in chapter 4 that there is an increasing tendency for those who develop valuable new software techniques to use patent law to protect their intellectual property. One problem there is that taking out a patent is a time-consuming process. If the inventor of a new machine expects the market for it to last for decades, it may not matter that it takes a few years to secure patent rights. But with computer technology it can happen that an innovation is marketable for only two or three years before being superseded by an even newer and superior alternative – in which case the patent system may not be much use in practice.

Another feature of IT which is arguably "special" from a legal point of view is that crucial issues are often highly technical. Any technology has esoteric details that take extended study to master, but often there is no need for lawyers to go deeply into technicalities. A rough everyday understanding will often be enough. Cases about buying and selling cars, motor accidents, and so forth come before the courts every day, but the judges and the barristers arguing before them will not normally need to know anything in detail about the engineering issues involved in fuel injection, gear ratios, or the like. For computing, comparable technicalities are often crucial.

In consequence, we sometimes encounter cases where the judge's decision is based on flat misunderstanding of our technology. Consider for instance the 2002 case *SAM Business Systems* versus *Hedley & Co*. SAM supplied a firm of stockbrokers with a software package which the purchasers were unable to get working satisfactorily; SAM argued that the problem lay with the purchasers rather than with the package, pointing out that the latter was in use without problems at other sites. Explaining the reasons for his decision, the judge treated that argument dismissively:

> I am no more impressed by it than if I were told by a garage that there were 1,000 other cars of the same type as the one I had bought where there was no complaint of the defect that I was complaining of so why should I be complaining …? We have all heard of Monday cars, so maybe this was a Monday software programme.

As readers will realize, this analogy is wholly misleading. Two cars may be the same model, yet one could have defects while the other runs perfectly. With a digital product such as a computer program, two copies should be not just very similar but precisely identical. Unless the judge was suggesting that the package sold to Hedleys was a corrupted copy (in which case it would have been a trivial matter for SAM to replace it with a good copy), his remarks about Monday cars, with due respect, were senseless. Yet his decision not only resolved that particular case, but (through the legal system of precedent which we shall look at shortly) has the potential to affect the decisions in an indefinite number of future cases – the reason why I know about this case is that it is widely cited as setting a legal precedent. It may be that there are few areas where limited technical knowledge creates as many difficulties for the law as IT.

Thus it perhaps is fair to see IT law as "special" in some respects, though it is not a separate kind of law. But there are "kinds of law"; the next thing to look at is how law can be classified. There are three important ways of categorizing different areas of English law:

- by the nature of the adversaries
- by source
- by the basis of authority.

2.3 The nature of the adversaries

Here the distinction is between *civil* (or "private") and *criminal* law.

All English law consists of rules for resolving disputes between two sides – it is *adversarial*. (An English court never does anything on its own initiative, but only resolves conflicts that are brought to it.) In criminal law, one side is the state – nominally, the Queen.

It is worth taking a moment to consider what we mean by the word "state". Fundamentally, a state (in our case the United Kingdom) is an organization which maintains a *monopoly of force* in a territory. We recognise the UK as a state because we accept that it reserves to itself the right to make people and organizations in our country behave, by force if necessary, where "behaving" means among other things not using force on one another.

If A murders B, then B cannot as an individual prosecute A; but the state does not want murder happening in its territory, so it prosecutes A (and, if A resists arrest, the state is quite prepared to use force to compel A into court and later into prison). If A maims or defrauds B, then B could prosecute A privately; but the state does not want maiming or fraud occurring, so it prosecutes A on its own behalf. Modern states do many other things too, but the fundamental functions without which we would not recognize an organization as constituting a "state" are defence (protecting the population from external force) and keeping the peace (forcing the population to behave among themselves). Criminal law is the body of rules of behaviour which the state requires individuals and organizations in its territory to conform to.

One might query whether it is correct to think of criminal justice as a system for resolving conflicts between "two sides", when the state both sets the rules of criminal law and also forces everyone to obey them. The reason it is correct is that our system makes a sharp separation between the organs of state which bring cases against criminals (including the Crown Prosecution Service, and regulatory agencies such as the Office of Fair Trading), and the system of courts and judges which resolves cases. Judges are intended to be neutral between prosecution and defence. Continental legal systems are sometimes called *inquisitorial* rather than adversarial, because there is less separation in their criminal law between the prosecuting and judging roles.

Civil law, on the other hand, is about rules for resolving conflicts between particular individuals and/or organizations, where the state commonly has no interest of its own in who wins, but simply provides a dispute-resolution service. The role of the state as monopolist of force is still relevant, though, since it means that this dispute-resolution service can require the losers to accept its decisions, even if they disagree with them.

Clearly, in practice the ultimate threat of state force commonly remains so far in the background that people do not think about it. Someone arrested for a crime will usually recognise the inevitable and "go quietly". And certainly a business which loses a civil case against another business (and which has exhausted the appeal possibilities which the legal system offers) will comply with the resulting court order, for instance by paying compensation to the winning side. The directors will not sit round the boardroom table saying "If that's what you expect us to do, Queen, just you try and make us!" – it would be absurd. But, if they *did*, and if they persisted in the absurdity, then in the end the state would make them obey, by force if unavoidable. Otherwise, the UK would not be a "state".

For completeness I should mention that the contrast I have drawn between civil and criminal law is a little too neat in one respect: there are many regulations imposed by the state which are enforced through the machinery of civil rather than criminal law. For instance, someone who employs an illegal immigrant, or who fails to produce information needed to set his council tax, faces a civil fine. In this way, respectable individuals can be given a motive for making sure that they obey regulations, without being criminalized if they sometimes fail.

Most law considered in this book will be civil rather than criminal law. That is not because there is no criminal law specially relevant to IT – there is. We have laws relating to downloading or possessing online child pornography, for instance, and laws attempting to control new computer-mediated techniques of fraud, such as phishing. But most of these laws are not very relevant to a textbook like this one.[3] Few computing students plan careers as online fraudsters – and if any do, it is not part of my job as a university teacher to offer them advice! A few computing graduates will go in for careers related to enforcing this area of criminal law, but those students will need a deeper knowledge of law than this book can offer. On the other hand, many computing graduates will work in business, where it will be important to grasp what rights and obligations their organization has vis-à-vis suppliers, customers, and competitors. Some law applying to business IT is criminal law, but the majority is civil law.

Having considered the links which ultimately exist between law, states, and force, it is important to appreciate that law is about rights and obligations, far more than about courtroom battles. In the ideal situation – which most of the time is the actual situation – both parties to a potential conflict of interest know and agree what the law says about their respective entitlements, so they have no reason to go to court. One business might wish that its rights were a bit larger than they are in some particular respect, but it will not be so foolish as to start a lawsuit about it if it knows in advance that it will lose.

Textbooks about law like this one tend to contain a lot of discussion of court cases, which can give the reader the impression that law is all about fighting. That is because courtrooms are where law is visible in action – and also because English law is specially dependent on individual court cases, in a way that we shall examine shortly. But most of the time when a manager needs to look into some aspect of law it is simply in order to check where his business stands. Having found out the position, he will accept it and run the business accordingly, without considering litigation.

2.4 Sources of law

Here, the categories to be distinguished are:

- Common Law
- case law
- Equity
- statute law
- judge-made law

2.4.1 Common Law

For most of English history, most of our law was essentially a body of customs which had evolved among the population from a very early period. It certainly traced back before the Norman Conquest, and perhaps to a time when the tribes which migrated to this country in the Dark Ages had not yet learned to read and write. Different local areas had slightly different customary law; during the Middle Ages, after England had become a unitary state, the differences were ironed out to produce a consistent national system of laws which was consequently called the “Common Law”. Much of the Common Law is still our law today. Disputes relating to information technology often depend on Common Law rules for their resolution.

To grasp how the Common Law works, it is important to understand that its rules evolved in a “bottom-up” fashion among the people, and that they were established as custom before being written down. Since the rules evolved through decisions made in specific disputes, they are often rather un-general – “rules of thumb” rather than abstract logical principles. The Common Law has of course long ago been reduced to writing – the classic written exposition was a four-volume treatise by Sir William Blackstone in the eighteenth century; but such documents are more like summaries of past decisions than plans for how decisions should be made in the future.

English Common Law contrasts in this respect with the legal systems of Continental countries such as France. Continental legal systems are modelled on Roman law, which was formulated as a comprehensive written code. Modern Continental nations naturally have laws which differ in their detailed contents from those of the sixth-century Code of Justinian, but they retain the idea that individual cases are resolved by reference to a written code that aims to anticipate and lay down a logical rule for any debatable issue that may crop up. Modern French law, for instance, is based on the 200-year-old *Code Napoléon* and its sister Codes.

The term used for legal systems modelled on Roman-style written codes is "Civil Law". England and the USA (which inherited its law from England) are said to have "Common Law systems", while France and Germany, for instance, have "Civil Law systems".

Earlier in this chapter, "civil law" was contrasted with "criminal law", to refer to law governing private disputes as opposed to disputes where the state is one of the parties. This is a confusing ambiguity in the language of law. "Civil Law" as opposed to "Common Law" has nothing to do with "civil law" as opposed to "criminal law".

Because the double usage would certainly lead to confusion in an introductory textbook, from now on I shall use the term "Continental-style law" rather than "Civil Law" in the sense opposed to "Common Law". But unfortunately that is just my own coinage; readers who consult other books about law will find that "Civil Law" is the standard term (and one cannot even rely on capital letters being used to distinguish the two senses).[4]

2.4.2 Case law

Human life is so immensely complex that there is no end to the variety of circumstances surrounding individual disputes. When a body of rules of thumb have been worked out through judges settling past disputes, they are sure to leave many questions open about how to apply the rules to cases that come along in the future. One way in which the Common Law achieves a measure of predictability is through the principle "follow precedents". If some debatable issue has been settled one way in a particular case, then whenever a new case crops up that turns on the same issue, it is required to be decided the same way.

For instance, if I help myself to something in your possession, you are entitled to get it back from me – that is age-old law. But what if I can show that the thing was not actually your property but belonged to a third party: does that make a difference? It is not obvious what the answer ought to be. But in a case heard in 1856, *Jeffries* v. *Great Western Railway Co.*, the court decided that the answer was no. Jeffries had some railway trucks which he claimed to have obtained fairly from their previous owner Owen, but the railway company tried to retain them; it knew that Owen had gone bankrupt so that the trucks were no longer his to sell to Jeffries, and it was afraid that Owen's creditors would demand the trucks from the railway company. The court decided that whether or not the trucks belonged to Jeffries, he was entitled to repossess them. Consequently, since 1856 it has been the law that you can reclaim something that was taken out of your control, from anyone other than its true owner.

Courts form a hierarchy, with the House of Lords (that is, the law lords sitting as the supreme court of the UK) at the apex,[5] and it is open to a higher court to decide that a lower court has made a mistake. At a given level, though, courts must follow previous decisions. In this manner, the issues left open by the law as it has evolved up to a given time are settled and closed one after another (though the process will never terminate, because the supply of open questions will never dry up).

The traditional theory was that the Common Law embodied underlying principles which were not spelled out explicitly, but for which an experienced judge would develop a feeling, so that he could see how to apply them to a new case. Judges "discovered" the law case by case. No-one would describe the situation in those terms with a straight face today; we recognise that, when a case has novel features, often it might quite reasonably be decided either way, depending on which analogies with past cases weigh heavier in the judge's mind. But even though the first case of its kind might have gone either way, after it has been decided one way then every future case which resembles it in the relevant respect must be decided the same way.[6]

This means that English law depends heavily on citing particular lawsuits which happened to establish important precedents. As we look at specific areas of IT law, we shall often find ourselves considering details of individual cases. Much of the total body of English law is in essence an accumulation of numerous individual precedents.

This forms another difference between English and Continental law. Because Continental law is based on systematic written codes, the concept of precedent is less important. The theory is that the abstract provisions of the code should be comprehensive enough to yield a definite answer to any question that might arise; a judge ought not to need to look at past cases, because he only needs to read the code.

Of course, that theory is as much a fiction as the English theory that judges "discover" law by reference to unwritten but unambiguous principles. In real life no written code can anticipate every issue that will arise. But because that is the theory, Continental-style legal systems do not have the rule about following precedents. In practice, Continental courts do often take precedents into account in deciding how to resolve awkward cases, but they are not rigidly bound by precedent as English courts are.

The significance of precedent for English law has led to conventions for citing cases which enable lawyers to locate the detailed judgements in the various standard series of published law reports. (The *judgement* in a court case is the document, often many pages long, in which the judge(s) spell out the reasoning which led to his/their decision. Precedents for later cases are distilled from the judgements in earlier cases.) For instance, a full citation of the *Jeffries* case would be "*Jeffries* v. *Great Western Railway Company* (1856) 5 E & B 802", meaning that the report of this case begins on page 802 of volume 5 of "Ellis and Blackburn's Queen's Bench Reports".

For our purposes, full citations would be unduly cumbersome. To keep things simple, cases will be identified by just the names of the contending parties and the date. (The cases mentioned in this book are well-known ones, so a reader who does want fuller information should easily find them in detailed legal textbooks like those listed in chapter 1. Judgements for recent cases are published on the Web.) When one side of a case involves multiple parties, rather than spelling them all out we shall give the first name followed by *& anor* or *& ors* (legal shorthand for "and another/others"). If a date is given as a span of years, say 1980–82, that will mean that an initial decision in 1980 was appealed, and the appeal was decided in 1982.

2.4.3 Equity

The distinction between Equity and Common Law is nowadays only of historical relevance. But it is worth looking briefly at this piece of legal history as an illustration of principles which affect rapidly-changing areas of law, such as IT law, today.

After the Norman Conquest, the Common Law became a settled, nationwide system. But it was a limited system: it provided solutions to some kinds of dispute but not others. One example is that the only remedy it offered to a successful litigant was money compensation. If a defendant failed to meet his obligations under a contract, the plaintiff might want "specific performance" – that is, rather than money he might want the defendant to be made to do what he had actually contracted to do, perhaps to hand over a particular plot of land. Common Law had no mechanism to achieve that.

In consequence, when it was useless to take a dispute to a lawcourt, people would petition the King to redress their various grievances, and the Chancellor (the officer to whom the King delegated this aspect of his work) would decide the cases in terms of what seemed to him fair – not by reference to specific laws, but in the light of his moral intuitions.

That provided a cure for blatant injustices which the law of the time could not deal with. But it was problematic, because people's ideas of what is fair differ. It was said that legal decisions "varied with the length of the Chancellor's foot" – that is, there were no clear settled principles underlying them, different holders of the office would make decisions in unpredictably different ways.

Because this was unsatisfactory, in due course the practice of successive Chancellors crystallized into a set of rules of Equity (i.e. "fairness") which are nowadays just as fixed and explicit as the rules of the Common Law – and which, consequently, do not inevitably yield results in individual cases that everyone would recognise as "fair".

Equity and Common Law are still separate bodies of law, but in modern times the distinction matters only to professional lawyers. The reason why it is worth mentioning is that it illustrates the tension that exists between fair rules and predictable rules. Many of us as individuals tend to feel instinctively that fairness must be the overriding test of good law. If an existing law gives a result in a particular case that seems manifestly unjust (particularly if we ourselves are on the losing side!) then we may feel that the law is obviously bad and ought unquestionably to be changed. The trouble is, we also want the law to give predictability. We want the rules to be fixed and clear, so that we can make our plans knowing where we stand. It is in the nature of fixed rules that there will be individual cases where they give unfortunate results; we cannot have predictability *and* perfect fairness in all cases.

People who run businesses often say that, for business purposes, predictability matters *more* than fairness. The suggestion is that, however arbitrary the rules might be, so long as a well-run business knows what the rules are and knows that they will be applied impartially, then it can find some way to succeed – whereas if laws are applied capriciously there is just no way to manage a business rationally. We shall notice this tension between fairness and predictability when we look at various areas of IT law. It may be that our instinctive preference for fairness above all, while natural and understandable, is not altogether appropriate for this business-oriented area of law.

2.4.4 Statute law

When people say "there ought to be a law about it", they mean that Parliament ought to enact a statute which forbids or requires whatever it is that concerns them. Parliament can introduce Acts on any topic it pleases, and if an Act of Parliament contradicts something in the Common Law then the Act – the "statute" – overrides the Common Law rule.

For most of English history, statute law was a minor component of the total body of law. Acts were passed infrequently, and those that were brought in tended to be for specialist purposes not affecting the population as a whole. For instance, in the eighteenth century, divorces were individual acts of parliament.

That situation has changed dramatically over the past hundred years or so. During that period there has been an explosion of legislation; governments nowadays tend to be assessed by voters (or at least to assess themselves) in terms of the laws they introduce, so they introduce many. As a result, much of the original content of the Common Law has by now been replaced by statute law. Calling England a "Common Law country" nowadays does not mean that the content of our law remains what it was when Blackstone wrote his compendium 250 years ago – that is true only to a limited extent. Rather, it means that the system by which our law adapts to new circumstances is through accumulation of precedents created by decisions in specific cases.

The system of developing law through precedents applies to statute law as much as to the original rules of Common Law. An Act of Parliament is professionally drafted to be as precise and unambiguous as possible, but quite inevitably situations arise after it is passed which were not foreseen by the parliamentary draftsmen, so that it is debatable how the Act applies. In the IT domain this happens particularly frequently, because statutes make assumptions about technology which are overtaken by technological innovation almost before the ink on the Act is dry. When a debatable case comes before a court, the judge decides it as best he can on the basis of the wording of the Act and the need to interpret it consistently with the rest of our law – and then his decision becomes a precedent, so that however ambiguous the relevant wording in the Act may have been before, it ceases to be ambiguous and in future means what that judge decided it meant. The process by which English law becomes increasingly precise through accumulation of precedents is essentially the same process, whether the rule round which precedents accrue is an Act of Parliament or a custom inherited from our Anglo-Saxon forebears.

2.4.5 Judge-made law

In one sense, all case law is "judge-made": judges make the decisions which become precedents. The phrase "judge-made law" is sometimes used in that broad sense. But, here, it is intended in a narrower sense, referring to instances where judges consciously introduce new law.

In the traditional theory of English law, judges were not supposed to do that. They presided over courts and "discovered" rules which (so the theory went) had been latent within the existing body of law; they did not invent new rules on their own initiative. That is Parliament's job; judges are not elected, so they do not have a democratic mandate to impose laws on the population.

However, in recent years there has been a trend – *judicial activism* – of judges openly creating new law.

One well-known example concerns “marital rape”. Under the Common Law, a husband could not be convicted of raping his own wife. What is effectively rape could be prosecuted under other legal categories, such as indecent assault, but if the couple were married then there could be no charge for the specific offence of rape. This had been an established Common Law rule for centuries and was quite clear and unambiguous. A parliamentary committee had in fact considered in 1984 whether the rule should be changed by statute, but decided that the balance of arguments was against the change. However, in 1991 the House of Lords announced that they were changing the rule. Since then it has been open to courts to convict a husband of raping his wife.

Many readers may well feel that this was a good change. What is not so clear, to some observers, is whether it is a good idea for law to be made in this way, independently of democratic control. (Once a judge is appointed, he or she is virtually unsackable; things are set up that way deliberately, so that judges can make impartial decisions without fear or favour.) Whether it is desirable or not, judicial activism is becoming increasingly significant as a source of law.

2.5 Bases of legal authority

Here we need to consider the difference between indigenous English law and EU law; and we shall also look at the "Law Merchant", which until recently was a half-forgotten piece of mediaeval history, but has become newly relevant in the context of information technology.

2.5.1 Indigenous v. European law

Until a generation ago, the Westminster Parliament was the supreme authority over British society. Laws applying in Britain could only be made or unmade by Parliament, or by the subordinate bodies (for instance local authorities, or government departments) to which Parliament delegated certain limited law-making powers.

All that changed when the UK joined what is now the European Union in 1973. EU membership entailed giving the European Commission and Council the authority to make laws applicable EU-wide, including in Britain. If a European law conflicts with an indigenous one, as they often do, the EU law takes precedence. By now a large proportion of all new legislation is European rather than indigenous in origin.

This does not mean that the British Parliament is completely out of the picture in connexion with European legislation. Some EU law does have "direct effect" – British courts apply it independently of any action by the UK Parliament, ignoring any indigenous law which contradicts the European rule. But for the areas of law we are concerned with in this book, that is not the usual situation. When a new law is made for a complex area of life such as business, in order to make sense and function effectively it needs to take account of the large existing body of legal tradition in that area, and must be worded in ways that relate to that tradition. The EU comprises many nations with their own legal traditions, so a statute in a single form of words could not do this. Instead, the EU issues *Directives*, which are instructions to the national legislatures to implement whatever legal effect the EU wants to achieve, by introducing laws that make sense in terms of the respective national legal traditions. So the European laws we encounter in this book will be Acts of the Westminster Parliament, but Acts introduced in response to EU Directives rather than on Parliament's own initiative.

Because of the weight and complexity of existing legal traditions, it is not always easy for a national legislature to devise a way of implementing a European directive that succeeds in giving full force to its intention. What is more, sometimes the national legislature does not agree with the directive, and implements it in a grudging, minimalist fashion. On occasion the European Commission comes back and objects that their directive has not been implemented adequately by some national legislature, so it must try again.

For our Parliament, implementing EU directives can be specially difficult, in view of the difference between Common Law and Continental-style law. The two legal systems lead to statutes of different types. Because Continental law aims to settle debatable questions in advance rather than leaving it to judges to create precedents in individual cases, Continental statutes are drafted in more general, abstract terms than would be normal in English law; and Continental courts are encouraged to consider the motives of the legislators when interpreting statutes – "they passed the law in order to address problem X, so they must have meant to say so-and-so". In the English tradition, that was entirely excluded. A barrier was maintained between the legislature which makes laws, and the judiciary which applies laws, so that whatever motives Parliament might have had for passing a new Act were no concern of the judges – what they worked from was just the actual wording of the Act, together with a general understanding of what words mean in English and familiarity with the existing body of law.

