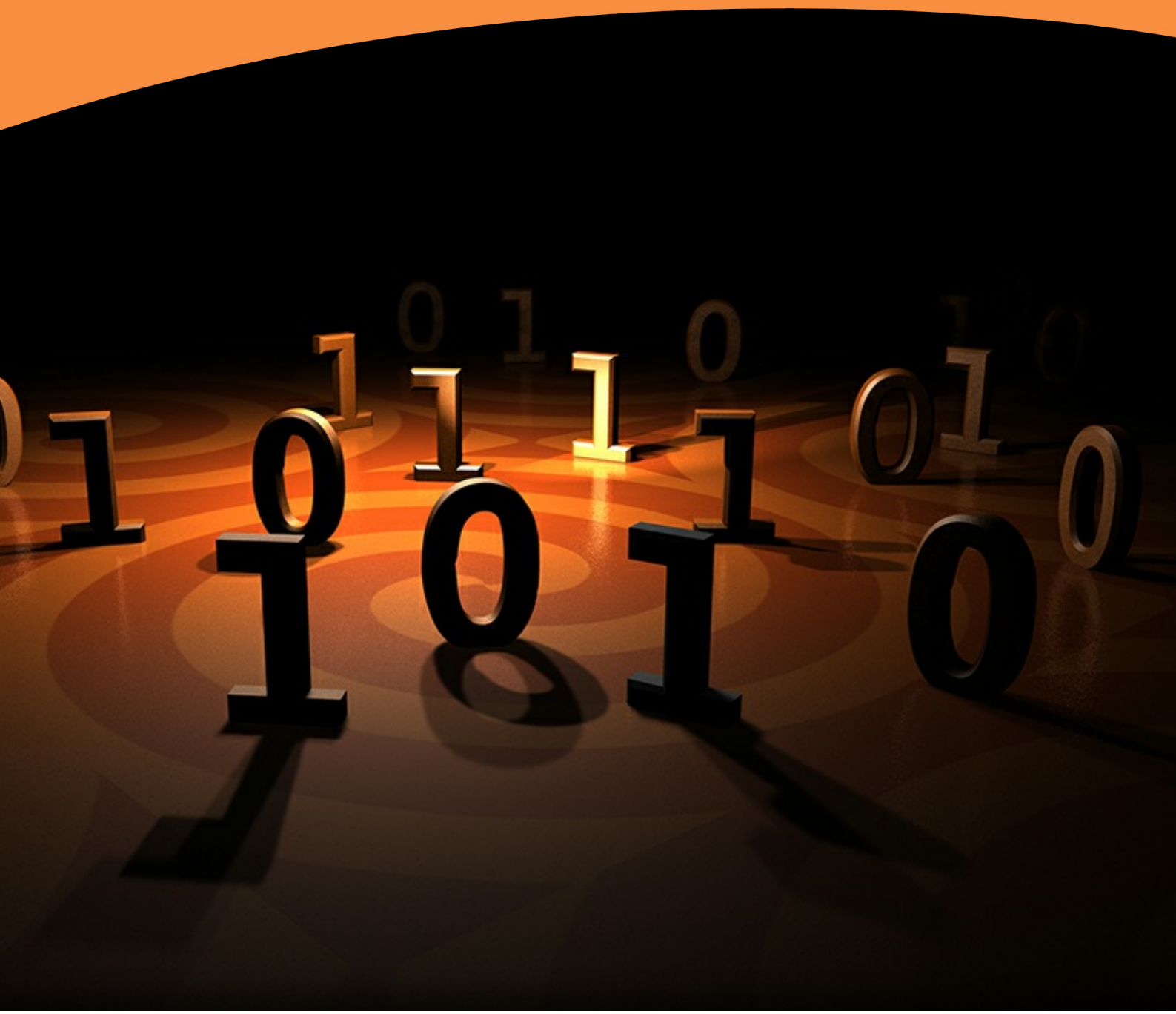
Law for Computing Students

Geoffrey Sampson



bookboon
The eBook company

GEOFFREY SAMPSON

LAW FOR COMPUTING STUDENTS

Law for Computing Students
2nd edition

ISBN 978-87-403-1972-9

CONTENTS

ACKNOWLEDGEMENTS

I should like to express my gratitude to Robin Fry and Charlotte Shakespeare, both of Beachcroft LLP (of the UK and Brussels), and to Anthony Weston LLM PhD, for comments on successive editions 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 may not last. Some people find it odd that maintaining a gas boiler requires a registered person, but at present designing the software to control a nuclear power station does not.[1] Already back in 2006 the British government made the first moves towards introducing statutory controls on entry to jobs in computer security, and it seems possible 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 cared about. But if there still exist degrees which do not yet have a strong "LSEPI" dimension, they 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, spelled the point out clearly ten years ago:

> 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.[2]

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. (The first edition of this book appeared in 2009, but by now many points in that edition are out of date.) 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. If one wants to learn about how a horse gallops or a bird flies, a photograph which freezes one instant in time offers limited help. Law, too, is a dynamic affair; it develops in response to the changing needs and attitudes of society. To understand this dynamic, and particularly to see which way the law is likely to move in the future, we shall often want to look at why particular laws were brought in, or what their effect on society has been, in addition to looking at the state of the law as it stands at the time of writing (namely 2017).