Now that IT-related statutes originating in Brussels are coming into English law, we shall see that this contrast sometimes leads to practical difficulties for English courts, which have to interpret legislation in a manner that conflicts with their training. The European dimension is leading to compromises in legal "styles" (on both sides – the English approach is influencing the European legal régime, as well as the other way round). Where different systems have to compromise with one another, it can be difficult to guess which way particular issues will go. Europe is a factor making currently for more unpredictability in our business law than it might otherwise contain.

As the English legal profession becomes more accustomed to EU legislation, it may be that some areas of our law will lose their national distinctiveness. Already, the idea that everything must be rewritten into English terms is beginning to wear thin. Bainbridge comments (p. 149):

> Where provisions in Directives are required to be implemented without variation, judges in the UK now tend to go straight to the text of the Directive rather than the UK implementing legislation.

But it will be many years, if ever, before English law feels like just a local variant of European law.

2.5.2 Law Merchant

We normally think of law as imposed on society by authority. The English Common Law may have its ultimate origin long ago in tribal customs, but it was a mediaeval king who ordered the local variations to be assimilated into one consistent system and imposed that system as the law of the land. Statute law is decreed by Parliament or by the European Commission.

However, historically, much commercial law was not imposed from above. What was known in the Middle Ages as Law Merchant (often the Latin term *Lex Mercatoria* is used) was created and applied by merchants themselves, without reference to authority. This might sound like a quaint but irrelevant echo of the past; however, some commentators are beginning to argue that the global nature of IT and the internet is leading to the creation of a new digital Law Merchant.[7]

In the Middle Ages, most people stayed put, but merchants travelled from town to town to trade. In many parts of the Continent, jurisdictions were geographically small: each petty principality or duchy might have its own separate laws and courts. If a dispute arose between merchants, they could not hang around for it to be heard by the official court in that place; their livelihood required them to keep on the move. In any case, in societies that were still feudal there had been little development of commercial law. (Mediaeval law contained a mass of detail about land tenure, but not much at all about buying and selling.)

Consequently the merchant community developed its own system of law for settling commercial disputes among themselves. They ran their own courts which came up with instant verdicts, rather than making the parties wait weeks or months for the king's court to stir into action. (In England these rapid-response merchants' courts were called Courts of Pie Powder, from French *pieds poudreux*, dusty feet.) The origins of the law of contract, for business one of the most significant areas of law, lie to a large extent in this "Law Merchant" system, which comprised ranges of explicit legal rules just as ordinary state-backed legal systems do. One might wonder how judgements could be enforced on losing parties if the Law Merchant was not imposed by authority; but merchants needed to go on doing business with each other in the future, so perhaps someone who lost a case would know that any immediate gain from ignoring the decision would be far outweighed by other merchants' future reluctance to trade with him. The fact is that the Law Merchant worked.

In England, which was a large unitary state from an early period, the need for separate merchant law was less than on the Continent, and by the seventeenth century the Law Merchant was absorbed into the ordinary state-backed legal system. Until recently it was little discussed. But the spread of the internet has reawakened interest in it. In later chapters we shall encounter problems that arguably will only be solved satisfactorily through new law developed by the international community of "netizens".

This concludes our survey of the general nature of the legal system. In the chapters which follow, we shall look one by one at the areas of law that matter most to IT professionals.

3. Faulty supplies

The first area we shall examine is what happens when there is something wrong with IT supplies. Nothing created by human beings is perfect, and that generalization is particularly pertinent to the software side of computing: it is a computing cliché that the "last bug" in a sizeable program is never located. What does the law have to say if something goes seriously wrong?

3.1 Breach of contract v. tort

First, we need to grasp a fundamental distinction between two ways in which "things can go wrong": *breach of contract*, and *tort*.

Suppose I am a car dealer and agree to sell you a low-mileage demonstration model, but after I deliver it you find that it is an old banger – someone else might have been happy to buy it, but only for a fraction of the price you paid. You will threaten to take me to court for breach of contract. We all know what a contract is: two parties promise to swap things they can provide and the other wants – commonly, though not necessarily, goods or services in one direction and money in the other. A contract for car purchase will include specific statements about the car, which have not been fulfilled.

But now suppose instead that I am pruning a tree that overhangs my boundary, and I do the work carelessly, so that a heavy bough falls on your new car parked in the road below and damages it. When you complain, you will not be very impressed if I blandly reply "Oh, that doesn't matter – we have no contract, I never promised to take care of your car"! Again you can take legal proceedings against me, but this time for a tort (French for "wrong"). I have done you harm in a way that I am not entitled to do, regardless of whether or not there was any prior relationship between us.

Both contract law and tort law are potentially relevant to IT supplies, and we shall consider each in turn. Under contract law we shall look first at some practical considerations facing a manager responsible for entering into computing contracts, and then at the chief issues concerning how such contracts are interpreted by courts. Under the "tort" heading there will be less to say. There are plenty of ways that unsatisfactory IT products may harm individuals outside any contractual relationship with the supplier; but we saw in chapter 2 that English law adapts to new phenomena through individual cases which establish precedents, and as yet there have been no significant cases about IT-related torts.

3.2 IT contracts

Managers who deal with contracts for IT supplies are often in a difficult situation. Many of them have a strong IT background, but sorting out contractual details is a whole separate ball game, and a difficult one. If, conversely, the manager has a business rather than IT background, his situation may be even worse: how can he foresee what technical points it is important to get down in black and white, if he does not really understand the technology too well? The situation is admirably summarized by Jeremy Holt, in a book which goes into more depth on these issues than the present book could aspire to:

> Pity the unfortunate manager. It has been bad enough trying to get the computer project organized. Now, possibly at the last moment, the contracts have arrived, some with print small enough to make the reader go blind. The manager suspects (rightly) that these contracts are one-sided in favour of the supplier, but knows that the project will only proceed if those contracts (or something similar) are signed. How does the manager work out what needs to be done and from whom advice can be obtained?[8]

IT contracts are difficult both because the law is complicated, and because IT is complicated. To quote Jeremy Holt again, "Among the most common causes of computer project failure are unclear client requirements and unrealistic client expectations."[9] A supplier company's sales representative will of course spend time discussing the client's needs and offering assurances about worries that the client voices (we are considering large-scale business-computing contracts here, not one-off purchases of a PC for home use); but the rep, and his employer, will be hoping that – if the client decides to go ahead – he will sign their standard contract terms. If the customer is willing to accept those, a great deal of expensive time and effort in sorting out the details of a tailor-made contract will be saved on both sides.

As an example of why that saving might be a false economy (for both sides), consider what is believed to have been the first occasion when a case turning on computer software came before a British court: *Mackenzie Patten & Co.* v. *British Olivetti Ltd* (1984). Mackenzie Patten were a firm of solicitors (so should have had more savvy about contracts than the average IT client!) They decided to computerize their accounts, at a period when it was still quite unusual for a non-technical business to use a computer. The Olivetti salesman discussed Mackenzie Patten's needs, and assured them that one of Olivetti's systems would be suitable. Mackenzie Patten leased it and spent considerable time trying to implement the intended functions, but it eventually turned out to be unusable for their specific purposes.

The problematic features were points which the written contract did not cover; so Olivetti may have thought they were in the clear. But in fact the judgement went in favour of Mackenzie Patten, because the salesman's assurances were treated as part of the contract. (Nothing in law says that a contract must be wholly written – indeed, legally it is quite possible to create a contract purely by word of mouth, though to enter into a significant business contract that way might be foolish, to say the least.) Olivetti had to repay the sums paid out by Mackenzie Patten, with interest. Meanwhile, from Mackenzie Patten's point of view the outcome was certainly better than losing the case – but they had wasted a great deal of expensive time and effort, and were presumably no closer to acquiring a system that would do what they needed.

In another similar case the plaintiff[10] could easily lose, perhaps because evidence about what the salesman said was contested and the judge did not accept the plaintiff's version. Sometimes a written contract will contain a so-called *entire agreement* clause, specifying that nothing external to the written document (such as salesmen's remarks) shall be treated as part of the contract – though a clause like that ought to be a signal to the client to make doubly sure that anything important said by the salesman gets written in. (In fact the contract in *Mackenzie Patten* did have an entire agreement clause, but for technical legal reasons the court treated it as inoperative.)

3.3 Letters of intent

With most things a business buys, their properties are understood well enough for the period between initial discussion and conclusion of a contract to be reasonably brief. An IT supplier, on the other hand, will often have to undertake a lengthy development project in consultation with the client, before it has a system ready to meet the client's needs, and both sides' understanding of those needs will be refined as the project proceeds. If the prospective supplier had to do that at its own risk, the expense might be difficult for its business to absorb and it would have an incentive to cut corners. The standard solution is a *letter of intent*: at an early stage in negotiations, the client puts on paper its intention to enter into a contract and agrees to pay for work done by the supplier in the interim – that way, the supplier can afford to make a proper job of exploring the client's needs and developing a suitable solution.

3.3.1 Service level agreements

Another general problem with IT contracts is that points which matter to the client are often details which would be "below the radar" of normal legal language. They need to be right, but they would not fit well within the kind of document a commercial contract is. In any commercial contract it is understood that the thing delivered has to be in saleable condition: one would not normally spell out explicitly that apples must not be rotten, a new car must go, or the like. But, with computer systems, the two sides may well have conflicting assumptions about what is saleable. Consider *Micron Computer Systems Ltd* v. *Wang (UK) Ltd* (1990). Micron claimed that the system it had bought from Wang was faulty, because it did not provide transaction logging. Wang responded that transaction logging was not part of the design specs of that system. On this aspect of the case, the judge sided with Wang and said that if Micron had needed transaction logging it should have made that clear. The essential problem here was that, for one side, mentioning this feature in the contract seemed as redundant as specifying in a car-purchase contract that the motor must run, the doors must lock, and so forth, but for the other side the feature was an optional extra.

The usual solution to this type of problem is a *service level agreement* (SLA): a separate document, referred to in the contract, but written by and for techie types rather than lawyers. An SLA will typically specify things such as technical quality standards, e.g. host/terminal response times, permissible levels of downtime, and so forth; and it will also lay down procedures for *change control*: in a sizeable development project it is certain in advance that specs will be modified in the light of experience as the project proceeds, so there must be agreed processes by which the client is kept up to date on progress and asked to consent to alterations of details. The SLA will lay down how particular departures from agreed service levels are to be compensated, for instance through adjustments to contract price. (The sanction of terminating the contract and claiming damages for breach of contract is an ultimate "nuclear option", not a first choice.)

Developing a useful SLA is itself a challenging task. The danger is that it can become an end in itself, full of metrics that can be objectively quantified but which have little to do with service quality as actually experienced by the client. There are recognised standards that can help. ITIL, the British government's IT Infrastructure Management Method, claims to be "the most widely accepted approach to IT service management in the world".[11] An international standard, ISO/IEC 20000, describes itself as "the first worldwide standard specifically aimed at IT Service Management" (and as "aligned with and complementary to the process approach defined within ITIL").[12] But these general standards are only guidelines; they cannot in themselves produce a suitable SLA for a particular contract.[13]

3.3.2 Governing law

There is no law requiring contracts executed in England to be governed by English law, though that is the default. Sometimes a contract will specify that if a dispute arises, it is to be resolved by a named private-sector arbitration service, such as IDRS or Longworth. Private arbitration has the large advantages of being cheaper and quicker than resolving a dispute in the public court system. For the client it also has a potential disadvantage, though. Arbitration proceedings are private, so the supplier under such a contract does not face the risk that a poor job will lead to adverse publicity. Negative publicity can cost a firm far more than compensating the client in an individual case, so it forms one of the strongest pressures on suppliers to do good work.

3.4 Interpretation of contracts

That is as much as we have space for on the practicalities of IT contracts. The other large issue is how a court will interpret the terms of a contract, if a dispute does arise (and assuming that the contract is governed in the normal way by English law).

Here we shall consider five areas:

- consequential loss
- goods v. services
- implied terms
- unfair terms
- development risk

3.4.1 Consequential loss

If a product (an IT system, or anything else) fails to perform as promised, the law will naturally require the supplier to refund the money actually paid for it. But the failure might have adverse knock-on effects on the purchaser's business. For instance, the purchaser could have been planning to bid for a piece of business which would have been lucrative if the bid was successful, and the failure of the product in question might make it impossible to bid for the work. That would be a very indirect effect (even if the purchaser had been able to put in a bid it might not have won the business), but it could be a serious one.

A supplier will want the contract to exclude liability for indirect (in legal language, *consequential*) loss. If the IT industry is to flourish, it is often reasonable that consequential liabilities should be excluded. IT products are often so general-purpose in nature that it is difficult to foresee the range of uses they might be put to (hence a supplier could not quantify the risk involved in liability for consequential losses); and potential losses will often be large relative to the value of an individual IT contract, so that suppliers could not easily afford to accept liability.

However, an IT supplier needs to appreciate that a court's view of which losses count as direct rather than consequential may be surprisingly broad. A leading case is *British Sugar plc* v. *NEI Power Projects Ltd* (1997–9). NEI supplied power equipment which proved defective, for a cost of about £100,000, under a contract which excluded liability for consequential losses. British Sugar claimed damages of over £5 million because the defective equipment increased their production costs and hence reduced their profits. The court agreed with British Sugar that these losses were direct, not consequential; NEI had to cover them.

The *British Sugar* case related to another area of technology, but the legal precedent applies to our industry as much as to any other (indeed it has already been applied in deciding a subsequent IT-related case). For an IT supplier, then, liability under contract will often be much larger than the supplier might suppose.

3.4.2 Goods v. services

Things traded normally come under the heading either of "goods" or of "services", and often the distinction is clear. A car is a "good", a driving lesson is a "service". Computer software seems to fall in between: should it count as goods or as services?

To an IT expert, the question may seem silly. Software is what it is; if it does not fit these categories clearly, too bad for the categories. But in law these categories are crucial, because the nature of a supplier's liability for defects depends on them. If you supply a service, the law requires only that you act with due care, not negligently. If you supply goods, you have an absolute obligation to supply goods which are reasonably fit for use; if they are not, it is no defence to say "That is not my fault, I had no way of knowing about the defect."

To understand the rationale of this longstanding distinction, think for instance of a doctor, who provides a clear example of a service (even if nowadays, under the NHS, most patients do not pay for it). We cannot demand specific results from a doctor, for instance we cannot insist that all his patients must be cured, though we do expect him to exercise the levels of skill and care that are normal within his profession, and if things go wrong through his negligence he may be sued. Contrast that with a greengrocer, who sells goods. If a greengrocer sells mushrooms which are poisonous, we do not want him to escape liability by saying "I didn't realize there was anything wrong with them." We need the greengrocer to ensure that he sources his mushrooms in a way which leaves him confident that they are safe, and if he is not prepared to do that then he is in the wrong job.

Is the software engineer more like a doctor, or more like a greengrocer? We might feel that a software engineer is much more like a doctor, in terms of the subtlety of the work and the impossibility of ensuring that outcomes are always perfect (and evidently, in terms of legal liability, it is preferable to be a provider of services rather than goods).

But one reason why society is willing to hold doctors only to the standards of care normal in their profession (rather than making absolute demands about outcomes) is that the medical profession defines and enforces high professional standards. Rules are laid down by the General Medical Council, and every now and then we read that some delinquent doctor has been struck off the register of those allowed to practise.

Is software engineering a "profession" in this sense? If so, how are its "normal levels of skill and care" defined and enforced? As we saw in chapter 1, we have a professional organization, the British Computer Society, which attempts to define standards of professional practice; but only some IT workers apply for its qualifications. The BCS maintains a register of Chartered Information Technology Professionals – but I have never heard of it striking anyone off its register, and if it did I am not sure that newspapers would bother to report it.

All this may change. Until it does, we perhaps cannot complain if the law classifies us with greengrocers rather than doctors, and accepts no excuses when software is unfit for purpose.

To date, the legal issue is open: it simply is not settled which side of the goods/service boundary software falls, despite the potential importance of the issue for suppliers. There are classic cases which illustrate how thin this boundary is. A dentist who makes a set of false teeth draws on a great deal of professional skill, and must tailor the work closely to the individual client's needs: but it is settled law that false teeth are goods, not a service. Conversely, when someone commissions a portrait from a painter what he gets is a purely physical object, a canvas covered with pigment: but portrait painting is treated by the law as a service rather than supply of goods.

With software, one can argue either way. When a client commissions a bespoke one-off software system to meet a specialized need, the client is paying for programmers' intellectual skill, not for the physical disc it is delivered on. On the other hand, a standard off-the-shelf software package might seem more like goods, even though (if it is delivered online) nothing physical changes hands. These are two ends of a spectrum with plenty of intermediate cases: for instance, a standard package may be adapted to a certain extent to suit an individual client, or a bespoke software system may be sold not separately but in a bundle with hardware (which is certainly "goods"). The question where software stands with respect to this legal distinction will remain open until future cases establish a body of concrete precedents.

3.4.3 Implied terms

Contracts aim to achieve precision by spelling details out explicitly, but no contract spells *everything* out. It is not possible: there is no limit to the range of considerations that could turn out to matter in some future dispute. One way in which the law addresses this problem is by, in effect, rewriting aspects of a contract which comes before its notice in a dispute. The law will add extra, "implied" terms to those which appear in black and white. (In the next section we shall see that the law may also cross out some of the terms which do appear in writing.)

One type of implied term relates to *business efficacy*: if a contract fails to make commercial sense without additional wording, the court will supply that wording.

An IT-related case was *Psychometric Services* v. *Merant* (2001). Merant contracted to produce software to enable Psychometric Services to run its business online, but the object code delivered by Merant proved not to work adequately. Psychometric Services asked the court to order Merant to hand over the source code, so that (having lost faith in Merant) it could get the system completed by someone else. The contract did not state that the client was entitled to the source code, and a supplier will commonly keep this to itself so as to ensure future business from the client. But the judge noted that the contract bound Merant to maintain its system for no more than two years; after that, if the client had no copy of the source, "none of the inevitable bugs [would] be able to be fixed. No development [would] be possible", and Psychometric Services would almost certainly go into liquidation. That would mean, the judge said, that "the agreement made no commercial sense at all"; so the contract was to be read as containing an implied clause giving Psychometric Services the right to the source code.

Another common reason for adding an implied term will be that the supplier knows how the client intends to use the goods. In that case, even if the contract does not make the intended use explicit, the supplier will be required to supply goods suitable for that purpose.

This is a sensible rule in principle, but in practice it can be hard to say what counts as suitable. A classic precedent was set long before the computer age in *Griffiths* v. *Peter Conway Ltd* (1939). Mrs Griffiths ordered a bespoke tweed coat from the tailors Peter Conway. When she got it, she complained that it brought out a rash on her skin, which was unusually sensitive. Her case was that Peter Conway knew the coat was for her to wear, and this coat was not suitable for her, so they were in breach. But the court decided that there was no breach, because although Peter Conway knew Mrs Griffiths intended to wear the coat herself, they had no way of knowing about her sensitive skin.

With software, problems like this occur in spades. Mrs Griffiths could have warned her tailors about her sensitivity, if she had thought to do so; but in IT, as Rowland and Macdonald put it (p. 138), "at the time when a contract is made, it may be difficult for the parties [either of them – GRS] to accurately define the software required".

By now, courts do understand that under software contracts one cannot require suppliers to get things right first time. That was established in *Saphena Computing Ltd* v. *Allied Collection Agencies Ltd* (1995). Saphena contracted to produce a system for a debt-collecting agency, but their system proved unsatisfactory; the two sides agreed to terminate the contract so that Allied could find an alternative supplier. Allied argued that the inadequacy of Saphena's system put it in breach of contract (so that Allied would be entitled to withhold payment). But in his decision the judge quoted with approval the evidence of an expert witness for Saphena: "no buyer should expect a supplier to get his programs right first time. He … needs feedback on whether he has been successful." Thus it seems that contracts for software will be interpreted as giving the supplier the right to test and modify its system over a reasonable period (which would not always be so for contracts in other business domains).[14]

That point might seem to suggest that a supplier of imperfect software is fairly safe. But the *St Albans* case to be discussed in the next section means that suppliers are not as safe as all that.

3.4.4 Unfair terms

The tradition in English law was almost total freedom of contract. By and large, two parties could agree whatever contractual terms they pleased, and the law would enforce them. This began to change towards the end of the nineteenth century, and the present situation is rather different. The law will refuse to enforce various explicit terms in a contract as "unfair". The statute currently applying is the *Unfair Contract Terms Act 1977*.[15]

Unfair terms fall into two classes. Some terms will be struck out in any circumstances: a clause excluding liability for death or personal injury will never be valid. More interesting for our purposes are cases where some term is regarded as unfair in the context of the particular contract in which it appears.

The motive behind the doctrine of "unfair terms" is society's wish to make bargaining power more equal as between the "little guy" and big business. However, the effects of the law extend more widely.

Take the case of *St Albans City and District Council* v. *ICL* (1996). ICL was then the leading UK computer supplier (it has since been taken over by Fujitsu), and it supplied St Albans with software to calculate the poll tax (the unpopular system of financing local government which operated for a few years before being replaced by the council tax that we know today). Poll tax was charged at a set rate per head, decided annually by each district council. A council knew what its total budget was, so it arrived at a figure for poll tax by dividing that total by the number of taxpaying residents. Unfortunately, ICL's software contained a bug which had the effect of overestimating the St Albans population, meaning obviously that the poll tax figure was set too low. The loss to the council was £1·3 million.