1.2 LAW CAN BE VAGUE

A central thing which computing students need to understand about law is how vague 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.

I know that computing students can find it quite hard to get their minds round this. Joichi Ito, a Japanese venture capitalist who is director of the MIT Media Lab and a visiting professor at the Harvard Law School, comments that

> Typically the people who are focused on computer science and AI don't like the messiness of the real world. Most engineers don't understand law; most engineers don't understand why governments exist.[3]

Those are sweeping statements, but there is some truth in them. If they apply to the reader, I hope that this book may help him or her to make the mental leap to a world whose texture is very different from the certainties of information technology, but which none of us, techies or not, can afford to ignore. Understanding that the law is often vague is an important part of understanding the law.

1.3 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, has originated in Europe rather than being purely "home-brewed" – and, as we shall see below, this will not cease to be true after Brexit. 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. That is

why the book often uses the terms "English" and "England", where books on other topics might be more likely to refer to "Britain" or the "United Kingdom".

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.

1.4 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 e.g.:

Catherine Elliott and Frances Quinn, *English Legal System*, 18th edn, Pearson, 2017.

Richard Ward and Amanda Akhtar, *Walker & Walker's English Legal System*, 11th edn, Oxford University Press, 2011.

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

Ian J. Lloyd, *Information Technology Law*, 8th edn, Oxford University Press, 2017.

Andrew Murray, *Information Technology Law*, 3rd edn, Oxford University Press, 2016.

Diane Rowland, Uta Kohl, and Andrew Charlesworth, *Information Technology Law*, 5th edn, Routledge, 2017.

Chris Reed, ed., *Computer Law*, 7th edn, Oxford University Press, 2011.

David Bainbridge, *Introduction to Information Technology Law*, 6th edn, Pearson Longman, 2007.

and, on important special areas of the subject:

Lilian Edwards and Charlotte Waelde, eds, *Law and the Internet*, 3rd edn, Hart Publishing (Oxford), 2009.

Christopher Millard, ed., *Cloud Computing Law*, Oxford University Press, 2013.

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*, 2nd edn, British Computer Society, 2011.

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. (Sometimes, though, an aspect of law which is covered well in one edition of a textbook will be neglected by later editions, in favour of expanded coverage of

other aspects. For that reason, I shall occasionally quote from older editions.) 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.

Details of other books and articles quoted will be found in the list of references at the end of this book. Journalistic sources, and web pages, are cited in endnotes, and I also use endnotes to explain some technical terms.

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 (and the systems of various other countries once ruled by Britain, including the Irish Republic and many Commonwealth countries) are very similar to that of England and Wales, while the legal systems of the main Continental European countries, including most of those in the EU, are rather different from the English legal system. The legal consequences of Britain's forty-odd years of EU membership mean that, Brexit notwithstanding, we shall need to look at differences between English and Continental styles of law, later in this chapter.

Because the internet links people seamlessly across national borders, in principle it can raise questions about *jurisdiction* – which country's laws apply, if problems occur? But (contrary to what some readers perhaps expect), within the field of IT law as a whole jurisdiction questions do not loom large.

They do arise sometimes. One well-publicized case related to Nazi memorabilia on the online auction site of Yahoo! (an American company with a French subsidiary). Like some other countries with first-hand experience of the horrors of Nazism, France has strict laws against activities which tend to condone or glorify that movement. French law forbids displaying or offering for sale any Nazi uniforms, emblems, etc. US law, on the other hand, lays heavy stress on freedom to express unpopular opinions, and that covers selling Nazi paraphernalia and indeed holding neo-Nazi rallies, which sometimes occur in the USA and are protected by American police. The laws are incompatible, but Yahoo!'s website was equally visible in both countries.

In the year 2000 two organizations, the International League against Racism and Anti-Semitism and the Union of French Jewish Students, took Yahoo!'s parent company and its French subsidiary to court for violating French law. Yahoo! argued that the French court had no jurisdiction, because the offending website was hosted in America; and it also argued that it was technically unrealistic to expect Yahoo! to block access from a particular foreign country, and that it would be a violation of the US constitution to restrict Yahoo!'s freedom of expression in that way.