The contract limited ICL's liability for software faults to whichever was less of the price paid for the software, or £100,000; so St Albans would have been seriously out of pocket. But the court struck this limitation out as unfair, and ICL had to compensate the council fully. Grounds for the judgement of unfairness included the following (as well as some other points we shall not go through here):

- ICL was an organization with more resources than St Albans (which was true, though a city council in South-East England is not most people's idea of a "little guy");
- ICL had product liability insurance under which it could claim, whereas (according to the judge) one could not expect a local authority to insure against commercial risks (a number of commentators wondered "Why not?" – but the judge was the judge);
- St Albans had tried to renegotiate this particular clause, but being up against a tight deadline they did not succeed. By law, a council must send out its annual tax demands by a certain date, so St Albans had to have some system in place by then.

So, although the law recognises that bugs are unavoidable, if a bug has particularly expensive consequences an IT supplier cannot always rely on a cautiously-worded contract to protect it from those consequences. What counts as "unfair" has an unavoidable element of subjectivity. The trend of unfair-terms decisions related to IT has been so adverse to suppliers that by 2001 the profession was asking "Do the Courts have it in for the IT industry?" (Since that date, Jeremy Newton sees signs that the tide may have turned somewhat in favour of suppliers.[16])

3.4.5 Development risk

If courts have appeared unduly harsh towards software suppliers whose products are less than perfect, this may be partly because the law has not appreciated how much innovation and unpredictability is involved in our industry. Many IT professionals may feel that it would be quite unreasonable to treat an unsuccessful software system as proving that the developers of the system must have been culpably negligent: it is not like building a bridge, where the engineering issues have been settled for some time and perhaps a qualified bridge designer really does not have much excuse if his construction collapses. To quote Rowland and Macdonald (p. 235):

> An important consideration for a technologically advanced industry such as the software industry is the legitimate concern that innovation should not be stifled by legal rules. Designs for systems that are "at the cutting edge of technology" may not have been tried and tested in the same way as a more pedestrian project, and the industry owes its success to its ability to create and market new methods of control or new systems and products.

Perhaps the law ought to regard a measure of what is called *development risk* as inescapable.

However, computing is not the only industry which innovates, and the law has taken a hard line with other industries where innovation has proved dangerous. Rowland and Macdonald cite *Independent Broadcasting Authority* v. *EMI and BICC* (1980), a professional-negligence case which eventually reached the House of Lords, stemming from the collapse in 1969 of the television transmitter on Emley Moor near Huddersfield. In its day the Emley Moor mast was one of the tallest freestanding structures in the world, designed in an innovative way by BICC (now Balfour Beatty) and built by EMI (which used to be a manufacturing as well as a music company). It was brought down by a combination of ice and high wind. Defending themselves against the accusation of negligence, BICC

> argued vigorously that a finding of negligence would be likely to stifle innovation and inhibit technological progress. They produced evidence that there was neither any available source of empirical knowledge nor agreed practice; they were "both at and beyond the frontier of professional knowledge". (Rowland and Macdonald, *loc. cit*.)

The Lords did not accept this as an excuse, and found that BICC's design was negligent. Quoting the judgement:

> The project may be alluring. But the risks of injury to those engaged in it, or to others, or to both, may be so manifest and substantial, and their elimination may be so difficult to ensure with reasonable certainty that the only proper course is to abandon the project altogether …

By good luck, when the Emley Moor mast fell no-one was hurt – but they easily might have been. Thus the supreme court of the UK has laid down that where such risks exist, innovation is not a defence against the allegation of negligence: what a responsible professional is expected to do is to refrain from embarking on the project.

One way of looking at this is that development risk may be inescapable, but the law wants the risk to be borne by the people who practise the innovative technology, not by their clients or by third parties. IT practitioners ought to be in a better position than others to evaluate IT risks and decide whether they are too great to proceed.

Nowadays IT is being deployed in many safety-critical applications. So far there seems not to have been an IT case analogous to *IBA* v. *EMI and BICC*, but this is surely only a matter of time. Our profession may often be oblivious to the legal risks it is running in this area. If you design a transmitter mast, you cannot fail to be aware that you are dealing with a tall and heavy construction exposed to all weathers, whereas computer code tends to insulate those writing it from the physical realities it is destined to control.

3.6 Torts

Mention of safety-critical applications brings us to the issue of torts. Because no-one was hurt at Emley Moor, there were no tort cases; BICC, EMI, and the IBA were in contractual relationships with one another, whereas if a passer-by injured by the collapse had sued one or more of these parties the case would have come under the "tort" heading. IT is used routinely nowadays in applications such as fly-by-wire aircraft, or computer-controlled administration of drugs in hospitals. What would the legal situation be, if bugs in the relevant software caused an aeroplane to fall out of the sky, or a fatal overdose to be administered to a patient?

At the time of writing, there has been no new statute law relating specifically to IT-mediated torts, and, what is quite surprising, no significant cases have come before the courts yet. So anything said about how existing tort law will be extended to cases where IT is crucial can be only educated guesswork.

3.6.1 Strict liability for products

Consider for instance the *Consumer Protection Act 1987*, which implemented the requirements of the European *Product Liability Directive*. Before that Act, an individual who was harmed in some way by a product could take the retailer to court under the contractual relationship between them (whenever you buy so much as a bag of crisps, legally speaking you and the shop are creating and fulfilling a contract); but it was not easy for an individual to take legal action against the manufacturer, since there was no contractual relationship between manufacturer and consumer and to establish a tort it would have been necessary to prove negligence by the manufacturer. Yet the manufacturer might often seem the appropriate target for litigation. If its products are harmful, it is the manufacturer rather than retailer which is in a position to cure the defect or withdraw the line from the market; and, if the harm is serious and calls for a serious level of compensation, the manufacturer may have deeper pockets than a corner shop.

The Consumer Protection Act has the effect of imposing "strict liability" on the producer of a product. No longer is it relevant whether the producer acted in a blameworthy way; to render the producer liable, one need only establish a causal link between a defect in the product and the damage arising.

For our profession, the question then arises whether a software system is a "product"; legal experts have discussed this at length. It sounds like the same question as whether software is goods or a service, but "goods v. service" is a distinction rooted in English law. Because the Consumer Protection Act implements a European directive, it has to use the separate European legal concept of "product". As things stand, we do not know for sure whether software counts as goods, and we do not know whether it counts as products either, but when relevant decisions arise it could turn out that the answers to the two questions will be different.

Jane Stapleton suggests that the European legal system is likely to interpret "product" widely, to include software even if English law classifies it as services rather than goods, because the fallible human activity which is the hallmark of services is "masked" in the case of software. When a customer visits a hair salon she physically witnesses the stylist exerting professional skill, whereas it is hard to see past pages of program code to the programmer toiling in his cubicle.[17] Evidently, for the welfare of our profession we should hope that software does *not* count as a European "product", but the question is impossible to decide *a priori*: we must wait to see which way courts go.

If software is counted as a product so that the Consumer Protection Act creates strict liability for damage caused by bugs, there will be a further issue which is perhaps more problematic for IT than analogous issues would be in other domains. What counts as a "causal link" between a software bug and damage arising in connexion with it?

Rowland and Macdonald (pp. 222–3) refer to the notorious 1980s episode in Canada and the USA when faulty software led the computer-controlled Therac-25 radiotherapy machine to administer excessive doses of radiation to a number of cancer patients, killing some of them.[18] In this case the causal link is clear, but what (Rowland and Macdonald ask) if the bugs had happened to work the other way, so that patients received too little radiation? Then, some of the patients would have died from cancers that could have been cured. Legally speaking, would there be a "causal link" between the software defects and the deaths – or only between the cancers and the deaths?

3.6.2 "Development risks" in the case of torts

In one respect, our Consumer Protection Act explicitly differs from the corresponding laws in some other EU countries, although all were introduced to implement the same Directive. The European Directive gave EU member states a choice over whether or not to include a "development risks" defence in their implementing legislation: if a product turns out to be harmful, is the producer allowed to escape liability by arguing "that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered"?[19] On the one hand, not allowing that defence "might discourage scientific research and the marketing of new products". On the other hand, allowing it might leave the new legislation fairly empty.

Some EU countries did not include a development risks defence in their implementation of the Directive. The UK did include it, and in fact the form of words in our Consumer Protection Act is so broad that the European Commission took proceedings against the UK for failing to implement the Directive properly. (However, those proceedings failed, and the Consumer Protection Act stands.)

This might suggest that British law will be reasonably merciful to producers of software which does unforeseen harm (even if software is counted as "products"). But development risk is about things that in some sense push the boundaries of current human knowledge. Very often, when software bugs cause harm, this will not be because of limits to our scientific knowledge about the consequences of any specific bug, but merely because it is so difficult to locate and eliminate every last bug in a complex program. Each individual bug may be recognisable as an error once it is found, but no matter what régime of testing is applied before the package is released, some bugs are missed. How much testing does it take to discharge one's legal responsibilities?

We saw, above, that English contract law accepts that some bugs are inevitable. But we are discussing tort law now, where harm is done not to trading partners but to third parties; and in this area, while there are no IT-related precedents as yet, what precedents do exist suggest a much tougher line.

A frequently cited case is *Smedleys Ltd* v. *Breed* (1974). This was not in fact a tort action but an appeal against a criminal prosecution under the *Food and Drugs Act 1955*; and that Act has been superseded by newer legislation. But neither of these points are seen by commentators as necessarily important; the case set a standard for the required level of quality control with respect to risks to third parties.

Mrs Voss bought a tin of Smedleys' peas at Tesco's, and opening it she found a green caterpillar among the peas. The resulting case went as far as the House of Lords, which accepted that Smedleys carried out extremely thorough mechanical and manual testing to guard against foreign bodies in its food production; statistically speaking they achieved an impressively tiny incidence of complaints. (In the judgement, Lord Hailsham also pointed out that even if Mrs Voss had not spotted the caterpillar, being thoroughly cooked it would have done her no harm – she "could have consumed the caterpillar without injury to herself, and even, perhaps, with benefit.") But none of this got Smedleys off the hook. The conviction they were appealing against was upheld, because if they had examined that caterpillar during the testing process they could have recognised it.

In other words, *no* amount of testing is sufficient, if it leaves some individual defects which could be recognised as defects in the current state of human knowledge. It is irrelevant that the overall incidence of defects may be as low as current technology permits.

The analogy with software testing is uncomfortably close. Even if it is accepted that the "last bug" in a program can never be found, that fact looks unlikely to help a software developer whose undetected bug leads to a tort action. Indeed, Lloyd (p. 569) argues that the law will see the software developer's liability as specially clear. A caterpillar is a natural object, but "With software, the producer is put in the position of creator … the producer cannot disclaim knowledge of his or her creature's properties." So, at least, the law may assume.

4. Intellectual property

4.1 The growing importance of intangible assets

Readers will appreciate that the concept of *property* is crucial for business. A firm needs to know what it owns (and can therefore use freely, and/or charge others who want to use it), and what belongs to others (so that if it needs to use those things it must do deals with their respective owners). Business looks to law to define property rights and enable them to be enforced.

Before the IT revolution, the things over which firms needed to assert ownership were usually tangible things – goods, land, and so forth. The law of "intellectual property", under which for instance a company might own a patent on a newly-devised industrial process, was a fairly obscure legal backwater. Information technology has changed this, by hugely raising the profile of intangibles. Ever since the Industrial Revolution, the economies of nations like Britain and the USA had been dominated by manufacturing. But by the late 1980s, the share of GDP (gross domestic product) attributable to manufacturing fell below half in both nations, and it has continued to fall – outweighed partly by growth in services, but also by growth in trading of intangibles.

By now, intangibles form a large proportion of the assets of a typical firm, as measured by the prices which the market sets on them. Gordon Brown, then Chancellor of the Exchequer, said in 2006:

> Twenty-five years ago the market value of our top companies was no more than the value of just their physical assets. Today the market value of Britain's top companies is five times their physical assets, demonstrating the economic power of knowledge, ideas and innovation.[20]

What Brown was saying was that most property of the "top companies" is now intellectual property. It is largely IT which has brought about this change; and it naturally means that intellectual property law has become a very significant area of business law, which is having to develop in response to developments in the technology.

The topic which might perhaps come first to a student reader's mind is the way that sharing music over peer-to-peer networks has been undermining the copyrights owned by music companies, which have been struggling either to invoke the law to defend their position, or to develop novel business models that allow them to make money within the new technological environment. But for present purposes, this area is not actually very significant. The law of copyright as it applies to music is clear; the only change introduced by IT lies in making the law easy to break and hard to enforce. More interesting, for this textbook, are areas where the property itself (not just the means used to reproduce it or move it around) consists of things like computer software or electronic databanks. In those areas, it is often far from clear how the existing laws of intellectual property apply. Courts are adapting laws that were written long ago for other purposes in order to develop an intellectual-property régime for the IT industry, and so far this is not working too well.

The issues are not about enforcement – unlike with music filesharing, where many of the individuals involved do not care whether their activity is legal, provided they feel safe from detection! In civilized societies, most organizations by and large aim to keep within the law and respect one another's property rights – but they need to know what those rights are. It would be hard for a business to be profitable, if it made a habit of not insisting on rights which it did legally possess.

4.2 Copyright and patent

There are two longstanding legal devices for defining and protecting different sorts of intellectual property: copyright, and patent. Copyright was originally introduced to define ownership in "literary works", such as novels, poems, or non-fiction books, but came to be extended by analogy to things like musical compositions, films, and so forth. Patents relate to newly-invented machines or industrial processes.

Neither copyright nor patent law was part of the Common Law; both devices were introduced by statute. (Indeed, the USA has had a general law of copyright only since the 1890s – it was a standing grievance for Victorian novelists that no sooner did the fruits of their labour emerge from the press than American publishers' agents would rush single copies across the Atlantic, where they would be reprinted and sold without reward to the author.) The original motivation of both copyright and patent law was the same: they were intended to stimulate advances (in literature, and in industry) which would benefit society, by creating concrete incentives for the innovators.

The kinds of protection offered by the two areas of law are different. Copyright is something that the author of a "literary work" acquires automatically in producing the work, and it forbids anyone else to make a copy of the work (for a set number of years into the future, and with various provisos that do not matter here) without the right-holder's permission. Thus an author's copyright is a piece of property which he can sell or license for money; in the case of books, typically a publishing company contracts with an author for permission to publish his book in exchange for royalties paid to him on copies sold. With newer media such as films, the business models are different, but the underlying law (which is what concerns us) is essentially the same.

A patent, on the other hand, is not acquired automatically by the inventor (or anyone else). Taking out a patent is a complicated and expensive undertaking, but if a patent is granted, it forbids anyone (again, for a set future period) from exploiting the process or mechanism without the patent-holder's permission; so again the patent is an economically-valuable piece of property, which can be sold or licensed to companies wanting to use the innovation in their business.

The legal contrast between copyright and patent was neatly summed up by Tim Press:

> A document setting out a novel chemical process would attract copyright protection, but that protection would protect the document against copying, not the process from being carried out. A patent for the process would prevent it from being carried out but not from being written about or broadcast.[21]

Computer programs are "text" which defines and controls "processes". So on the face of it there is a question about which kind of intellectual-property protection is more relevant to software. Over the years during which IT has been economically important, the answer has been shifting.

4.3 Do we need intellectual-property laws?

Before we look at how intellectual-property law is being adapted to the needs of our industry, it is worth taking a moment to recognise that quite a few people are sceptical about whether such laws are needed at all. Society has changed since these laws were introduced. The inventor of a useful industrial process will nowadays not typically be a lone genius who needs income from his patents to keep afloat: he will be a salaried researcher, working for a company which will be best placed to exploit his invention whether or not its competitors are legally forbidden to do so. Some commentators point to the numerous books which are written essentially for love of writing rather than for money, and to the success of the Open Source movement in producing software systems (such as Gnu/Linux) which are made freely available to all comers, and they argue that intellectual-property law as a whole has outlived its usefulness.

Others who do not go that far argue that legal protection is specially undesirable for computer software, because it interferes with the ways in which software advances. Tim Berners-Lee has expressed this by saying "Programming is always about reassembling existing stuff – novel ideas are rare".[22] To those who see things this way, legal protection for software creates progress-stifling monopolies rather than socially-desirable rewards for innovation.

A third group accept that there is a need for intellectual-property laws in our field, but they argue that trying to generate such a body of law by adapting copyright and/or patent law is not going to work – from poetry or Newcomen's Atmospheric Engine to Java is just too great a stretch. They argue for *sui generis* laws, that is, new kinds of law which do not extend existing concepts of copyright or patent but introduce some third, separate type of protection. (*Sui generis* is Latin for "of its own kind".) We shall see that in one area (databases) this argument has now prevailed.

On the whole, though, the consensus seems to be that the IT industry does need a régime of legal protection for intangible property, and that most of this protection will have to come via development of existing intellectual-property laws. People who suppose that the best way of dealing with a novel phenomenon must surely be through brand-new laws often fail to appreciate the massive amount of work and time needed to develop adequate legal frameworks from scratch. Some features of existing law may be inappropriate for the new area, but the body of case law and statutory revision which builds up round established legal concepts over the years will comprise a great deal of material which applies just as well to the new area as to older areas. By adapting existing law, society gets all that legal predictability for free.

4.4 Copyright for software

The initial assumption was that software should be protected by copyright rather than patent law. After all, what a programmer produces is lines of source code, usually on paper at first: this has at least a superficial resemblance to a "literary work", but it is not at all like a physical machine. In English copyright law, the term "literary work" has no implication of aesthetic value – a user manual for a microwave oven counts as a "literary work" as much as a Shakespeare sonnet.

For a while there was debate about the status of a program after it was compiled into object code, when it was likely to exist only in electronic form rather than on paper – was object code still protected by copyright law? But Parliament settled this question with the *Copyright, Designs and Patents Act 1988*, which among other things laid down that for legal purposes computer programs in any physical form are literary works. Hence there is now no doubt that copyright law does apply to software. If firm A develops a valuable software application, firm B is not free just to copy and use the application, without negotiating a license fee with firm A.

However, this protection is less robust than it might seem. Remember that copyright law is only about *copying*. Imagine that I had never read the Harry Potter novels, but wrote a novel out of my own head which just happened to be word-for-word identical with one of those books. Then, in theory, I would be free to sell my book and compete for a share of J.K. Rowling's income; I have copied nothing. Of course, in practice, no court would allow this; but that is because the chance of identical manuscripts being composed independently is so tiny that the law would assume I *must* have copied. With software, though, scenarios rather like this are more realistic than they are with novels.

Consider (1) a case where I take someone else's program and mechanically substitute new names for each variable – wherever, say, *myvar* occurs it is replaced by *varA*, and so on with the other variables. Variable names are arbitrary, so the new program will behave exactly as the old one does, and it is not an identical copy. Would copyright law allow this?

The literary analogy might be to publish a novel identical to one of J.K. Rowling's, except that "Harry Potter" is changed to "Jimmy Cotter" throughout, "muggles" are consistently replaced by "poggles", and so on. British copyright law is clear on this: it protects the plot of a novel, not just the words, so J.K. Rowling would win a breach of copyright case. Analogously, just changing the variable names in a program would not be a defence against an action for breach of software copyright.

But now consider cases where the copying is less direct:

(2) While working for firm A, I developed a program to carry out some task; having moved to firm B I write a new program from scratch for the same task, using the same techniques as I remember them, though without access to my old code. (Note that copyright in my old program will belong to firm A, not to me. Although I said above that copyright is automatically acquired by the author of a "literary work", that is not true when the writing is done as part of an employee's duties: in that case copyright belongs to employer rather than author.)

(3) Working for firm B, I examine the behaviour of a software system owned by firm A and write code to emulate its behaviour, but without access to the source code from which firm A's object code was compiled.

In these cases, the analogy with literature does not tell us whether there are breaches of copyright or not. (The literary analogue of (2) might be a case where I read a Harry Potter novel and then try some time later to reconstruct it from memory: the law would very likely not care about that, because the result would just be a laughably clumsy novel which would do nothing to damage J.K. Rowling's sales.) What is more, not only is it unclear what copyright law *does* say about these cases, but it is not obvious what we *want* the law to say. Society does not want to see producers of worthwhile software ripped off, but it does want to encourage fair competition.

4.5 Two software-copyright cases

To see how copyright law is being applied in practice, we must look at cases. An example like (2) above was *John Richardson Computers Ltd* v. *Flanders* (1993). Flanders was a programmer who worked for John Richardson's company as an employee and later as a consultant. He helped Richardson to write a program allowing chemists to print prescription labels and keep track of their stocks of medicines; the program was in assembly code for the BBC Micro (a popular home and small business computer of the 1980s). After leaving John Richardson Computers, Flanders wrote a program in QuickBASIC for the IBM PC to execute the same functions, and he set up a company to market this program.

Clearly, there will be no character-by-character similarity between a Basic program and one in assembly code. Any similarity would be at the level of the logic of the various routines – something that cannot be compared mechanically, but requires human understanding to detect. Richardson's side argued that the logical similarities in this instance did make it comparable to copying the plot of a novel, so that it amounted to breach of copyright. But on the whole that was not accepted by the court. The judgement was complex, but (to cut a long story short) it said that while "non-literal" copying of software might in principle be a breach of copyright, in this case there were only a few minor infringements.

A case like (3) was *Navitaire Inc.* v. *EasyJet Airline Co. & anor* (2004). Navitaire developed a reservation system for airlines, "OpenRes", which EasyJet licensed to use in its business. Later, EasyJet wanted to own the software it relied on, so it commissioned another software house to develop a system "eRes" to emulate OpenRes. The two sides agreed that "EasyJet wanted a new system that was substantially indistinguishable from the OpenRes system … in respect of its 'user interface' ". Again the court decided that eRes did involve some minor infringements of Navitaire's copyright, but the overall weight of the decision went in favour of EasyJet.

So the trend is clear: extended from "literature" to software, copyright law protects software producers against little more than direct, character-by-character copying. That level of protection is important in itself; it is copyright law which is invoked when people or organizations are convicted of using pirate copies of valuable proprietary software, or of uploading such software to P2P networks such as KaZaA. (Since 2007 the law has taken a tough line against software piracy, with new powers for Trading Standards officers to investigate suspected breaches and more serious penalties than before for convictions.) But copyright is not providing much defence against subtler ways of misappropriating programmers' intellectual output.

Incidentally, discussions of this area in law textbooks often confuse two different kinds of similarity between programs. After Apple commercialized the first GUI (graphic user interface), it objected when competitors produced their own GUIs with a similar "look and feel". For instance, having chosen to represent the "Trash" concept with a dustbin icon, Apple objected when others did the same (which is why some systems use a swirly "black hole" for the same concept). Without entering into the legal complexities of the look-and-feel arguments, this issue is rather separate from the question of copying program structure. Copyright in "look and feel" is rather like copyright in artistic images – the fact that in this case the graphic material is acting as gateway to a computer system has limited relevance. Copying the logical routines of a program, on the other hand, is something which relates exclusively to IT; and copyright law is not providing strong protection against it.

4.6 Databases

Commercial electronic assets comprise not only the software which processes information, but the databases of information to be processed. (The word "database" is ambiguous. It can refer to a DBMS – database management system – such as Oracle; a DBMS is itself a software application. But I am using "database" here to refer to the collection of pieces of data which a firm uses a DBMS to store and process, for instance a large collection of details of potential customers, or the geographical data assembled by the Ordnance Survey to generate its maps.) The IT revolution has turned databases into big business. A Department of Trade and Industry minister said in 1997:

> Estimates of the size of the UK database market range up to £10 billion but even that may be an underestimate … It is growing at more than 11 per cent. a year.[23]

Although English copyright law has protected databases as "literary works", they are as far as they could be from literature in the everyday sense. We have seen that our law did not care about that. But the corresponding laws in some other EU states did: German copyright law, for instance, applies only to documentation having at least some minimal aesthetic or scientific value. Consequently the EU introduced special *sui generis* intellectual-property protection for databases via a *Database Directive*, transposed into UK law in 1997. Under this, the copyright protection which had applied to databases in Britain was explicitly withdrawn in cases where the database is a purely mechanical listing of facts without intellectual content (e.g. a phone directory); those databases are now protected by new legal rules independent of both the copyright and the patent régimes.

Unfortunately, the new rules are not very clear. This was illustrated by the chief case so far brought under them in Britain: *British Horseracing Board & ors* v. *William Hill Organization Ltd* (2001).

The Horseracing Board keeps a database of horses and jockeys due to run in particular races. Maintaining it is a significant commitment, costing about £4 million to add or update about 800,000 entries annually. Naturally the information is important for betting firms like William Hill, and for many years they used it without objection. However, when the World Wide Web arrived and William Hill began displaying information taken from the Horseracing Board's database on their website, the Board claimed unauthorized reuse of their data.

When the initial decision was appealed, the Appeal Court found it necessary to ask the European Court of Justice for rulings on eleven questions about precisely what the Database Directive was intended to mean. (This is a standard procedure for European legislation; it contrasts with the English legal tradition, where a law means just what the words say and courts are supposed to do any necessary interpretation for themselves.) The upshot, based on the ECJ's rulings, was that what was crucial to the Board's property rights was the "stamp of authority" it could associate with its data by virtue of its role as governing body of the sport. A betting firm could never confer that stamp of authority on racing data, no matter how much it copied from the Board's database; so the verdict went in favour of William Hill – it had not and could not take over the crucial feature of the Horseracing Board's intellectual property.

Before 1997, the Board would have won the case under British copyright law. So, ironically, it seems that a Directive which was introduced in order to strengthen the protection of databases has actually reduced their protection (in some respects, at least) in Britain – and British databases are believed to account for about half of all databases in the EU.[24]

4.7 The focus shifts from copyright to patent

Returning from databases to software: we saw that the profession initially looked to copyright rather than patent law to protect intellectual-property rights in software. More recently, though, patent law has begun to seem more relevant. This is for three reasons:

- copyright protection is proving inadequate
- the software industry is changing
- patent law is expanding its scope

Let us take these points in turn.

4.7.1 Copyright protection inadequate

We have seen that the trend in software cases has been to interpret copyright as covering little more than character-by-character copying – which is often not what is at issue in practice. Patent law, on the other hand, does not care whether anything has been *copied* or not. If A holds a patent on a mechanism or process X, then B is forbidden to use X (without A's permission) *even if B really did invent X independently*. What matters, for patent law, is which of A or B applied to the Patent Office first. If A is granted a patent on some programming technique – let's say, an efficient sorting algorithm – then anyone else who wants to use that technique must pay A for the right to do so, even if he has never heard of A or A's work.

So patent law offers the prospect of a more worthwhile level of protection for intellectual property in software than copyright law is providing.

4.7.2 The software industry is changing

In the early decades of industrial and commercial computing, a firm wanting to computerize some of its operations would typically buy the relevant hardware, and employ in-house programmers to develop software to automate its particular activities, or commission an outside software house to develop a bespoke system for its individual needs. Before the 1980s, the concept of standard software applications was scarcely known. But, as readers will be well aware, things have changed. A high proportion of all commercial software nowadays consists of standard application packages carrying out standard functions, with copies of the same package often being used by hundreds or thousands of different client organizations. Recent developments such as SaaS (software as a service)[25] are accelerating this trend.

That makes patent protection for software more economically attractive than before. It takes effort and expense to take out a patent, and for a one-off system this would often be pointless. It is not very likely that an outsider could study its details closely enough to adapt it for use elsewhere, and even if that were feasible, adapting the system to the different individual requirements of the new organization might be almost as expensive as producing a new system from scratch. But, once software applications are standardized and widely-used commodities, the balance changes. Spread over perhaps thousands of copies of a package, the cost of a patent becomes trivial; and the danger of a competitor emulating the package becomes much more realistic.

4.7.3 Patent law expanding its scope

From these points it may seem self-evident that someone wanting to protect his rights in novel software would be in a stronger position under patent than under copyright law; why would anyone bother with copyright law in the first place? But the attraction of patent law is irrelevant, if patent offices will not grant patents on software; and until recently that was the position. However, this has been changing. We need to look at the rules under which patent offices operate.

4.8 The nature of patent law

Countries have their own patent offices; but in the 1970s European countries agreed a European Patent Convention which aimed to harmonize patent rules across Europe, and established a European Patent Office (EPO) as a one-stop shop issuing patents valid in different European countries. (This is not an EU creation – the signatories to the Convention include non-EU countries such as Switzerland; and what the EPO issues are bundles of separate patents valid in separate countries – there is no such thing as a single Europe-wide or EU-wide patent, though the idea has been discussed.) Someone wanting a British patent can apply either to the EPO or to the Intellectual Property Office (as the UK patent office is known).

In discussing the legal systems of Western nations, much of the time we find Britain grouping with the USA and contrasting with the Continental European countries. Because of the Convention, patent is exceptional in this respect: British law resembles the laws of European nations and (as we shall see) contrasts in some important respects with American law. The UK *Patents Act 1977* aimed to implement the agreed principles of the European Patent Convention.

In order to patent an invention, one has to submit a *claim* showing that it meets a number of requirements. (Here I refer to British law, but these requirements are similar in any national patent law including that of the USA.)

- the invention must be genuinely new, so far as *public* knowledge is concerned;
- it must not be obvious – there must be an "inventive step";
- it must be capable of industrial exploitation;
- it must not fall within a class of things which the law explicitly excludes from the scope of patent, which includes intellectual matters such as ideas or scientific discoveries, as opposed to industrial processes which exploit ideas or discoveries. Someone who invents a novel sorting algorithm would never be allowed to patent it – it is an idea rather than an industrial process; on the other hand, a machine which uses the algorithm to sort filecards could well be patentable. The EPO glosses the ideas v. processes distinction by saying that the invention must be "technical", in the sense that it involves some tangible end product.

When someone applies for a patent, an official called a *patent examiner* sets out to check whether the requirements are met. This is not straightforward: the test of novelty (lack of *prior art*, in patent-law lingo) implies attempting to prove a negative. Since patent examiners cannot be omniscient, they sometimes make mistakes and issue patents that ought not to be granted. The grantee's competitors can challenge a patent, for instance as not genuinely new, and if they make their case the patent will be revoked.

A patent on an industrially-significant process can be a valuable piece of property. It forces would-be competitors either to abandon attempts to compete, or to do things in some different way which may be less efficient, or less appealing to customers.

4.9 Is software patentable?

Where does software stand in all this? In Britain and elsewhere it was seen as more analogous to mathematical formulae or abstract algorithms than to physical machines or processes. The Patents Act explicitly lists, among the class of things that are not patentable:

> a scheme, rule, or method for performing a mental act, playing a game or doing business, or *a program for a computer* (my italics)

That is why people initially tried to use copyright law to protect their software; and one might think that it leaves no room for debate – patent law is just irrelevant to the software business.

However, the Act has a loophole. The article immediately following the one just excerpted goes on to say that the list of unpatentable things

> shall exclude patentability … only to the extent to which a [patent claim] relates to such subject-matter or activities *as such*. (Again my italics.)

So the question arises: would a patent for software which executes process X be a patent for the "software as such", or would it be a patent for process X? If the former, the patent would not be valid; but if the latter, it might be.

This is a good example of an issue which a scientist, a computer specialist, or another non-legal mind might well dismiss as a non-question. How could one possibly decide that an application relates to "software as such" rather than to the process which the software carries out? But the Patents Act is part of the law of the land, so lawyers are not allowed to treat the issue as meaningless and empty – even if it is. Cases are being fought out to give it a meaning. The trend of the decisions is towards increasing willingness to grant patents for software. Unfortunately, the trend is also turning this area of law into a very messy one indeed.

4.10 Some software-patent cases

To exemplify that last point, consider three patent claims from a period of a few years about the turn of the century.

4.10.1 PBS Partnership/controlling pension benefits system (1995)[26]

In 1995, the Pension Benefit Systems Partnership asked the EPO for a patent on a software system which calculated pension benefits. The EPO refused the claim, not because it related to a program – the combination of computer hardware and software was deemed to be "a physical thing of a technical nature", hence in principle patentable – but because of the nature of the "inventive step": since pension benefits can be (and traditionally were) calculated manually as a purely clerical activity, the inventive step in this case was deemed non-technical, hence the claim failed. (The hardware was technical, of course – but the hardware was not novel.)

4.10.2 Fujitsu's Application (1996)

In 1996 the English courts upheld a refusal by the UK patent office to grant a patent on software which enabled chemists to display and manipulate crystal structures on screen. Part of the reasoning was that what was novel in this claim was the ability of the user to choose how to rotate a three-dimensional crystal structure one way or another, but this act of choice is a human rather than mechanical activity – one cannot patent "mental acts", though one can patent "processes methods or apparatus based upon such acts", quoting the judge who upheld the refusal in the Court of Appeal.

The judge went on to illustrate this distinction from a more concrete sphere of activity:

> Rules as to the planting of potatoes in which the operator is instructed to measure and evaluate matters such as the type of soil, location, weather and availability of irrigation is a method for performing a mental act [and hence unpatentable]. Directions to plant one seed potato every metre is not. It is a precise process.

As Lloyd remarks (p. 332), this way of drawing the boundary round patentable processes seems paradoxical. One could easily imagine that a computer-controlled potato-planting machine might incorporate routines to take account of soil type, irrigation, and so forth. Apparently, this level of sophistication would prevent the machine being patented, while a simple machine that plants at regular intervals could be patented if novel; yet the sophisticated machine would surely be "more … deserving of protection".

4.10.3 Microsoft Corp./Data transfer with expanded clipboard formats (2003)

A few years later, the EPO granted Microsoft a patent on a type of clipboard operation within Windows which allowed data in one format to be copied into an application that is based on some other format, for instance a graphic copied into a plain ASCII file. Microsoft's claim opened with the words "A method in a computer system …". Yet the EPO accepted that this was not a claim for a "computer program *as such*", which (as we have seen) would have made it unpatentable. They saw it as a novel technical process for making data available across applications, and granted the patent.

Perhaps the reader thinks he can see differences between these examples which might justify the different outcomes of the claims; but, if so, it would be easy to quote further examples to convince him that a consistent logic just is not there. Discussing another claim which was granted in 1994, Tim Press comments "The reasoning of the [EPO] Board in finding (as they did) technical content in the *Sohei* case is at times impenetrable".[27]

By now, the situation is such a morass that in 2006 the English Court of Appeal announced that Britain should abandon the attempt to follow precedents set by the EPO and go its own way: it is impossible to follow EPO precedents, because the EPO is not following its own precedents consistently.

(Part of the problem here stems from the contrasting attitude to precedent in English versus Continental legal systems, discussed in chapter 2. Continental law treats precedent as persuasive only, rather than binding, so the charge of inconsistency might not seem so damning in the eyes of Continental lawyers as it does to English lawyers. But the fact remains that there is no clear basis at present for deciding whether some commercially-valuable new software might be patentable.)

The Court of Appeal's "declaration of independence" bore fruit in 2007, when the UK Intellectual Property Office refused to activate a patent that had already been granted by the EPO to Symbian for a software system which enables other software to run faster (*Mapping dynamic link libraries in a computing device*). The UK IPO saw this as clearly excluded from patentability by the law which both it and the EPO are supposed to be applying; and when the High Court allowed Symbian's appeal, the IPO counter-appealed – making it clear that its motive was simply to get some clarity about what rules it is meant to work by. (In 2008 the Court of Appeal gave its verdict in favour of Symbian, urging that the British and European patent offices should try to compromise with one another's ways of working where possible – while agreeing that the law on software patents is vague and inconsistent.)

4.11 The American position

Meanwhile, in the USA, software patents have become wholly normal. Before 1998, the American rules about unpatentability of computer programs were similar to ours, but in that year *State Street Bank* v. *Signature Financial Group* established a radically new precedent, allowing a patent on a software system for administering and keeping accounts for "mutual funds" (the US equivalent of unit trusts). Under English law, such a system would have been doubly unpatentable. Not only is it a program rather than a machine, but what it automates is "business methods" – the kind of processes carried out manually by clerical workers, rather than technical, industrial processes. Before 1998, business methods were unpatentable in the USA also, but since *State Street Bank* that rule has been abandoned; very large numbers of patents are being granted on business-process software.

This expansion of American patent law is being amplified by a separate development, independent of IT: excessive workload is leading the US patent office to grant many patents which it shouldn't, on "inventions" which are obvious, or not truly new. When patent examiners reject a claim, they have to justify the rejection with solid argument, but it is a straightforward matter to accept a claim. So, inevitably, when a patent office is overwhelmed by numbers of claims the outcome is that too many are granted. (A classic example is US Patent no. 5,965,809, granted in 1999 for a method of determining a woman's bra size by running a tape measure round her bust.) In the case of software, "prior art" is specially difficult to check, which exacerbates the problem. Consequently software patents, even for trivial-seeming techniques, are now very usual in the USA.

4.12 An unstable situation

The American patent situation creates pressure on Europe to move the same way: it is difficult, when the economies of the two regions are as closely bound together as they are nowadays, for their patent régimes to be widely different. And the fairly chaotic current nature of European patent law makes this pressure hard to resist (even supposing Europeans want to resist it). By now, the European Patent Office is in practice granting many software patents and refusing few claims in this area. Yet, on paper, it remains the law that one cannot patent "a program for a computer".

One way to regularize the situation would be for the law in Europe to be brought into line with practice, by explicitly abandoning the rule which says that programs are not patentable. The European Commission proposed a *Directive on Software Patents* which would have done that. But this Directive proved highly controversial and, to the surprise of many observers, in 2005 the European Parliament overwhelmingly voted it down. They were swayed by arguments of the kind quoted from Tim Berners-Lee above. Many people see the likely effect of software patents as being to stifle rather than encourage valuable technological progress; they urge that software patents would merely confer "licences to print money" on Microsoft, Amazon, and the like.

These are weighty considerations. On the other hand, we saw in chapter 2 that predictability is valued by business. At present, whether or not a patent claim for a software system will succeed is far from predictable.

Meanwhile, public opinion in the USA has been building up against the consequences of the *State Street* decision. In 2008 a decision was issued by the US Federal Circuit Court of Appeal (on the case *in re Bilski*) which looks likely to rein in the patentability of business methods and software programs in America, though it is too early to say what the future US patent régime will be like.

All in all, the best answer one can give to a question about software patentability, in England or in the Western world in general, is: watch this space!

5. Law and rapid technical change: a case study

English law has long tried to suppress pornography, though the boundaries to what counts as criminally obscene have fluctuated down the decades. One can debate how far the law ought to intervene in this area. Some would argue that looking at porn is a private thing that does not harm others, and may even do some good by providing a form of sexual release for lonely men who might otherwise pester women. Others urge that porn harms women in general by promoting a degraded perception of their status. Most people who see no harm in adult porn would regard porn involving children as a special case, since making it brutalizes the children involved.

For the purposes of this book, it is not necessary to discuss the moral rights and wrongs of outlawing porn, or where the boundary should lie between legal titillation and illegal obscenity. The reason to look at the topic here is that it offers an unusually clear case study of the difficulty law has in adapting to rapidly-changing technologies. We saw in chapter 2 that this is one respect in which IT law is a distinctive area of law. The case study will also illustrate the way in which law has to interact with highly technical matters through the woolly medium of everyday language. Language is not a precision instrument, but it is all we have; law has somehow to make language precise despite itself.

Circulating pornography was a crime under the Common Law, but this is one of the many pieces of Common Law which was eventually superseded by statute law. The chief statute covering the porn trade is the *Obscene Publications Act 1959*.

5.1 Film versus video

When the Obscene Publications Act was passed, obscene publications came either as what we nowadays call “hard copy” – books and magazines printed on paper – or as reels of cine film. (Showing a film to members of the public is “publication”: to “publish” something just means to make it public, not necessarily using ink on paper.) The first big technical innovation for porn after the Act was video recording. When video technology arrived, the porn industry was glad to adopt it. (For one reason, if you trade in illegal goods it is obviously convenient for their nature not to be apparent from a casual inspection, as it might be to anyone who looked at a few frames of a cine film.)

So it came as an unwelcome shock to the authorities when the first case under the Obscene Publications Act relating to videotapes, namely *R.* v. *Donnelly & ors* (1980),[28] was thrown out by the Crown Court judge who heard it, not because the films were not obscene but because they were not films. Donnelly and his fellow defendants had rooms in Soho where they showed blue movies to paying customers. Because their technology involved displaying pictures on a television screen controlled by electrical impulses generated from a videotape, rather than shining a light through successive frames of a cine film, the attempt to prosecute them failed.

The Obscene Publications Act forbids publication of an "obscene article" (or possession of an obscene article with a view to publishing it for gain), and it defines the word "article" in the following words (here labelled **A** for ease of reference later):

A

> In this Act "article" means any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures.

To a non-lawyer that sounds pretty comprehensive, and it is obvious that when Parliament passed the Act they would have wanted it to cover blue movies irrespective of the recording technology used. Nobody would dispute that. But under English law, what Parliament might have wanted is irrelevant. What matters is the wording of the act they passed. If judges were allowed to say "it is obvious that X would have been made illegal if anyone had thought of X when the law was drafted", the next step would be for them to say "it is obvious to me that X ought to be illegal, so I find you guilty" – and the law would become whatever individual judges happened to want it to be.

After the prosecution case in *R.* v. *Donnelly & ors* was presented, the defence made three points:

1. a videocassette is not an "article" in the sense of the Obscene Publications Act;
2. the showing of the videotape was exempt from prosecution, under wording in the Act (not quoted here) relating to films shown in ordinary commercial cinemas;
3. alternatively, since the display technology was the same as that of television broadcasting, the display was shown "in the course of television", which would again exempt it under other wording in the Act.

Each of these points requires explanation. Point (2) relates to the fact that films are already controlled in Britain through the official censorship system which awards the familiar certificates (U, PG, X, and so forth) and refuses any certificate to some films. Because Parliament saw this as an adequate means of controlling the film industry, it did not want also to burden that industry with the possibility of prosecutions brought by individuals who happened to object personally to particular films; so the Obscene Publications Act was worded to disallow that (except in special circumstances not relevant to this case). Likewise with (3): television at that period was produced just by the BBC and one national authority for commercial television, and in 1959 their internal safeguards were presumably seen as making private prosecutions for obscenity on television redundant.

As for (1): the defence pointed out that law requires an "or other" phrase, such as "any film *or other* record of a picture or pictures" in passage A, to be interpreted narrowly. It is a standard principle of English law that the "other" things in a list like this must be understood as covering only things of the same kind as whatever appears before "or other". So for instance if a statute refers to "houses flats or other buildings", then "other buildings" in this context will cover other types of dwelling, but not, say, churches – this is one of the ways in which the law achieves precision and avoids open-ended vagueness despite the inexactness of the English language.[29] But a videocassette is not the same physical kind of thing as a film, so it is not an "article" as defined by the Act.

The judge agreed with point (1), which meant that whether points (2) and (3) were right or wrong, the prosecution must fail. He directed the jury to find the defendants not guilty.