The French court brushed aside the American constitution as irrelevant to harm being done within France, but it took the technical objection seriously. The court convened a three-man

expert panel to report on the issue: one American (Vint Cerf, one of the "fathers of the internet"), one Frenchman, and one from a "neutral" country (Britain). The panel concluded that while excluding French visitors from relevant web pages perfectly might be impractical, it would be possible in various ways to block the great majority of them. Accordingly the court required Yahoo! to do that, with a penalty of 100,000 French francs per day (then equivalent to about £9500) until they did so.

Yahoo! asked a Californian court to declare that the French legal decisions had no force against the American parent company, which it did, laying down that the French court "may not enforce a foreign order that…chills protected speech [occurring] simultaneously within our border". (Some of the means for barring French visitors were going to be visible to Americans too, although the Americans would be allowed through; hence "chilling".) The contradiction between the respective national bodies of law was very clear, and it was not obvious how in principle it could be resolved. It still is not obvious today: the Californian decision was appealed, and the appeals process yielded an extremely complex legal outcome, too messy to explain here, but in January 2001 Yahoo! made the problem go away (in this specific case) by deciding to ban Nazi and Ku Klux Klan memorabilia from its website. (American law allows such things to be displayed but obviously does not require anyone or any organization to display them.)

When issues of jurisdiction over the Internet do arise, then, they can be exceedingly difficult. But in practice they do not arise very often. The Yahoo!/Nazi case was an issue of criminal law, but the areas of law that interest us in this book are mainly commercial rather than criminal. If firms make contracts across national boundaries, they will usually settle which legal system is to apply through an explicit clause in the contract.

Furthermore, in many cases jurisdiction hardly matters in practice, because it is not practical to resort to law. In theory there are many interesting legal issues about buying and selling internationally, but, as Julia Hörnle (2009: 121) puts it,

> cross-border litigation and enforcement is so expensive and time consuming that access to redress by conventional court-based means is effectively barred for all but the largest claims (and the wealthiest litigants). For small claims, the costs and delay of cross-border litigation are frequently entirely disproportionate to the remedy potentially available.

An EU survey in 2006 showed that most consumers who were sufficiently dissatisfied with some cross-border purchase to make a formal complaint in the end just gave up pursuing it (Hörnle 2009: 158). And Hörnle's "wealthiest litigants" excludes not just consumers but many firms. Even traditional commerce within a single country depends heavily on trust –

law is there mainly to act as a long-stop. For internet-mediated international commerce, trust is very important indeed.

I have discussed problems about jurisdiction for e-commerce in my *Electronic Business* textbook, but the issue is not significant enough to discuss further in this book.

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.

Some experts believe it would be better if law did change in order to deal with IT in a more unified way. Andrew Murray (2016: 14–15) suggests that

> attempts to broker a piecemeal settlement – here a Database Directive, there a Convention on Cybercrime – are wrong-headed and will eventually lead to a fragmented approach which will fracture…instead of a law of property [it is as if] we have a law of the steam engine, a law of the gramophone, and a law of the pocket watch…[it may be] time to take a more comprehensive approach to the legal regulation of digital information rather than attempting to fit the square peg of the world of bits into the round hole of a legal system designed for a world of atoms.

This is a very interesting idea, though personally I happen to be sceptical. But for present purposes it scarcely matters, because the aim of this book is to display the law as it is, rather than as it possibly ought to be. In the early 21st century, our law certainly does not take Murray's "comprehensive approach" to IT.

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 a 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. (The essence of the Yahoo!/Nazi case was that the USA and France have different definitions of "misbehaviour".)

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 offenders (including the

Crown Prosecution Service, and regulatory agencies such as the Competition and Markets Authority, to be discussed in sec. 2.4.6), 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 (or private) 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".

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 citizens can be given a motive for making sure that they obey regulations, without being criminalized if they sometimes fail. For that matter, there is an increasing tendency today for the civil/criminal distinction to become blurry in certain areas (Ward and Wragg 2005: 16–17). But for most purposes the distinction is clear, and important.

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. A very high proportion of all crime today uses computers, and quite a lot of recent legislation is aimed specifically at computer crime. (Lloyd, 2017: 204, quotes data on the incidence of computer crime versus "traditional" crimes, though his figures are difficult to interpret.) We have new laws relating to downloading or possessing online child pornography, for instance, and laws attempting to control computer-mediated techniques of fraud, such as phishing. But most of these laws are not very relevant to a textbook like this one. Few computing students plan careers as online fraudsters – and if any do, it is not part of my job as an academic 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
- regulatory 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. Because 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.