5.2 The Attorney General seeks a ruling

If this Crown Court decision had stood as a precedent, it would have meant that there was no possibility of prosecuting pornography that used video technology (which soon became the standard medium for porn films), short of new legislation by Parliament; and Parliament never has enough time for all the big things it wants to do, let alone filling in strange little gaps in wording of statutes which it has already passed.[30]

The defendants in this particular case had been acquitted and there could be no question of reopening that. But when the Attorney General (the officer in overall charge of criminal prosecutions) believes that an acquittal may have been mistaken in law, he can seek to prevent it becoming a precedent to be followed in future cases, by asking the Court of Appeal to rule on the legal point. The Court of Appeal is above Crown Courts in the hierarchy, so it can overrule a precedent they set. The acquitted defendants can choose to be represented in such a referral, and on this occasion – *Attorney General's Reference (no. 5 of 1980)* – they were represented. The gap in the law was highly advantageous to their business, and they evidently hoped to keep it that way.

At the Court of Appeal, Donnelly et al. were represented by a new advocate, who took a rather different line from the argument which had brought them success in the Crown Court. He focused on another passage in the Obscene Publications Act, which defines "publication":

B

For the purposes of this Act a person publishes an article who –
(a) distributes, circulates, sells, lets on hire, gives, or lends it, … ; or
(b) in the case of an article containing or embodying matter to be looked at or a record, *shows, plays or projects* it. [Italics added]

Clause (a) of passage B did not apply in this case – the videocassettes were not handed over to the customers; and, the advocate argued, clause (b) did not apply either. The customers were not "shown" the videocassettes: that would be pointless, there is nothing to see except magnetic tape whose contents are invisible. The advocate argued that the videocassettes were not "played" either; the court accepted that what mattered was how ordinary words like "play" would have been understood "by ordinary literate persons" at the time the Act was passed, and by that criterion (the advocate contended) "play" would apply only to a sound recording. The word that would certainly apply to a cine film is "project"; and that means (he claimed) projecting light behind the film to throw an image onto a screen. Nothing like that happens with video technology.

The three Appeal Court judges did not accept this argument. Their judgement conceded that the videocassettes had perhaps not been "shown", but the words "play" and "project" were both appropriate to the new technology. A tape recorder also uses magnetic tape whose contents are invisible to the eye, and it is said to be "played" (though the judgement seems not to have considered the claim that "play" refers in ordinary parlance to sound recording only). As for "project", etymologically this word means "throw forward", and video does involve throwing a beam of electrons against the coated screen of a cathode ray tube to create the picture.[31] The Court of Appeal found that the Crown Court had misinterpreted the statute; in consequence, future prosecutions similar to *R.* v. *Donnelly & ors* could lead to convictions.

But it was a close-run thing. Although no-one would ever seriously suppose that Parliament could have wanted to outlaw obscene cine films but allow the same films on videocassette, the Act they passed succeeded in outlawing both only because of tiny points about how "ordinary literate" people use words in everyday speech.

5.3 Pornography meets the internet

Technology does not stand still. Another major development for the porn industry was the internet. It is obvious that distributing porn via the internet, so that men can access it in the privacy of their homes, will create a large new market among those who would hesitate to visit sleazy sex shops.

Indeed, although it is not often discussed, the truth is that after the internet was made available for commercial use in the early 1990s, the porn industry were pioneers in developing business models which function successfully with this medium. Again, the technical innovation has created problems for the law.

The problems as they existed when the internet was first commercialized were surveyed in detail by Colin Manchester.[32] Manchester concluded that, without new legislation

> legal control is likely to become increasingly ineffective as computer pornography becomes more prevalent and replaces videos as the dominant medium for the dissemination of obscene material

Although there are also other statutes relating to pornography (for instance a law specifying what imported material should be confiscated by the Customs), much of Manchester's analysis related to the Obscene Publications Act, including the interpretative precedent established by the Attorney General's reference to the Court of Appeal in 1980. Let us look at why Manchester felt that the internet was making it difficult to prosecute under that Act.

Internet porn involves data held on hard discs and transmitted over phone lines. So a first question is whether a hard disc, or the data on a disc, counts as an "article" in the sense of passage **A**. We saw that the Crown Court judge in *R.* v. *Donnelly & ors* accepted that a videocassette was not an "article" for these purposes, because it is not a thing similar to a film and hence by the strict rules of legal interpretation cannot be included under the description "any film or other record of a picture or pictures". Since the Court of Appeal declared the Crown Court decision to be erroneous, it might seem that by implication that Court accepted that a videocassette *can* be an "article" – in which case perhaps there would be no reason not to extend this word to cover a hard disc also. For Manchester, though, it was not entirely certain that the Court of Appeal finding did have that implication; the judgement did not make it crystal clear that this was the appeal judges' reason for overturning the Crown Court decision.

But in any case, to convict someone for distributing porn over the internet it might be necessary to establish that the information on a hard disc, rather than the disc itself, counts as an "article" – we saw that the defendants in the videocassette case did not hand over the videocassettes to their customers, and certainly hard discs do not travel physically over the internet. Manchester saw it as by no means clear that the information on a disc could be an "article containing or embodying matter to be read or looked at", which is one of the alternative definitions in passage **A**, because "information is intangible whereas 'article' here suggests something of a tangible nature". The data on the disc *might*, on the other hand, come under one of the two other definitions: either "any sound record" (if it is porn with a sound track rather than pictures alone), or "any film or other record of a picture or pictures" (if the Court of Appeal decision is taken to establish that "or other" in this context does not have to mean only "things like films").

From a computing point of view, it may seem that the linguistic difficulties stem in part from the choice of the words "information" or "data" to describe the contents of a hard disc. The information on a disc is of course organized into files, and it might be much easier for the law to accept that "a file" can be "an article" than to accept that "information", which does not sound like something that comes in well-defined units, can be "an article" or "articles". Computationally, it will seem absurd that this kind of choice between words could have important implications. But, for the law, it can.

5.4 Are downloads publications?

Be that as it may, even if the law accepts that internet porn, or the discs on which it is stored, count for the Obscene Publications Act as "articles", that would be only a first step towards satisfying the requirements of the Act. There also needs to be *publication*, or an intention to publish for gain.

If the obscene article is the disc itself, then Manchester thought it unlikely that making its contents available over the net would count as "publishing" the disc. Under the (a) clause of passage **B**, the disc is not distributed, circulated, sold, or the like; it remains attached to its fileserver. And under the (b) clause, one would not describe making the contents available for downloading as "showing", "playing", or "projecting" the disc itself.

On the other hand, it may be more appropriate to talk about "publication" of an obscene article if the "article" is the information on the disc (or part of it). To make the disc contents available for downloading could be described as "distributing" or "circulating" it (clause (a)). Admittedly, the data travels not directly to the user but only to a client computer – Manchester pointed out that the user still has to access it, but he argued that this is only like the fact that someone who receives porn through the post has to unwrap the package containing it in order to see it. The law would not treat that as contradicting the proposition that the porn has been published to the user.

Actually, one might think that this last point is not the real legal problem: on the Web, someone who downloads a picture to his machine normally does see it immediately without taking further action. But the downloading is initiated by the user, whereas words like "publish", "distribute", and so forth sound like actions by the person controlling the server. However, the Web was still fairly novel when Manchester was writing, so it may be that he was thinking of other methods of transferring files over the internet, such as ftp.

As for clause (b) of passage **B** with respect to information on the disc, Manchester suggested:

> it might be said that a person "projects" the information onto the receiving computer, when transmitting it electronically, in that the information is thrown forward or thrown onto the receiving computer through the medium of the telephone line. Secondly, it might be said that a person "projects" the information when, having transmitted it to the receiving computer, it is displayed on the visual display unit (VDU) attached to that computer.

Thus, although the words "show" and "play" do not fit this case, Manchester believed that "project" probably does (though, again, he ignored the point that it is not the owner of the hard disc who initiates the download).

5.5 Censoring videos

All in all, while Manchester believed it was possible that a court would interpret the Obscene Publications Act as covering internet porn, he felt far from certain. And with another, more recent statute also concerned (among other things) with the control of pornography, the *Video Recordings Act 1984*, Manchester found it fairly clear that it would *not* cover what was then the latest technology.

The point of the Video Recordings Act was to subject videos, other than innocent home and educational videos and the like, to a censorship régime such as already operated for cinema films, with X-rated videos being restricted to licensed sex shops, and some videos refused any certificate. (Part of the problem in *Donnelly & ors* was that, in 1980, censorship did not extend to videos.) To achieve this, the Act had to identify the class of things to which it applied; it called them "video works", and defined that term as follows:

C

"Video work" means any series of visual images (with or without sound) –
(a) produced electronically by the use of information contained on any disc or magnetic tape, and
(b) shown as a moving picture.

That is, both (a) and (b) must be true of an item before the Video Recordings Act says anything about that item.

But Manchester pointed out that, by the 1990s, video games were beginning to be stored on chips rather than discs or tapes, in which case clause (a) of passage **C** would not apply and they would not be covered by the Act. Furthermore some newer computer games and videos, including pornographic ones, were interactive: a series of still pictures is shown, and the user makes changes to the pictures displayed. These are not "shown as a moving picture" (clause (b) of **C**), so the Act would not catch them either. Yet Manchester was writing only about a decade after the Act was passed.

5.6 The difficulty of amending the law

None of the gaps in the law which Manchester identified would be difficult to cure (he felt) with brief amendments to the relevant statutes. The Parliamentary committee dealing with home affairs had recommended some changes in 1994, and Manchester suggested others. But we have seen that Parliamentary time is scarce. It just is not possible to amend a law whenever a problem is found in its wording.

Furthermore, it might not be hard to devise wording to deal with technological innovations that have *already occurred* – but, by the time Parliament has gone through the careful, long-drawn-out procedures to incorporate those amendments into the law, technology will have changed again. It is now over ten years since Manchester was writing, and the pace of innovation in IT has probably been even faster over this period than it was before.

5.7 *R. v. Fellows and Arnold*

Manchester could only surmise how the Obscene Publications Act and the other laws he discussed would be interpreted in connexion with internet porn. What ultimately matters is how courts actually do interpret them. So let us now look at the leading internet-pornography case, which was heard the year after Manchester's article appeared: R. v. Fellows and Arnold (1996).

Fellows was a member of the computer support team in a university department, and he used its equipment to maintain an "archive" of thousands of pornographic pictures accessible over the internet by password; he supplied the password to people who contributed further material to the archive, Arnold being one of these. The archive included a child-pornography section, so Fellows and Arnold were prosecuted under the Protection of Children Act 1978 as well as under the Obscene Publications Act. They were convicted in the Crown Court, whose judgement answered some of the questions raised in Colin Manchester's article, but not all of them – as he pointed out in a second paper.[33] The defendants appealed, and the Appeal Court judgement made detailed references to points raised in Manchester's second article, giving us an unusually complete "audit trail" of the gradual development of legal certainty about a novel phenomenon.

5.8 Allowing downloads is “showing”

So far as the Obscene Publications Act is concerned, we recall that one crucial issue was whether the obscene article had been “shown, played, or projected” (see passage **B**). The Crown Court judge decided that it had.

Counsel for Fellows had taken up the point which Manchester’s earlier discussion had seemed to ignore: he argued that “showing” means something more active than just letting someone else download from a server. He asked: suppose a picture was left out on a library table and someone made the library key available, would that person be said to have “shown” the picture to another person who used the key and looked at the picture? The advocate evidently expected the answer “no”, but the Crown Court judge held that “to give the key to someone who the donor knew would use it to enter the library in order to look at the picture would amount to a showing when the viewer did exactly that.” And the Appeal Court judges agreed. They accepted that “show” might require active conduct by Fellows, but

> it seems to us that there was ample evidence of such conduct on his part. He took whatever steps were necessary not merely to store the data on his computer but also to make it available worldwide … He corresponded by Email with those who sought to have access to it and he imposed certain conditions before they were permitted to do so. He gave permission by giving them the password.

So making pictures available for downloading is, legally, "showing" the pictures (at least if the person who puts the pictures on the server actively controls access to them in the various ways described in the quotation above – it might perhaps still be argued that someone who merely makes a picture freely available to all comers on the Web has not "shown" them the picture). Since these pictures were "shown" in legal terms, the law did not need to decide whether they were also "projected".

For the Appeal Court judges, the other issue which Manchester had seen as crucial, namely whether the "obscene article" in a case like this is the disc itself or the data on the disc, did not seem to arise. The defence argued that "it could not be said that the article, namely the disc, was shown, played or projected"; the response in the Appeal Court judgement was "the data stored in the disc was 'shown, played or projected' … within the ordinary meaning of those words", and there was no explicit awareness of the possibility that these two quoted statements could both be true. (The Court of Appeal did not refer to Colin Manchester's earlier paper, which had discussed this issue at length. His second paper, which the Court did refer to, mentions it only briefly, mainly in order to point out that in future cases it might cease to be an issue, because a new statute had introduced more clarity on this point.)

So not only is it unpredictable how a debatable issue will be resolved, but it can even be unpredictable which issues will be seen as requiring resolution.

5.9 What is a copy of a photograph?

So much for the Obscene Publications Act. But we saw that *Fellows and Arnold* involved child pornography, which is covered by a separate statute, the *Protection of Children Act 1978*; and here too the defence found ways of arguing that technological change had made the law inapplicable.

Some of the points were the same. The issue whether allowing people to download pictures amounts to showing them the pictures arose under both statutes. (The Crown Court judge in fact developed his "key to the library" analogy in connexion with the charges under the Protection of Children Act, though by implication he applied the analogy equally to those under the Obscene Publications Act.) But the Protection of Children Act offered further possibilities for defeating the prosecution.

This Act makes it an offence to possess "any indecent photograph of a child … with a view to [its] being distributed or shown by himself or others …", and it specifies that:

D

> references to an indecent photograph include an indecent film, a copy of an indecent photograph comprised in a film … references to a photograph include the negative as well as the positive version.

The defence argued, first, that what was stored on the server (though it was derived from photographs) was not itself photographs.

The Crown Court judge consulted a standard English dictionary, which defined a "photograph" as "a picture or other image obtained by the chemical action of light or other radiation on specially sensitised material such as film or glass", and he agreed that what was on the disc was not "photographs"; as the Court of Appeal judgement put it, "There is no 'picture or other image' on or in the disc; nothing which can be seen."

However, passage **D** covers not only an original photograph but also "a copy of an indecent photograph". Oddly, at neither hearing is the defence recorded as having discussed the immediately following words, "comprised in a film"; the defence line, rather, was that if the disc contained copies of indecent photographs, the law would apply, but it did not contain that. The original of a photograph, by the dictionary definition, is the photographic negative. (Bear in mind that in 1996 neither the dictionary nor the Court of Appeal were thinking about digital cameras.) Passage **D** specifies that a positive print taken from a negative also counts as a "photograph". A photocopy of a print, looking more or less the same as the print, would be a "copy of a photograph"; but a set of 0s and 1s on a hard disc (it was argued) is not a copy of a photograph.

The Crown Court judge rejected this suggestion that " 'a copy' must mean a copy which can be seen and appreciated to be a copy without any further treatment", drawing an analogy with the kind of secret writing that children used to do (and perhaps still do) with lemon juice:

> At one time it was quite common to use invisible ink which would become visible on heating. If, using such ink, the words of a document were repeated, would that be a copy? Even though the words could not be deciphered without heating the ink, there would, in my judgment, be a copy.

The Court of Appeal agreed that the wording of the 1978 Act did not limit the meaning of "copy" in the way suggested by the defence.

But the defence argued that newer legislation did imply such a limit. The *Criminal Justice and Public Order Act 1994* had included a section amending passage **D** in the Protection of Children Act to make the term "photograph" explicitly include "data stored on a computer disc or by other electronic means which is capable of conversion into a photograph". If the 1994 Act found it necessary to say this, the defence urged, then under the 1978 Act (which was what was in force when the alleged offences were committed) the word "photograph" must *not* have included "data stored on a computer disc …". To a layman it sounds like a telling point.

The Court of Appeal rejected it, on the basis of reasoning which was logically very subtle. If a given statute refers to X and Y, and X is capable of being understood either in a broad sense which would include Y as a special case, or alternatively in a narrow sense in which it contrasts with Y, then the legal rule is that the mention of Y will be a reason for taking X in the narrow sense – otherwise it would be redundant to mention Y. If we set X = "copy of a photograph" and Y = "data stored on a computer disc", it might look as though the reference to Y requires us to interpret X narrowly as not including data on a computer disc. But in the present case we are not dealing with two passages in the same statute. According to the Court of Appeal, once the 1994 statute was in force, wording Y in that statute might impose a narrow interpretation on wording X in the 1978 statute *as it applied in the future* (though this would make no difference in practice, because activities previously prosecuted under the 1978 statute would now be prosecuted with more certainty under the 1994 statute). However, the later statute could not affect the proper interpretation of 1978 wording as it applied to activities *before the later statute was in force* (as in this case).

Otherwise, Parliament in 1994 would have been legislating retrospectively – it would have been laying down new law to apply not just from that time forward but back into the past. Retrospective legislation is normally regarded as taboo and a characteristic of tyrannical régimes (since it is impossible for individuals to ensure that their actions are legal, if the actions come first and the law is invented later). The Westminster Parliament has very occasionally legislated retrospectively, but this is always controversial and therefore widely discussed – there was no hint at all that the 1994 Act was intended to function retrospectively.

5.10 Uncertainties remain

The defence had further arguments which we shall not examine here; they were weaker, and all were rejected by the Court of Appeal, which upheld the convictions. Readers may well feel that they have seen quite enough of *Donnelly & ors* and *Fellows and Arnold* already; they may suspect me of heaping up tiny details in order to exaggerate the difficulties which technological change poses for the law. If so, let me assure them that I have not done that. On the contrary, I have tried to set aside all the inessential issues raised in the various hearings, in order to focus just on the main points which illustrate the real nature of the problems. (I could easily have made this chapter *very* much longer, without looking at any further statutes or cases!)

Furthermore, although both of these cases led eventually to the law being declared to be what Parliament doubtless wanted it to be, either case could easily have gone the other way – the videocassette case did, initially. And although some doubts which IT has created have now been resolved, there will surely be others.

For instance, in *Fellows and Arnold* all the discussion of "copies" was about cases where the copied pictures were identical to the originals, as far as possible given the limits of the technology. But nowadays most home computers come with image-editing software which makes it easy to modify photographs, in ways ranging from simple adjustments to contrast or colour balance, to sophisticated modification of pictorial content. Porn merchants might well want to apply this technology to their stock in trade – probably they already do. Is an indecent picture which has been deliberately altered to look different from the original still a "copy" of the photograph?

The 1994 Act defines a concept of *pseudophotograph* for "an image, whether made by computergraphics or otherwise howsoever, which appears to be a photograph", so people cannot escape conviction by saying that their pictures never involved the use of a camera. But what if a photo is processed to look like an oil painting with visible brushstrokes, in the style of the Impressionists or of the Old Masters? – that takes just a mouse click within an image-editing package. For some porn users, by creating an atmosphere of gentility surrounding the obscene content this could add to the thrills. Is an indecent photograph which has been edited so that it does *not* "appear to be a photograph" still a photograph or pseudophotograph, for the purposes of the laws on obscenity and child protection? So far as I know no relevant case has yet come before the courts.

5.11 The wider implications

A point to make about this case study is that the difficulties which the law encountered in catching up with technology depended in part on the fact that we were looking at criminal rather than civil law. One established principle for interpreting the language of statutes is that in criminal cases, where individuals are threatened with loss of liberty, wording must be construed particularly narrowly in the defendant's favour. It might be difficult to find an area of civil law where technological change has been creating quite so many clear illustrations of legal obsolescence – though the same sort of thing does happen in the civil law, if less frequently.

Another point is that this is one respect in which Continental-style legal systems may be better placed than ours. Because the Continental approach is to write laws in terms of broad principle and to encourage judges to "fill in the gaps", interpreting written statutes by reference to the purpose of the legislation as much as to the precise wording on paper, difficulties comparable to those we have studied in the case of computer pornography might well be less likely to arise on the Continent.

The English tradition has seen the "purposive" Continental approach to law as mildly shocking and not really appropriate for a free society: since states have so much power over their subjects, that power needs to be tightly restrained, with individuals who wield a share of state power (such as judges) allowed as little discretion as possible about how they use it. Now that Britain is in the EU, our legal establishment has had to compromise with Continental-style approaches in areas where the EU is making law, but it has not found the compromises easy. (Laws about obscenity, and indeed most of the criminal law, remains a field where Britain and the other EU member states retain their independence.) The episodes examined in this chapter, though, suggest real advantages in the Continental approach. Views differ about how far pornography should be criminalized; but most people will agree that if some activity is objectionable enough for society to outlaw it, then we do not want people to escape conviction merely because of changes in society's technical infrastructure.

Lastly, the main lesson to draw is about the contrasting timescales of law and IT. Some statutes we have looked at were risking obsolescence because of technological development within a decade of being drafted. For the law, ten years is not a long time – and it should not be. A society in which laws changed overnight whenever someone in authority spotted something amiss, with no time for in-depth consultation of knowledgeable parties, careful consideration of possible knock-on consequences, and so forth, would be an uncomfortable society to inhabit (to put it mildly). But, for information technology, three or four years ago is "the old days". Think back ten years, and it is hard to remember what our technology was like at that prehistoric period.

This tension between contrasting timescales makes IT law a distinctive area within law as a whole.

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.

7. Web law

We turn now to aspects of IT law which relate specifically to the internet, and mainly to the World Wide Web. We shall look at four topics:

- contract formation in internet trading
- the right to make links
- ownership of domain names
- Web 2.0 and defamation

7.1 The internet and contract

7.1.1 Trading needs contracts

Trading at a distance is surely the leading function of the Web for most businesses. (Its function as an information source is also important, though far less productive of legal issues.) Suddenly, many delays and difficulties associated with finding a suitable supplier and agreeing terms, using traditional communication channels, have been electronically annihilated.

For buying and selling, the central area of law is contract law. We have already seen that, in the eyes of the law, even the most trivial consumer purchase involves creating and fulfilling a contract. For trading to function smoothly over the Web, it is essential that the technology should not get in the way of the legal process of contract-formation – otherwise there would be business chaos, with individuals and organizations not knowing what their commitments were or who actually owned particular goods. When one buys a tin of beans in a corner shop, these issues are self-explanatory; with larger-scale transactions – particularly so-called “B2B” (business-to-business) trading, the total value of which is much larger than that of business-to-consumer retailing – they are not. The respective parties’ commitments will often be far more complicated than “you give me this thing and I give you £X”. The parties need to be clear about just how far their legal commitments extend; if one side is disappointed, the other side needs to know whether it was legally obliged to do better. The stage at which ownership of goods is legally transferred may be crucial, for instance to determine when the purchaser needs to take responsibility for insurance coverage. Readers will perhaps understand that internet trading cannot flourish unless contract law is able to apply successfully.

That said, for English contract law the internet creates fewer difficulties than one might imagine. In some countries there have been problems about "electronic signatures": the laws of those countries required signatures, in the sense of handwritten names on paper, to validate contracts of more than some fairly low threshold value, and clearly much of the advantage of internet trading would be lost if agreements formed electronically became legal only after paper documents had been exchanged through the post. Not only is the rapidity of internet communication a benefit to commerce, but in some cases (where the things traded are sufficiently standardized) we want the possibility of automated trading, with no human intervention on the supplier side – or even, perhaps, no human intervention on either side.

The EU issued an *Electronic Signatures Directive* in 1999 which aimed to guarantee the availability of a legally valid electronic alternative to handwritten signatures. But for English contract law that Directive was largely redundant; English law requires signatures only in a few special cases, and in any case English law has not been particular about what counts as a "signature". In a 1954 case a rubber stamp of a firm's name was accepted as a signature; in a 2004 case (not concerned with computing technology) a typewritten name on a telex was accepted as a signature. For English law, a "signature" is simply an objective indication of the signer's approval of the contents of a document. Consequently signatures have not been a stumbling block for internet trading. The Law Commission commented in 2000 that

> We do not believe that there is any doubt that clicking on a website button to confirm an order demonstrates the intent to enter into that contract … we suggest that the click can reasonably be regarded as the technological equivalent of a manuscript "X" signature [as made by illiterates] … clicking is therefore capable of satisfying a statutory signature requirement (in those rare cases in which such a requirement is imposed in the contract formation context).

There are issues about how one knows that a mouse-click, or some other electronic alternative to a handwritten signature, was made by the relevant person, and that what he understood he was doing was approving the contract terms – but these are essentially practical problems rather than legal problems, and they are problems which IT should be able to solve without excessive difficulty. What English law cares about is simply that the person has approved the terms.

So there is not much danger that people using the internet as a trading channel will fail to create a legal contract when they believe they have done so.[46] However, there is more risk the other way round: people might find themselves prematurely committed to a contract, when they think they are still in the negotiation phase without a binding commitment. Understanding how this can happen will also show us how contract law copes with automatic trading.

7.1.2 Offers v. invitations to treat

Under the Common Law, a contract comes into being when one party makes a definite offer to the other party (which must involve a swap – one cannot "contract" to make a free gift without return), and the second party signifies acceptance of the offer to the first. Once the offer is accepted, both parties are committed. In B2B trading, there may be many rounds of revised offers as the parties negotiate precise terms acceptable to both sides, but the contract is concluded when one side accepts the same terms that are currently offered by the other side.

In a shop (where haggling is not usual), the shopper is construed as "making an offer" by taking goods to the counter or the checkout and tendering money, and the shopkeeper or assistant "accepts the offer" by actions such as ringing the sale up on the till or passing the items over a barcode reader. This is different in some Continental countries, where the shop is construed as "making an offer" by displaying goods with marked prices, and the shopper "accepts" the offer by taking goods to the counter or checkout. But in English law, what the shop does in displaying priced goods is merely to issue what the law calls an *invitation to treat* – that is, it invites shoppers to enter into negotiations with a view to agreeing a contract of sale.

In the context of traditional shopping this distinction between making an offer and inviting to treat may appear an absurd piece of legal pedantry. But in the context of internet trading it is a point on which merchants can come badly unstuck.

The risk is that a commercial website may advertise goods or services, thinking that it is "inviting site visitors to treat", in such a way that legally it is actually "offering" contractual terms. Usually that would not matter, because the company behind the website wants to sell things on the advertised terms. But in some cases the company could get into difficulties – for instance if stock of the item in question is limited and more orders come in than can be fulfilled, or if by mistake a wrong (too low) price is advertised. If the selling webpage is an "invitation to treat", the vendor is allowed to say "sorry, we are out of stock" or "sorry, the price should have been shown as £X". But if it is an "offer", then customer orders are legally-binding acceptances, and the vendor must either fulfil the orders (perhaps by finding a new source for the goods at a higher price which leaves the vendor with a loss), or else be prepared to face legal actions for breach of contract.

This kind of débâcle can happen independently of the internet, of course. The most notorious example in British retailing history occurred in the early 1990s, when the vacuum cleaner and washing-machine manufacturer Hoover ran a sales promotion which offered free flights overseas with purchases over £100. Hoover budgeted £2 million as the cost of the promotion, completely failing to anticipate how popular the offer would be. Many people bought two vacuum cleaners just to get access to the flights; some retailers put their prices up to help buyers to qualify. When Hoover was unable to buy enough flights to fulfil the offer terms, it received 30,000 complaints and faced numerous lawsuits. It ended up paying out at least £50 million; the UK Hoover subsidiary responsible was split from its American parent and sold off at much less than its previous value. Senior managers lost their jobs.

In the early 1990s, Hoover's error did not involve the Web. But with e-commerce it is so easy to put up a selling page over-hastily, and there are so many possibilities of unexpected technical glitches, that comparable errors become more probable than with traditional trading.

An American example occurred in 2001, when a programming error on the United Airlines site caused ticket prices to be "zeroed out", so that people booking flights were charged only the minor additional costs (e.g. sales tax). After it discovered the error, United first responded by charging the full prices to customers' credit cards retrospectively, but after a storm of negative publicity it reversed its decision and let customers use the tickets at the bargain rate. United claimed that this was an act of grace, and that it would have been within its legal rights to insist on full payment (and it is true that companies in a situation like this often do give customers the benefit of the doubt, for a sound business reason: when selling to the public, the goodwill forfeited by sticking to the letter of the law may outweigh the monetary loss from a one-off mistake). However, legal commentators did not agree that a court would have allowed United to change the terms of the flight sales retrospectively – particularly since plenty of discounting and promotional offers were occurring in e-tailing, so United customers could plausibly have believed that the ultra-low fares were "for real". Since England shares the fundamentals of its contract law with the USA, a company making a similar mistake here would also probably be legally committed to honour the giveaway price.

Thus unwary contractual offers can be expensive or even survival-threatening for firms that make them. But, provided one is aware of the problem, there is no difficulty about avoiding it. In 2005 the Argos website mistakenly advertised a television plus DVD bundle for 49p (instead of £350). Not surprisingly, it quickly received thousands of orders. Argos refused to honour them and gave the would-be customers their 49p's back, but in this case it was unquestionably entitled to do so. The terms and conditions on the Argos site included a provision:

> While we try and ensure that all prices on our Web site are accurate, errors may occur. If we discover an error in the price of goods you have ordered we will inform you as soon as possible and give you the option of reconfirming your order at the correct price or cancelling it …

Anyone ordering from the Argos site must tick a box to confirm that they have read these terms and conditions. This is enough to ensure that offers on the site are "invitations to treat", not "offers of contract".

So it is straightforward to eliminate this kind of risk from e-commerce. This really is a case where commissioning a lawyer to check that wording is watertight is a small price to pay for a large gain in terms of peace of mind. Nevertheless, major players often fail to cover themselves. Struan Robertson, a technology lawyer who commented on the 2005 Argos case, added that he knew another large site which was trying to cancel orders for Sony Vaio laptops priced below £2, where the published conditions were so poorly worded that customers probably had the law on their side.[47]

7.1.3 Automated trading

Turning to transactions executed automatically: the relationship of these to contract law was considered long before the days of e-commerce. A classic discussion is found in Lord Denning's judgement in *Thornton* v. *Shoe Lane Parking* (1971), where a car-park was controlled by an automatic barrier rather than a human attendant:

> The customer pays his money and gets a ticket. He cannot refuse it. He may protest to the machine, even swear at it; but it will remain unmoved. He is committed beyond recall. He was committed at the very moment that he put his money in the machine. The contract was concluded at that time. It can be translated into offer and acceptance in this way. The offer is made when the proprietor of the machine holds it out as being ready to receive the money. The acceptance takes place when the customer puts his money into the slot.

(This might be read as implying that a selling webpage is making "offers" rather than "inviting to treat"; but Rowland and Macdonald (p. 274) point out that in 1971 Lord Denning would not have envisaged cases where the machine processes customers' orders in complex ways – they see no reason to doubt that a suitably-worded selling webpage expresses invitations to treat rather than offers.) The reason to quote Lord Denning is to show that, even though contracts are between people and/or organizations, not between machines, the fact of an offer being physically made by a machine does not stop English law regarding it as emanating legally from whoever is responsible for the working of the machine.

In the car-park case, the "attendant" was a robot but the motorist was human. But one can presumably extrapolate from *Thornton* v. *Shoe Lane* and see a contract which is physically arranged by machines on both sides as having been legally executed by the persons or organizations who control the respective machines. Having set the machines up, they will be bound by the contracts thus formed – even though they only find out about these contracts after they are already bound by them.

7.1.4 Time of contract conclusion

There are other ways in which e-commerce creates special issues for contract law. For instance, in B2B contracts it may matter exactly when the contract comes into being. In some kinds of business, trading conditions change frequently and abruptly; before a contract exists, its terms can be renegotiated if they cease to suit one side, but once the contract is in being then whichever side is disadvantaged by a change in conditions is out of luck.

In English law, the general rule is that a contract comes into being when the acceptance reaches the offerer, but there is a special rule about contracts that are concluded via the postal service, which come into being as soon as the acceptance goes into the post. With e-commerce, where the path taken by a communication is both complex and often mysterious to both parties, the law is not yet entirely clear about when a contract comes into being. The issue is complicated by the fact that an EU *Electronic Commerce Directive* was implemented in the UK in 2002 and is based in part on aspects of Continental contract laws that conflict with English Common Law. So this area is at present somewhat messy; but, having drawn attention to it, I do not believe it is significant enough for the readership of this book to examine in detail.

7.1.5 The right to link

Hypertext and the World Wide Web were invented by academics, for whom it is axiomatic that publicity for one's writings is desirable. There was no thought in the minds of the Web pioneers that anyone might wish to restrain others from creating hyperlinks into his site; the more incoming links, the better. Hence the HTML language is designed in such a way that creating a hyperlink from site A into site B requires action only by the site A webmaster.

Once the Web became commercially important, freedom to link ceased to be axiomatic. Businesses want traffic to their websites, but they want the right sort of traffic. There has been considerable legal wrangling over the issue of whether website owners have an untrammelled right to link into others' sites.[48]

One issue about the right to link is not very relevant for this textbook, so I shall mention it briefly in order to set it aside: that is the question whether people can be held responsible for illegal content in sites they link to, or at least forbidden to link to such sites. For instance, a Dutch site Indymedia.nl had links to mirror sites for an extremist German magazine, *Radikal*, carrying articles about how to sabotage railways. Deutsche Bahn (the German state railway company) took Indymedia to court in the Netherlands in 2002 and Indymedia was required to remove the links. It is not clear whether a British court would have made the same order, but for most businesses one hopes that the question is academic.

More interesting for us are situations where websites aim to control incoming links because they want:

- to reside in respectable cyber-neighbourhoods
- to prevent visitors bypassing material the site owner wants them to see
- to avoid negative publicity
- to prevent their material being misappropriated

7.1.6 Cyber-neighbourhoods

An upmarket bricks-and-mortar boutique naturally wants to locate itself in a respectable area; it would prefer not to be next door to a betting shop or tattoo parlour. In cyberspace, "neighbourhoods" are defined by links between sites, so businesses would like to avoid links from sites they find unsavoury.

Some organizations have tried to impose blanket bans on unauthorized incoming links. The US National Public Radio network (a non-profit organization producing cultural programming) stated on its site that "Linking to … any material on this site without the prior written consent of NPR is prohibited", and those wanting to link were asked to fill out a lengthy form. When challenged, NPR explained that it aimed to preserve its integrity as a non-commercial organ of journalism by avoiding the appearance of association with commercial organizations. After protests from those who felt that freedom to link was essential to the Web, in 2002 NPR ceased insisting on prior authorization, but continued to claim the right to ban specific links. However, it is not clear to American legal commentators whether it could actually force anyone to remove a link to its site. (While NPR may in practice have given up trying to ban inward links, others continue to do so; in 2008 Associated Press was reported as threatening legal action against bloggers who linked to headlines on its site.)

In other instances, rather than trying to impose any general policy on incoming links, an organization has objected to a particular link. In 2001 the Ford Motor Company objected to the hacker magazine *2600* creating a link to the Ford site from a site called fuckgeneralmotors.com. Ford and GM are two different companies, so the domain name did not directly insult Ford, but Ford did not want to be associated with vulgarity. Ford sued under trademark law, claiming that the link infringed and tarnished its trademark. Dan Burk, an American professor of internet law, explained that "Tarnishment happens when you juxtapose my trademark with something that is offensive or unsavory. It causes consumers to view my mark with distaste", and in this case "the vulgar word will be associated in the minds of consumers with the Ford site or arriving at the Ford site."[49] Burk saw Ford's legal case as strong. But the court dismissed the case, on the ground that infringing a trademark was a tort only if done in connexion with the infringer's own commercial activity, which was not true in this instance.

7.1.7 Deep links

Websites are standardly designed with the idea that visitors will begin at their home page. But it is equally easy for another site to link to an internal page; such an incoming link is called a *deep link*.

A frequent reason why website owners object to deep links is that their site contributes to their business by carrying advertising, and the adverts will typically be on or near the home page. Consider the California case of *Ticketmaster Corp*. v. *Tickets.com* (2003) – since the USA is a Common Law country, it is likely that the precedents this case set would be taken seriously by a British court.

Ticketmaster was an established business that sold tickets to various events (sports, entertainment, etc.) conventionally and online; it took a commission on tickets sold, and its website also generated advertising income based on numbers of visitors to its home page. Tickets.com was a newcomer, which aggregated information on its site about where tickets could be bought. It used a spider to extract information about events handled by Ticketmaster from the Ticketmaster site to display on its own site; rather than selling tickets for those events directly, it sent purchasers via a hyperlink to the relevant place in the Ticketmaster site (making it clear that this was a separate site). Tickets.com derived its income from advertising alone.

By bypassing the Ticketmaster home page, Tickets.com clearly threatened Ticketmaster's profits, so Ticketmaster tried to invoke the law against Tickets.com. It objected on three legal grounds: breach of copyright, "trespass to chattels", and breach of contract.

The copyright issue related to the way that Tickets.com derived event information from the Ticketmaster site; but in a preliminary hearing the California court dismissed this issue, mainly on the ground that copyright law does not protect purely factual data but only its arrangement into a "literary work" – Tickets.com had been throwing away the Ticketmaster formatting, and arranging the facts of date, prices, etc. into its own format. "Trespass to chattels" is a rather obscure Common Law concept: *chattels* are pieces of movable property (say, a vase, a car, but not land), and trespass to chattels means interfering with someone's movable property in a harmful way. Since the Tickets.com spider did not affect the use or operation of the Ticketmaster computer, this claim also failed.[50] The court did accept that there was an arguable case of breach of contract: a notice on Ticketmaster's home page stated that anyone penetrating beyond it to internal pages was thereby accepting conditions which would have forbidden Tickets.com's usage. (Compare the way that shrinkwrapped software often has a notice saying that opening the packaging implies accepting various small-print licence terms; but there has been much controversy about the legal validity of such notices.) It would have been for Ticketmaster to pursue the breach of contract issue in a further hearing (but it appears not to have done so).

There are other reasons for a site to resist unauthorized incoming links. John Corker was head of an Australian online legal practice, OzNetLaw, which wanted to ensure that all visitors were aware of its terms and conditions:

> The idea was aimed at managing liability from people suing us for providing advice. If people were deep linking, then someone might bypass the terms and conditions, so we thought a [linking] policy could offer some protection.[51]

But this was more a matter of enabling OzNetLaw to tell a court that it had done everything it could to ensure that visitors had read the conditions, than actively using the law to eliminate unwanted links – Corker saw the chance of that as "negligible".

7.1.8 Negative publicity

A straightforward example of a link which promotes negative publicity might be wording such as "click here to visit a crooked firm", with the link leading to company X's site. But that would not really be an issue about linking; the law would probably treat it as no different from saying "Company X is crooked" in so many words on one's own site. However, there are subtler examples.

Diebold Election Systems (since renamed Premier Election Solutions) was an Ohio-based company making voting machines. It put its archive of internal company memos on the internet, presumably to make it easier for staff members to consult; some students found material in which Diebold people had raised worries about product quality, and created links to these memos from their own sites. Diebold threatened to take the students, and their ISPs, to court for breach of copyright.

But this rebounded. The Online Policy Group, a Web-freedom pressure group, sued Diebold (which it saw as trying to suppress public discussion of the integrity of the democratic voting process) for issuing baseless threats; in 2004 Diebold lost, and had to pay damages and costs of $125,000.

7.1.9 Inlining and framing

In the Diebold case the real issue for the firm was not copyright but negative publicity. In many other cases, though, organizations object because outsiders are using hyperlinks to hitch "free rides" on work which the objector is using as an asset in its own business.

If A simply downloads a copy of material on B's website and places the copy on its (A's) own site, that is no different from copying and publishing a book for which another publisher holds the rights, and can be dealt with straightforwardly under copyright law. But, typically, that is not what happens. Rather, A uses hyperlinks to B's site, so that a visitor to A's site sees elements of B's site looking as though they are part of A's site. For instance, A's page may include an HTML "img" tag telling the visitor's browser to download graphic material from B's site (lawyers are calling this *inlining*), or A's page may show an entire page from B's site framed with a border featuring A's logo and/or advertising (*framing*). A does not "copy" anything; the only copying of B's material is from B's site to the visitor's machine – and B put his site up in order to enable copying in that direction to occur. So how can B complain that A has breached his copyright?

Many organizations in B's position have tried to force A to remove such links; alternatively, some have tried to charge for the links. But the attempts have not been very successful, except where B has folded up at the threats stage without fighting the issue out in court.

The earliest case to attract international attention arose in the Shetland Isles: *Shetland Times* v. *Willis* (1997). Unfortunately for the law, this case was technically rather "blurry". The *Shetland Times* was a long-established local paper, and Willis started an online competitor, the *Shetland News*, which displayed headlines copied from the *Times* that, when clicked, took the visitor to the relevant stories on the *Times* site. The judge accepted that there was a *prima facie* breach of copyright (whereupon the case was settled out of court rather than fought through to the end), but this ruling was based largely on the fact that the headlines, at least, were actually copied onto Willis's site. Likewise, in a larger-scale, recent case, *Copiepresse* v. *Google* (2006–07), a Belgian court found that Google News was breaching the copyrights of newspapers whose articles it linked to, by displaying headlines and short extracts on its own site.

Perhaps more clearcut was the case *Haymarket Magazines* v. *Burmah Castrol* (2001). Haymarket's portfolio of magazines included two on motoring and motor racing, *What Car?* and *Autosport*. The oil company Burmah Castrol had a "Complete Motoring" website which framed pages from Haymarket's site so that they appeared to be on "Castrol – What Car?" or "Castrol – Autosport" pages, and which for good measure corrupted the banner adverts that Haymarket ran on its site. Haymarket sued not just under copyright law but also under the special database law discussed in chapter 6, under the law of trademark infringement, and under the law of "passing off" (trading under the pretence of being someone else). This case also was settled out of court and thus created no legal precedent; still, Burmah Castrol agreed to desist from what it was doing, so it must have been advised that Haymarket had at least a good chance of winning (but under which law?)

There has been one Continental case, *Vriend* v. *Batavus* (2003), where the Dutch judge ruled that "framing" counted as breach of copyright, because it "creates the impression that the framed information belongs to the linking website". But a published comment on that was:

> This decision is confusing in its argument: copyright law considers objective, not subjective elements of a violation, hence, there is no place for "impressions".[52]

("Confusing" here is probably a polite lawyer's way of saying that the judge got it wrong.)

In another Continental case, *StepStone* v. *OFiR* (2001), the plaintiff won under the special database law rather than copyright law. StepStone was a German-based international company running an online recruitment service. OFiR, also German, systematically hyperlinked to StepStone's individual job-vacancy notices, bypassing StepStone's adverts, and it used figures on StepStone's vacancies in order to publish claims about the numbers of jobs OFiR had access to. The judge ruled that OFiR's deep links infringed StepStone's exclusive rights in its database. This led Anthony Misquitta, of the distinguished London law firm Farrers, to predict that under the database law most websites would count as "databases" and that making someone else's website contents available via hyperlinks would count as "unauthorized re-utilizing", banned under that law.[53]

(Misquitta added:

> The law of intellectual property has had a terrible time of applying its principles to the internet, largely because it has not had its fundamental philosophies questioned as much since the invention of the printing press. The law of copyright is terrified of the internet and runs screaming from the court every time it is asked to address it.

Colourful language, from a lawyer!)

Something that seems strangely absent from most discussions of this area by lawyers (though computing people have often pointed it out) is that it is not hard to prevent outsiders creating deep links into one's site by technical means, if one really wants to do so. In the Diebold case, one might think it almost insane to place an archive of confidential messages on the public internet; someone ought to have mentioned the word "intranet" to Diebold's managers. But even when one wants one's webpages to be available to the public, it is not difficult to prevent them being accessed other than by the intended routes. Only the home page needs to remain in a fixed, known place, and there is usually no objection to links to one's home page. OK, defeating deep linking technically would take a little more effort than putting up a collection of pages and leaving them alone – but not nearly as much effort, expense, and uncertainty of outcome as taking linkers to court.

However, subsequently to *StepStone* this point was taken on board by the court hearing another German case, *Verlagsgruppe Handeslblatt* v. *Paperboy* (2003), where again the defendant's site was deep-linking directly to the plaintiff's newspaper articles, bypassing the newspaper home page. Contrary to Anthony Misquitta's prediction, the German Federal Court refused to treat this as unauthorized re-utilization of a database; it explicitly described deep links as important for the success of the internet, and ruled that it was down to sites which did not want them to block them by technical means.

Overall, then, the idea of controlling incoming hyperlinks by law has achieved little traction to date.

7.2 Ownership of domain names

The Western world has long-established trademark laws enabling firms to create strong brand images linked unambiguously to their identity. When URLs came along, the problem arose that bare sequences of characters offer much less scope for differentiation than traditional graphic trademarks. As one anonymous writer puts it:

> In the physical world, Cannon Towels, Cannon Fishmarket … and Robert Cannon can all co-exist peacefully. The trademarks at issue are distinct and not subject to confusion. But in the online world, only one gets the valuable cannon.com [domain name][54]

In the early years of the Web, trademark owners sought to insist that they were legally entitled to a given domain name – but in very many cases like "cannon", claims like that were mutually incompatible.[55]

One way in which this raises novel legal issues relates to the concept of the bottom-up Law Merchant, discussed in chapter 2. The domain name system is governed by the non-profit but private-sector ICANN (Internet Corporation for Assigned Names and Numbers), which delegates control over various high-level domains to different national or multinational organizations (*registries*) – for instance, the .uk domain is controlled by a non-profit organization called Nominet. Nominet and its sister registries have set up formal processes for arbitrating disputes over ownership of lower-level domains. ICANN monitors the activities of the registries, requires their dispute resolution services to harmonize with an agreed set of general principles, and occasionally it decides to take a top-level domain away from one registry and entrust it to another.

But where does the authority delegated by ICANN come from in the first place? The internet grew, historically, out of a US military and academic network, Arpanet, and domain names were initially allocated by an institute within the University of Southern California and then, from 1993, by various public- and (mostly) private-sector organizations under a contract with the US National Science Foundation. So decisions about domain names were at that time ultimately underpinned by the power of the American state.

As the internet grew into a commercially and socially crucial facility for the world as a whole, it was no longer acceptable for a single nation to control it. ICANN was established in 1998, largely in line with a memorandum published in the name of the "Internet Community"; the US government formally transferred responsibility for domain name allocation to ICANN. As a result, where authority over domain names ultimately stems from today is a rather nebulous issue. Lloyd (p. 464) comments about the UK Nominet organization that:

> As with much of the Internet, the legal basis for its actions is unclear, it being stated that Nominet UK derives its authority from the Internet industry in the UK and is recognised as the UK registry by [IANA, the immediate predecessor to ICANN] in the USA.

Quasi-legal rules which rest on the authority of an international "community" or "industry" sound very reminiscent of the mediaeval Law Merchant.

When ICANN was established, domain name allocation was a deeply sensitive and controversial area. The other thing to say about it, though, is that the heat has now been somewhat drained out of it by the rise of search technology. While the normal way to access a site was to type its URL manually, it was crucial to have a snappy, memorable domain name. Television commercials and print adverts do still display URLs that have to be remembered and typed in, but by now it is commoner for a visitor to be led to a website via Google or another search engine. Someone who surfs that way clicks on a link rather than typing in the URL – he may not even notice what the URL is. So this is not an area of computing law which I would expect to develop to any great extent in future.[56]

7.3 Web 2.0 and defamation

7.3.1 Slander and libel

English law distinguishes two kinds of defamation: *slander* (in speech) and *libel* (in writing); because writing is permanent, libel is treated as being more seriously damaging than slander. E-mails and the like are often composed as casually and carelessly as spoken remarks, but they can be preserved indefinitely and so the applicable law is libel law.

English libel law is strict: compared to other countries, it is easy for someone who feels damaged by the written word to win a case against whoever is responsible, and awards for loss of reputation have traditionally been large (though recent changes have moderated that to some extent).

As business first used the Web, libel law was scarcely relevant. Commercial websites were concerned with promoting their own businesses, not normally with knocking their competitors. But the Web is coming to be used in new ways. We have heard a great deal recently about "Web 2.0". This is a vague, hype-laden piece of terminology, but one thing it commonly refers to is the idea that websites – including commercial websites – are ceasing to be outlets for one-way communication exclusively, and turning into two-way, conversational affairs, where for instance a company will draw its customers and other interested parties into participation via blogs, chatrooms, and similar mechanisms.

There are several business reasons why the "virtual communities" fostered by interactive websites are potentially beneficial for a company. However, if members of the public are encouraged to post material on a company website, the legal danger is that some individuals' postings might include defamatory remarks about third parties. We know that electronic communication tends to encourage a kind of "flaming" that is rare in other media. For the firm owning the website, it would be regrettable enough to find one of its customers having to defend a lawsuit as a consequence of contributing to a blog which that firm had set up. Even worse would be the possibility of itself defending a defamation suit, if it is held responsible for others' contributions to its site. A plaintiff who hopes for a large damages award will be more interested in going after the firm than the individual; the firm is more likely to be able to pay.

So the question arises what legal responsibility a website owner has for material posted by others.

7.3.2 Distributors and publishers

Questions like this arose before Web 2.0 days, in connexion with ISPs and operators of bulletin boards. One way that lawyers think about the issue is to compare that kind of electronic communication infrastructure with the world of newspapers and magazines, and to ask whether the organizations are more like distributors (such as newsagents) or publishers. If a newspaper contains a libellous article, the newsagents who sell the paper to readers would not normally be held liable – they have no control over what appears in the paper and may not even be aware of it; but the newspaper publisher has editorial control over what its journalists write, so will routinely be treated as equally responsible with them for any libel.

In the case of electronic bulletin boards, some are moderated and others not. Ironically, although providing moderation would normally be seen as the responsible thing for a bulletin board operator to do, legally it might be a rather dangerous thing to do: it implies taking on a role more like publisher than distributor.

In the USA (although libel law is far milder there) this situation was seen as creating such risks for organizations which undertake the socially-valuable task of promoting electronic communication that the risks were eliminated by statute (section 230 of the *Telecommunications Act 1996*). This broadly says that service providers are not to be held responsible for content posted by others, and that no liability arises from the moderating role.

Without a blanket exemption such as American law provides, a website run by a commercial firm would be more likely to be held responsible for its contents than some bulletin board run by amateur enthusiasts – the site contributes to business profits, so there would be little excuse for not taking the trouble to moderate it. English law contains nothing parallel to §230 of the US Telecommunications Act. Our *Defamation Act 1996* provides that no-one is liable for the contents of electronic communications if they act purely as unwitting distributors, but if they act as "publishers" they are liable; a commercial website owner, like a newspaper publisher, would have a duty to take reasonable care about what it publishes.

7.3.3 Godfrey v. Demon

Even an ISP, with no commercial interest of its own in the contents of material it hosts, will probably not escape liability under the 1996 Act if it has been told about defamatory material on its servers (so that it can no longer claim to be an unwitting distributor). Consider Godfrey v. Demon Internet Ltd (1999).

Dr Godfrey was a British computer science lecturer who allegedly made a hobby of starting online flame wars and then bringing libel actions when people responded to his flames by being nasty about him. In 1997 he faxed the MD of the leading British ISP Demon demanding the removal of a scurrilous newsgroup posting which had come in from the USA. Demon routinely deleted newsgroup postings after a fortnight, so the issue concerned only the ten days between Godfrey's fax and the normal deletion date; during that period, Demon failed to act (apparently the fax never reached the MD's desk). In view of this delay, the court found in preliminary hearings in 1999 that Demon could not satisfy the requirement about taking reasonable care – at which point Demon threw in the towel and settled out of court, paying Godfrey about a quarter of a million pounds.

Although Godfrey v. Demon set no formal legal precedent (because it was settled rather than fought out to a conclusion), the terms on which it was settled sent a thrill of fear through the industry. It seems that (unless an ISP is prepared to investigate and satisfy itself that a complaint is legally unfounded, which would often be difficult or impossible for it to achieve), its only safe response to any complaint will be automatically to take down the material complained about. This is what British ISPs have been tending to do.

Indeed, they sometimes censor material before it is received. Outcast was a small-circulation magazine for homosexuals; its February 2000 issue contained material alleging financial irregularities at the company Mardi Gras 2000 Ltd, part-owned by a group of "gay press barons". No actual libel action arose from that, but after receiving a complaint Outcast's ISP, NetBenefit, required Outcast to satisfy it that arrangements were in place to avoid possible future libel. When Outcast were unable to comply within a two-hour deadline from receipt of their letter, NetBenefit took their entire website down. Commentators objected to this "censorship" of the Web; but NetBenefit explained that it would otherwise be exposed to unacceptable legal risks. It invited Outcast to "campaign on the real issue: the need for a change in the law to allow [ISPs] to provide the service Outcast and others are seeking."[57] Legal commentators see NetBenefit's attitude as entirely understandable given English law as it stands.

7.3.4 The *Mumsnet* case

If a neutral ISP, which simply offers Web hosting services to all comers, can be this vulnerable, an organization inviting website postings by its clients will surely be even more so. The classic example is *Gina Ford* v. *Mumsnet*, settled out of court in 2007.

Gina Ford is a well-known but controversial author of books about childrearing, who advocates methods much stricter than those which used to be in vogue. Mumsnet is a parenting website run as a part-time activity by seven mothers, which includes chatrooms. Gina Ford's lawyers sought to have the entire Mumsnet site taken down, because the chatrooms contained defamatory remarks about her, ranging from what sound like defensible opinions (Gina Ford must be cruel and uncaring, because her *Contented Little Baby Book* recommends leaving a five-month-old to cry for three hours at a time) to ridiculous flames (Gina Ford straps babies to rockets and fires them into south Lebanon). Mumsnet took down individual postings whenever Gina Ford complained about them, but it admitted that it could not comprehensively monitor 15,000 postings a day. In the attempt to placate Gina Ford, Mumsnet banned its users from mentioning her, though it had been neither a pro- or an anti-Gina Ford site – "the pro voices met the antis" – and it saw banning mention of her as "a bit like barring discussion of Manchester United from a football phone-in".[58] It matters how babies are treated; many Mumsnet mothers were outraged at not being allowed to discuss this freely.

Under the settlement, Mumsnet formally apologized to Gina Ford and paid a five-figure sum in damages (though the website continues in being). Again, because it was settled the case does not constitute a legal precedent, but it shows that website owners do not feel legally secure with respect to material posted on their sites by others.

7.3.5 Weak protection

The year after *Godfrey* v. *Demon*, the EU *Directive on Electronic Commerce* (2000) seemed set to offer ISPs a measure of protection. It required national laws, among many other things, to hold distributors of electronic communications immune from liability provided they are mere distributors. However, this was not to apply if they "select or modify the information contained in the transmission" (i.e. moderate the postings). The Directive was implemented in Britain by the *Electronic Commerce (EC Directive) Regulations 2002*. A Law Commission report looked at these Regulations, and concluded that they did not clearly offer an ISP any greater protection in practice than it had under the 1996 Defamation Act.

ISPs took some comfort from a 2006 decision, in *Bunt* v. *Tilley & ors*. John Bunt regarded himself as defamed by material in Usenet postings by David Tilley and two other individuals; he sued not only these individuals but also the ISPs (AOL, Tiscali, and BT) which they used to transmit the material. The issue decided in 2006 was whether the ISPs shared any responsibility for the postings. The court found in the first place that an ISP which passively provides an avenue of access to the internet is not a "publisher" in Common Law, and also that the ISPs were exempted under the European Regulations from responsibility for the contents of material they transmit to and from the internet.

However, this protection was limited. It depended on the ISPs acting only as transmitters rather than hosts, so it would not have helped Demon Internet to defend itself against Godfrey; the *Mumsnet* settlement came after the *Bunt* precedent was already established.

Evidently, companies need to be wary of setting out to reap the commercial advantages envisaged by enthusiasts for "Web 2.0".

8. Regulatory compliance

In earlier chapters, the state was essentially saying to organizations and to individuals “If you choose to use computers, here are the rules of the game. You are forbidden to do A, B, or C. Your trading partners, or others you are involved with, are entitled to expect you to do D, E, and F.”

For most of the history of information technology, this was all the IT law there was. But now that there is no longer a question about whether organizations choose to use computers (because they all do), the state has begun to command positive actions as well as issue prohibitions. It has started to say “you must do P, Q, and R”, where P, Q, and R are things that could not be done without computers.

What is more, after many years when lawyers seemed fairly mystified by IT and its potential, the law has swung to the other extreme and is taking the technology so much for granted that anything the law might like to have is assumed to be readily deliverable. Some of the Ps and Qs and Rs which the law is beginning to demand are things at the very edge of what we are capable of achieving, or even beyond current capabilities.

For the readership of this book, that is rather good news. It creates work, and interesting work, for computing graduates. Most people would prefer a job which challenges them to achieve novel goals to one consisting of humdrum routine.

8.1 Sarbanes–Oxley and after

The term “regulatory compliance” includes the topics discussed under “personal data rights” in chapter 6. But regulation of business IT has stepped up to a higher gear recently, in connexion with financial aspects of business. Since about 2004 compliance has become one of the main burdens on IT departments, comparable with the burden of getting the actual work of the organization done.

The events that triggered the first of the new regulations were the Enron and WorldCom scandals in the USA. When the energy-trading company Enron collapsed in 2001 this was the biggest bankruptcy in American history, but it was soon dwarfed by the collapse of the telecomms company WorldCom in 2002; in both cases the problems were caused largely by fraudulent accounting. The American public demanded safeguards to prevent such things happening again (that was the hope, at least), and the response was the *Sarbanes–Oxley Act 2002* (known for short as “Sox”). Sox has turned out to be the first of many new laws imposing demands on financial IT on both sides of the Atlantic.

Sarbanes–Oxley essentially requires a business to monitor its financial activities and to be prepared to demonstrate their integrity to outside auditors, down to a level of detail that was unheard-of in the past. Traditionally, managers tended to assume that things were all right until they picked up a hint that something might be amiss, and only then did they look into the problem. Before IT, this was really the most that was possible. Sox turns this round and requires businesses to put systems in place through which senior managers can *guarantee* that everything is all right (so far as financial integrity is concerned). Managers take these requirements seriously, because the penalties are severe. A chief executive or chief finance officer who signs off accounts that turn out to be misleading may face up to twenty years in gaol, without necessarily having been a party to fudging the figures. Under Sarbanes–Oxley, he is guilty for failing to make it impossible to fudge the figures.

This requires large changes to a firm's IT systems. For instance, a word-processed document can be altered undetectably; so Sox-relevant documents must routinely be held in tamper-proof electronic formats, just in case the need to demonstrate their integrity should arise. The law does not go into technical detail about how companies are required to work; it gives concise specifications of functional goals, which might imply different technical solutions for different firms, depending on their business. But for many firms the impact on their IT activities is massive.

> … some interpretations [of the Sox provisions] say that IT must be able to validate and control the operation of not only the core, recognised enterprise accounting systems, but every ad hoc spreadsheet formula in the company.
>
> "It is IT's responsibility to test for integrity, so if finance people are creating special spreadsheets that feed up into the financial master system, they need to go into those formulas, and prove to IT and the financial audit teams that the formulas are in accordance with … accounting standards," says Brent Houlahan, chief technology officer of managed security services provider NetSec.
>
> IT's responsibility would be to validate that assessment and log the use and susceptibility to change of that spreadsheet, and the entire process it launches.[59]

Sox imposes requirements not only on data processing but on storage and retrieval; many business documents must be archived for at least five years in ways that allow them to be readily retrieved if called for. Dan Schrader of FaceTime comments "There's nothing in SOX that says: 'thou shalt record every instant message', but some companies are coming to interpret it that way". And what has to be retained includes not only the first-order data, but also the records of tests applied in order to check that systems are compliant.

Sarbanes–Oxley is an American law, but that does not mean that it is irrelevant for British business. If a UK company is a subsidiary of a US parent, if it is listed on an American stock exchange (as many UK-based firms are), or even if it has more than a handful of American shareholders, then US law requires it to comply with Sox.

No-one in Britain takes this exposure to US law lightly, since the case of the "NatWest Three". These were British citizens, living in Britain, who in 2007 were sentenced in the USA to 37 months in prison each, for Enron-related activities that were carried out in Britain, were directed against a British bank, and (while not admirable) were not clearly enough in violation of UK law for our authorities to prosecute. (The NatWest Three were extradited under a treaty with the USA agreed by the Blair government which many commentators find disturbingly one-sided.) The relevant law in that case was not Sarbanes–Oxley, but the case showed how aggressive the US authorities are now prepared to be with people overseas whom they regard as infringing their financial legislation.

Sarbanes–Oxley in fact gave non-US companies a longer grace period before it applied to them than American firms got. But since 2006 it has been fully applicable to relevant British firms.

In any case, there is now plenty of new British and European legislation which imposes comparably burdensome demands on all our firms, not just those with US connexions. In one case, the *Companies (Audit, Investigations, and Community Enterprise) Act 2004*, the UK government did in fact have second thoughts and cancelled provisions that would have placed a challenging Sox-like burden on companies, before these came into force in 2006. But there are plenty of other new regulations which are fully in force.

MiFID, the EU *Markets in Financial Instruments Directive*, has applied since 2007: it requires financial-services organizations to be able to prove that trades on behalf of clients are executed at the most favourable available combination of price, transaction cost, speed, etc., with relevant data retained for five years. *Basel II* is an international agreement on risk control for banks, which was to be fully implemented EU-wide by the start of 2008 – the events of autumn 2008 suggest that it must have failed in its purpose, but that does not contradict the fact that it requires penetrating electronic analysis of constantly-changing capital holdings and liabilities. Even the *Working Time Regulations 1999* were very costly to business in terms of new kinds of record required to be kept about individual employees. It would be tedious to discuss here the detailed contents of these various new regulations; in any case there are now various others which I have not even mentioned. By 2006 the British Chambers of Commerce estimated that the cost to British business of regulatory compliance had reached £10 billion a year.

Many of the new regulations are not just expensive to comply with, but require organizations to work in ways that they would not have chosen. For instance, traditionally building societies often had a decentralized IT strategy, with processing occurred largely at branch level. When the Financial Services Authority was given oversight of the mortgage industry in 2004, the resulting regulations forced societies to switch to a centralized approach.

Furthermore, regulations are often over-optimistic about what is possible. Bob Fuller, an IT director at Dresdner Kleinwort Wasserstein, commented in 2006 that

> MiFID assumes that IT works 24/7, and doesn't say what happens if it fails. You have to deliver 100 per cent availability on your systems if you want to keep your job in the new world.[60]

Under the EU *Data Retention Directive* which came into force in 2007, telephone companies, ISPs, and companies such as Google must retain data on individual calls for at least six months (a limit that may well be extended), and – a far more challenging requirement – must be able to pick out specific data without "undue delay", which is being interpreted as more than about fifteen minutes. Jim Pflagling, chief executive of the security analytics firm SenSage, says that it will be a challenging target for even a medium-sized telephone company, handling some hundred million calls a day, to put in place systems that

> can quickly answer queries such as: "Who has phoned person X from mobile provider tower X within the last day?" … you're not going to be able to point your Oracle database … at this to sort it out.[61]

One reaction to the sudden blizzard of regulation is to say that the many new rules are so extremely demanding and at the same time inadequately thought through that it is just impossible for any organization to achieve full compliance, because the rules are not all consistent with one another. Already in 2003 Michael Fabricant, shadow minister for e-commerce, was claiming that

> We are approaching the Byzantine situation in Russia, where one decree conflicts with another and industry does not know what it is supposed to do.[62]

By 2006 the lawyer George Gardiner was more forthright:

> Nobody can comply with every law; it's a question of prioritising business interests and watching out for which regulator has the big stick.[63]

But some regulators have large and painful sticks.

8.2 Accessibility

A very different aspect of compliance is "accessibility", which in a legal context refers to making services available to the disabled.

Legal prohibition of discrimination against the disabled was introduced by the *Disability Discrimination Act 1995*, and extended by the *Disability Discrimination Act 2005* and the *Equality Act 2006*.[64] These laws apply, among others, to anyone offering goods or services to the public; broadly, they are required to make them equally accessible to the disabled, so far as that is practical.

The most obvious way in which this relates to IT has to do with usability of websites by (in particular) blind people. (This is far from the *only* way in which disability discrimination law impinges on our profession; for instance, the Acts also place duties on employers, which apply as much to employers in the IT sector as to any others, and might be specially problematic in some areas of IT. But we have not been looking at employment law in this book, and we shall not do so in connexion with disability discrimination.) Obviously, most people experience websites mainly or entirely through the sense of sight. But blind people routinely use the Web via screen-reader software which translates text into spoken words. However, that method of access is often defeated, for instance by graphic material that cannot be "read" as wording. One minimum requirement, if the blind are to be able to use a site, is that every "img" tag should have an "alt" attribute describing the image in words (which a screen reader will use). But the guidelines that have been promulgated for Web accessibility contain many further points. For instance, if colour differences are used in a meaningful way, then colour should not be the *only* distinction used.

(Likewise, for deaf users, site content which is normally auditory should be equipped with some visual alternative.)

The Acts themselves do not spell out the technical features needed to make websites accessible. This has been done, in great detail, by the international World Wide Web Consortium (W3C), which defines three levels of accessibility criteria, from criteria which *must* be satisfied down to those which it is preferable to satisfy.[65] The W3C guidelines have no legal force, in Britain or elsewhere; but in 2006 the British Standards Institution published a specification on website accessibility which refers to the W3C guidelines, and a court would probably treat compliance with those guidelines at some level as a good defence against a discrimination claim. (The European Parliament in 2002 recommended compliance with the middle of the three W3C levels.)

To date there has been no court case about Web accessibility in Britain, though the Royal National Institute of Blind People is known to have raised accessibility problems with two large companies, which agreed to make the appropriate changes to their sites voluntarily, in exchange for anonymity. The only well-known case fought out to a conclusion in a Common Law jurisdiction was a case under the similar Australian Disability Discrimination Act: *Maguire* v. *Sydney Organizing Committee for the Olympic Games* (2000). Bruce Maguire was a blind man whose business was supplying the kind of assistive technology for reading websites that was mentioned above. He complained that parts of the Sydney Olympics site were inaccessible to him; not just did some img tags lack alt text, but links within the site, for instance from a general index page to the pages for individual sports, depended on graphics which a blind person could not use.

Maguire won his case and the Olympics Committee was fined A$20,000. As a precedent this case is not straightforward, though. Because the plaintiff was himself in the assistive-technology business, he wanted a great deal of technical information that would be irrelevant for most blind site visitors, and which the Olympics Committee resisted handing over because it was commercially-sensitive intellectual property belonging to themselves and their IT contractor, IBM. Another problem seems to have been that some of those involved in the legal dispute were not technically competent; at one point the Committee stated that because of commercial confidentiality it would not release the HTML source code for pages it had already put up on the

Web – whoever drafted that statement evidently did not know how the World Wide Web works! Rather than being heard in an ordinary law court, *Maguire* was decided by a "Human Rights and Equal Opportunity Commission". Reading their judgement makes it difficult to avoid the suspicion that they were swayed more than an ordinary judge would be by bias in favour of the disabled.

In the USA, cases against Ramada.com and Priceline.com were settled out of court in 2004, with the defendants making the changes requested and paying a total of $77,500 towards the costs of the investigation that led to the cases. But the relevant American law is fairly different from the British Disability Discrimination Act, so these cases may not have much significance for British courts.

At present, a high proportion of commercial websites fail to comply with the accessibility guidelines. But, remarkably, so too do a high proportion of government sites; this is very much an area where the organization responsible for promoting legislation is effectively saying "do as I say, not as I do". The Department of Work and Pensions' informal statement of UK legislation cited in a footnote above is a pdf file; there is no HTML alternative, and the file uses four colours apart from black to identify distinct categories of text, with no alternative indication of the distinctions. As another example, in 2006 the Department for Trade and Industry spent £200,000 revamping its website, and claimed that the new site achieved the middle of the three W3C accessibility levels. In fact it failed at the most basic level; one blogger summarized its accessibility characteristics by describing it, in typical blog language, as "about as shit as it's possible for a large, corporate website to be."[66]

In this situation, it may be difficult to blame hard-pressed commercial firms if they do not treat Web accessibility as their top priority.

8.3 E-discovery

Another kind of "compliance" is compliance with the rules of court procedure.

In the early stages of a civil case, each side is required to supply the other with copies of any documentation potentially relevant to the issues under dispute, so that the lawsuit can be settled by reference to the relative merits of either side's case rather than by who happens to have the most telling pieces of evidence in their hands. The traditional term for this process was *discovery*. In Britain this was officially changed in 1999 to *disclosure*, but "discovery" is still current in the rest of the English-speaking world. Because the new, electronic version of this process has developed much further to date in the USA than in Britain, the term *e-discovery* is commonly used on both sides of the Atlantic, and I shall use it here (though *e-disclosure* is sometimes used in Britain).

Before the IT revolution, discovery involved legal complexities, relating for instance to classes of document (such as letters between an organization and its lawyers) which were exempt from discovery, or *privileged*; but it posed no great practical problems. Correspondence on paper was filed in ways that made it fairly straightforward to locate relevant material. Phone calls were not normally recorded, so the question of discovery did not arise.

This changed with the arrival of e-mail. An e-mail can be saved, in which case in principle it is as subject to the discovery process as a letter or inter-office memo on paper. But e-mails are far more numerous, and they tend to be dealt with directly by the people they are addressed to rather than by secretaries who are skilled at organizing filing systems. Many people file e-mails chaotically, or at least idiosyncratically. An e-mail may not be saved by the person it was sent to but may still be retrievable from backup tapes, held at department or organization level – in which case the messages that matter will probably be mixed up with a great deal of irrelevant material. So "e-discovery" is challenging in a practical way, apart from any legal niceties involved.

The main reason why e-discovery is a hot topic is that American courts have begun awarding large sums in damages against organizations that fail to produce comprehensive collections of electronic documentation.

The first significant example was the 2005 case *Laura Zubulake* v. *UBS* (Union Bank of Switzerland, then Europe's largest bank). Laura Zubulake was an equities trader earning about $650,000 a year at the New York branch of UBS; she was sacked, and sued her employer for sex discrimination. She was awarded about $29 million, part of which was compensation for loss of earnings but $20 million of which was "punitive damages" connected with the fact that UBS had failed to produce all the e-mails demanded by her lawyers – backup tapes from years past were restored to retrieve the material, but some relevant material had gone missing despite instructions given that it should be preserved. Then in *Coleman (Parent) Holdings Inc.* v. *Morgan Stanley* (2005) the plaintiff was awarded $1.45 billion, including $850 million in punitive damages for similar reasons – this was reversed on appeal, but the huge initial award shows the risk that firms now face.

In both of these cases there were claims that adverse electronic evidence had deliberately been destroyed. But UBS seems to have been punished in *Zubulake* less for actively destroying evidence than for failing to put in place adequate mechanisms to ensure preservation of relevant material – something which is technically not at all easy to achieve, when items are scattered across directories on different servers (together with portable PDAs, memory sticks, laptops, etc.) in a complex computing environment, and when the items may be of very diverse kinds (not just e-mails but, for instance, voicemails, blogs, spreadsheets, videoconferences).

Zubulake and *Coleman* were at least concerned with very large sums of money. But e-discovery in the USA is becoming a large problem in lesser cases. In a linked pair of cases reported as ongoing in New Jersey in 2008, *Beye* v. *Horizon* and *Foley* v. *Horizon*, where a health-insurance company was resisting paying for two teenagers' treatments for anorexia on the ground that it might be psychological in origin, the company demanded

> to see practically everything the teenagers had said on their Facebook and MySpace profiles, in instant-messaging threads, text messages, e-mails, blog posts and whatever else the girls might have done online … [The court supported this demand, so] hard disks and web pages are being scoured in order for the case to proceed.[67]

Rebecca Love Kourlis, formerly a judge and now director of the academic Institute for the Advancement of the American Legal System, sees cases being settled out of court rather than fought to a conclusion purely because one side cannot afford the costs of e-discovery.

What is more, the difficulties of e-discovery do not fall solely on the side giving the material. The receiving side then has the problem of winnowing nuggets of evidence that can actually be used to strengthen its case out of a sea of irrelevancies, peripheral material, duplicate copies, near-duplicates, messages about other people with the same surname, and so forth.

Malcolm Wheeler describes e-discovery as "the single most significant change to the legal system" in his forty years as an American business lawyer.[68] American companies are having to take radical steps to impose discipline on their internal communication practices, so that they will be equal to the e-discovery challenge if it arises – waiting until they are hit by a lawsuit is seen as unworkable. One suggestion, for instance, is to prohibit any use of company servers for personal e-mail – surely a draconian rule, considering how much of people's waking lives is spent at work. A legal organization, the Sedona Conference, has been developing "Best Practice Guidelines … for Managing Information and Records in the Electronic Age" (over a hundred pages in the 2005 version), and American courts are treating compliance with the Sedona guidelines as a test of whether an organization is meeting its discovery obligations. The court system of England and Wales revised its rules on discovery (or "disclosure") in 2005 in line with the Sedona principles for electronic documents.

The English rules do differ from the American rules, in ways that mean that e-discovery in England will not lead either to such vast quantities of electronic material being handed over, or to eye-catching punitive damages awards. An English court would not require the level of discovery we saw in *Beye* and *Foley* v. *Horizon*. But that does not make e-discovery less significant here. The fact that English courts require the material handed over to be "surgically" limited to just those items which make a real difference to the case makes the burden of selection on the giving side all the greater. An organization which fails to manage e-discovery adequately will not have to pay out millions of pounds as a punishment, but it may well lose its case in consequence – which is what the whole system is about.

What must be a nightmare for lawyers is an attractive field of activity for computing graduates. The interest of e-discovery, for our profession, is that the requirements it creates to filter relevant items out of an organization's total data pool, and – just as important – to satisfy a court that the filtering has met legal obligations adequately are leading IT departments to draw on sophisticated areas of computer science.

An obvious, simple approach to finding relevant files within an ocean of textual material is keyword search on the contents. But that depends on those initiating the search being able to predict a set of keywords which will succeed in picking out the items of interest; because human languages are full of synonyms and messy complexities, people cannot do that. In one famous study of information retrieval accuracy in a legal context, involving selection of items from a database of about 40,000 documents, experienced lawyers using a keyword-based software system believed they had found more than three quarters of relevant items, but actually found only about one in five.[69] Consequently, lawyers are beginning to turn to artificial-intelligence-based "machine learning" techniques such as *clustering* or *latent semantic analysis*.[70]

One of the very few world-class British software houses, Autonomy, has for some time been supplying what it calls *meaning-based computing* systems, allowing computers to use the unstructured, ordinary-English text files that comprise the vast majority of a typical business's data holdings. By late 2008, Autonomy's advertising was focusing on the e-discovery function as the prime application of its technology.

E-discovery requires not only sophisticated software techniques but also new approaches to managing hardware. For an organization regularly involved in litigation, one problem about e-discovery is that it disrupts normal work. Chris Dale is an English lawyer specializing in e-discovery issues. He discusses the expense and disruption caused by a need to collect evidence from computers in various branch offices:

> The traditional approach would call for a technician to travel to each office and image the … machines (asking each employee to halt use of their computer for several hours while the imaging takes place). All that travel, expense and disruption take place *before* it is even determined that there is any usable information on any of those computers.[71]

By contrast, Dale discusses the advantages of a system widely used in American litigation, EnCase, which monitors an organization's hardware from a central location:

> EnCase works across the network, searching workstations, laptops, file servers, user shares, other data repositories, and removable storage media for whatever combination of file metadata, keywords, and digital fingerprints have been defined in the setup. The target files can be live and open, their users unaffected by the exercise.

At the time of writing, e-discovery is a very new issue on this side of the Atlantic, but its importance is set to grow.

8.4 Conclusion

Our brief survey of some aspects of law which matter to the IT profession is now complete.

It has necessarily been selective. For instance, we have not looked at outsourcing contracts, or employment law, or "distance selling" regulations, or computer fraud. (To me these topics seem less central; but the point is arguable.) Even the topics chosen have been discussed in only the barest outline.

But, for readers planning careers as computing professionals rather than lawyers, I hope this may be enough to give them the necessary general awareness of the legal framework within which their working lives will proceed.

Endnotes

[1] Ian Campbell, "The new skillseekers", *Computing* 13 Sep 2007.
[2] Earlier editions were entitled *Introduction to Computer Law*.
[3] Computer pornography will be examined in chapter 5, as an illustration of the difficulty law has in keeping pace with technical change.
[4] If readers wonder why Continental-style systems should be called "Civil Law", the answer is that the Romans called their law, or a central part of it, *jus civile*. This Latin phrase really meant "law of the city [of Rome]", as opposed to the laws of the neighbouring regions which Rome conquered and annexed; but the phrase looks as though its translation ought to be "Civil Law".
[5] From October 2009 a new Supreme Court is due to replace the House of Lords in this role.
[6] There are complex rules, which we shall not examine, to determine when a particular precedent is actually binding on a given court and when it is only "persuasive" – that is, the court will follow it by default but is allowed to depart from it if it has good grounds. A reader who wants the full story could consult e.g. C. Manchester and D. Salter, *Exploring the Law: the dynamics of precedent and statutory interpretation*, 3rd edn, Sweet & Maxwell, 2006.
[7] On the mediaeval Law Merchant and the idea that it is returning in a new form, see e.g. Jarrod Wiener, *Globalization and the Harmonization of Law*, Pinter, 1999, p. 161 ff.
[8] "IT contracts", in Holt and Newton, p. 1.
[9] *Op. cit*., p. 12.
[10] In 1999 the ancient term *plaintiff*, for the party who initiates a civil action, was officially replaced in England and Wales by "claimant". The older word continues to be used in other English-speaking nations such as the USA, and seems both more familiar and less ambiguous than "claimant" in this sense, so this book will continue to use the word "plaintiff".
[11] <www.itil-officialsite.com/home/home.asp>
[12] <www.isoiec20000certification.com/about/whatis.asp>
[13] For more about SLAs, see Holt, *op. cit*., pp. 10–11; and for detailed discussion of the art of drafting successful IT contracts, see particularly Jeremy Newton, "Systems procurement contracts", in the same book.
[14] A recent discussion of the question when bugs amount to breach of a software contract is Elizabeth Macdonald, "Bugs and breaches", *International Journal of Law and IT* 13.118–38, 2005.
[15] There is other, newer legislation relating to the special area of retail trade.
[16] "System supply contracts", in Reed and Angel, pp. 21–2.
[17] "Three problems with the new product liability", in P. Cane and Jane Stapleton, eds, *Essays for Patrick Atiyah*, Oxford University Press, 1991. The *Consumer Protection from Unfair Trading Regulations 2008*, which implemented the European *Unfair Commercial Practices Directive*, explicitly use "product" to cover services as well as goods.
[18] All lawsuits arising from the Therac-25 episode were settled out of court, so they yielded no precedents even for the North American jurisdictions where they occurrred.
[19] *Product Liability Directive*, article 7(e).
[20] Reported in the *Daily Telegraph*, 7 Dec 2006.
[21] "Patent protection for computer-related inventions", in Reed and Angel, p. 328.
[22] Quoted by Brian Runciman, "Berners-Lee visits key web issues", *Computing* 6 Apr 2006.
[23] House of Commons, Fourth Standing Committee on Delegated Legislation, 3 Dec 1997.
[24] Ian Lloyd (p. 413) is cynical about this, claiming that the Database Directive intentionally weakened the protection of databases in Britain in order to help other European countries to capture larger shares of this market.

[25] Readers unfamiliar with the SaaS concept may consult e.g. Sampson, *Electronic Business*, pp. 106–7.
[26] Claims at the EPO are conventionally identified as *Applicant's name/nature of invention to be covered.*
[27] "Patent protection for computer-related inventions", in Reed and Angel, p. 296.
[28] Criminal prosecutions are brought in the name of the Queen, and hence they are conventionally cited as *R.* v. *so-and-so*, where *R.* stands for *Regina*, Latin for "Queen".
[29] The name for this particular principle of legal interpretation is *eiusdem generis*, Latin for "of the same kind".
[30] Strictly, if the Obscene Publications Act did not apply, there might still have been the possibility of prosecuting under the Common Law – but not if the displays counted as cinema showings (as the Crown Court judge thought they might), because then the Obscene Publications Act exemption (point (2) above) would override the Common Law.
[31] Newer flat-screen technologies do not, so this argument might not work today.
[32] Colin Manchester, "Computer pornography", *Criminal Law Review* July 1995, pp. 546–55.
[33] "More about computer pornography", *Criminal Law Review* September 1996, pp. 645–9.
[34] David Brin, *The Transparent Society: will technology force us to choose between privacy and freedom?* Perseus Books (Reading, Mass.), 1998.
[35] Alongside the general Freedom of Information Act there are also the much more specialized *Environmental Information Regulations 2004*, which are EU-mandated law. For these Regulations, see e.g. pp. 542–5 of Timothy Pitt-Payne, "Access to electronic information", in Reed and Angel.
[36] Gateway Reviews are a mechanism by which the civil service monitors the progress of IT projects, with the aim of catching things that begin to go wrong before the situation becomes irretrievable.
[37] "Digital dilemmas: a survey of the internet society", supplement to *The Economist* 25 Jan 2003.
[38] F.G.B. Aldhouse, "UK data protection – where are we in 1991?", in K.V. Russel, ed., *Yearbook of Law Computers and Technology*, 1991. Aldhouse was referring to the 1984 Act, but this was already heavily moulded by Continental patterns of legal thought.
[39] An organization, or an individual; the law does not apply only to organizations, but I shall not repeat the phrase "or individual" below (since the main impact of the law is in fact on organizations).
[40] A.C. Raul et al., "EU privacy: European Court of Justice hands down landmark decision on EU Data Protection Directive", *CyberLaw@Sidley* Nov 2003.
[41] When a court decision is appealed upwards through the hierarchy of courts, the court which first heard the case is called the *court of first instance*.
[42] David Scheer, "Europe's new high-tech role: playing privacy cop to world", *Wall Street Journal* 10 Oct 2003.
[43] Stewart Room, "What's wrong with enforcement?", *DPA Law* 2005.
[44] SMSR Ltd, *Report on Information Commissioner's Office Annual Track 2006: Individuals*, p. 15.
[45] Cf. Sampson, *Electronic Business*, chapter 4.
[46] Though see Bainbridge, pp. 269–71.
[47] Quoted in "Argos in the clear over 49p TV e-commerce error", *ZDNet* 2 Sep 2005. Jane Winn and Benjamin Wright reported that the United Airlines website terms and conditions still did not provide protection against the type of error that occurred in its case, several months *after* the mistake was discovered (*The Law of Electronic Commerce*, 4th edn, Aspen Publishers (New York), 2005).
[48] Legal developments in this area worldwide are chronicled by the German lawyer Stephan Ott at <www.linksandlaw.com> – the following discussion draws heavily on references Ott provides.
[49] Quoted in C.S. Kaplan, "Cyber law journal: hacker gadfly at center of new suit", *New York Times* 18 May 2001.
[50]One American academic lawyer has argued that law is increasingly treating the metaphor of "cyberspace" as if it were more than a metaphor, so that laws governing the use of land (e.g. trespass in the familiar

sense) are being extended to the internet. See Dan Hunter, "Cyberspace as place and the tragedy of the digital anticommons", *California Law Review* 91.439–519, 2003.

[51] Quoted in Nicole Manktelow, "Net lawyers ponder the right to link", *The Age* (Melbourne) 10 Sep 2002.

[52] Katia Bodard et al., "Deep linking, framing, inlining and extension of copyrights: recent cases in Common Law jurisdictions", *Murdoch University Electronic Journal of Law* March 2004.

[53] Anthony Misquitta, "You've been framed", Farrer & Co. website, Spring 2001.

[54] "IP: Trademark & DNS", <www.cybertelecom.org/dns/trademark.htm> (June 2006).

[55] On the "DNS Wars", see e.g. Jessica Litman, "The DNS Wars: trademarks and the internet domain name system", *Journal of Small and Emerging Business Law* 4.149–66, 2000.

[56] Large sums do continue to be paid for attractive domain names. In 2008 the cruise community site cruise.co.uk paid half a million pounds to acquire the sister domain name cruises.co.uk.

[57] Statement of 6 Apr 2000 by Alison Sparshatt, MD of NetBenefit (rosecottage.me.uk/OutRage-archives/2000d24outcast.htm).

[58] Quoted by Hugh Muir, "Childcare expert threatens to have website shut down", *The Guardian* 8 Aug 2006.

[59] This and the Schrader quotation in the next paragraph are taken from Jason Compton, "Compliance: businesses will have to pull their SOX up", *Computing* 31 Mar 2005.

[60] Quoted by James Watson, "Banks urged to stay ahead of the MiFID game", *Computing* 2 Feb 2006.

[61] Quoted by Dave Bailey, "How data rules will burden business", *IT Week* 9 Oct 2006.

[62] Quoted by Sarah Arnott and James Watson, "UK swamped by data rules", *Computing* 18 Sep 2003.

[63] "Weighing up security and compliance", supplement to *IT Week* 24 Apr 2006.

[64] The Department of Work and Pensions offers an informal account of the current legal provisions at <www.dwp.gov.uk/employers/dda/consolidated_dda_equality_act_oct07.pdf>.

[65] For a brief summary, see p. 182 of Vivian Picton, "Accessibility and information security", in Fell, ed.

[66] <www.blether.com/archives/2006/05/dti_achieves_ne.php>

[67] "The big data dump", *The Economist* 30 Aug 2008.

[68] Quoted in "Of bytes and briefs", *The Economist* 19 May 2007.

[69] D.C. Blair and M.E. Maron, "An evaluation of retrieval effectiveness for a full-text document-retrieval system", *Communications of the ACM* 28.289–99, 1985.

[70] For a survey of artificial intelligence techniques in e-discovery, see "The Sedona Conference best practices commentary on the use of search and information retrieval methods in e-discovery", *The Sedona Conference Journal* 8.189–223, 2007.

[71] This and subsequent quotation from C. Dale, "The place for EnCase® eDiscovery in electronic disclosure for major corporations in UK courts", presented at the IQPC Information Retention and e-Disclosure Management Conference, 23 May 2008, <www.chrisdalelawyersupport.co.uk/documents/Guidance Software_EnCase_WhitePaper.pdf>.