(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".)

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 Supreme Court at the apex, 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.

(Incidentally, the Supreme Court just mentioned is very new, founded in 2009. Until then, the highest court in the UK was the House of Lords – that is, the law lords sitting as a court. Many cases cited in this book are older than 2009: references to the House of Lords are to what was the highest court at the time.)

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.

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. Manchester and Salter (2006).

The rule about precedents 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.[4] Precedents applying to 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 I 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 2013–15, that will mean that an initial decision in 2013 was appealed, and the appeal was decided in 2015.

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.[5] 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 pass 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. (A point of terminology: a proposed new law is a "Bill" while it is under consideration by Parliament, it is an "Act" once Parliament has adopted it as a law.)

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 (the then supreme court, see above) 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.

2.4.6 REGULATORY LAW

In modern times a great deal of law, particularly law relevant to business, is not directly enacted by Parliament; instead, specialist agencies (so-called "quangos", quasi-autonomous non-governmental organizations) have been set up to which Parliament delegates the power to devise and enforce regulations covering some particular area of activity. (For the detail of how legal validity is transmitted from Parliament indirectly to individual regulations made by civil servants, see e.g. chapter 4 of Elliott and Quinn 2017.) Regulations issued by these agencies are called "delegated laws" or "secondary laws". In Britain one obvious example of such an agency is the Competition and Markets Authority, which in 2014 succeeded the old Office of Fair Trading and another agency in the task of ensuring fair competition and eliminating monopolistic practices from commerce.

Regulation of competition has special relevance for our industry. In order to serve customers well, markets depend on competition between alternative suppliers of the same or similar goods or services. Competition gives suppliers an incentive to keep the quality of their offerings high and prices low – if one supplier tries to make excessive profit by raising its prices too far above the cost of production, customers will just switch to a competitor. But there can be circumstances that create monopoly situations, where a single supplier has no competition; in which case, its prices are likely to be unreasonably high and quality lower than it could be. Consequently competition authorities such as the British Competition and Markets Authority look out for cases where a firm seems to be abusing a monopoly position, and deal with them in various ways. Often they impose large fines as a deterrent, but where they see a possibility of creating a more competitive situation they may also do things like ordering a dominant firm to break itself up into independent units, or to change its business practices in specified respects.

For the IT industry, competition law (in America often called "anti-trust law") is particularly significant, because IT is full of what are called *network effects*. In many market sectors this kind of regulation is scarcely relevant, because monopolies tend to vanish almost as fast as they arise. If people see that there is currently only one supplier of X and consequently that supplier is making a killing, some of them will set out to gain a share of the attractive profits by setting up in competition, and the monopoly will be gone. But, depending on what X is, that will not always work – and IT is an area where this problem is specially salient. If you buy your groceries at Morrison's, it will not bother you that most people you know happen to favour Tesco (unless perhaps you like to combine shopping with hanging out in the supermarket aisles). Provided you like Morrison's food and prices, it is irrelevant to you whether others have the same preferences. But if you like spending time on Facebook, much of the attraction is that a lot of other people, including many of your friends, also use Facebook. Someone who set up a service similar to Facebook might find it hard to attract people to join his rival service, even if it had some special features that Facebook lacks, because initially he could not offer an established network of fellow users.

(The comparison is not perfect, because the price aspect, which is crucial for grocery shopping, does not apply to social media: there is no charge for joining Facebook. But even if there were a subscription fee, a would-be competitor could hardly get many takers just by undercutting that fee, if his network had few subscribers.)

Another special problem about competition in the IT industry is that companies tend to acquire dominant positions through ownership of massive quantities of data (about customers or potential customers).[6] Arguably, the data ought properly to belong to the individuals, if they belong to anyone, and many have suggested that monopolistic positions of this type

should be combated by requiring firms to make such data hoards into public resources. But that would be problematic because it would destroy individual privacy (a topic to be discussed in chapter 6): however one attempts to anonymize personal data, these days it is usually possible to re-link the data items to their individual subjects.[7]

Because the internet is international, regulations affecting our industry tend to apply at the EU rather than national level. I shall discuss the relationship between European and English law later, but suffice it to say at this point that the EU has regulatory agencies of its own, which are active in trying to police the behaviour of IT companies. Thus, in June 2017 the European Commission fined Alphabet (the parent company of Google) 2.4 billion euros, the largest anti-monopoly fine it had ever imposed, and ordered it to change the algorithm used by the Google search engine, which since 2008 (according to the Commission) has systematically promoted its own price-comparison website Google Shopping by displaying its response to Google search terms at the head of the first page of search results, while demoting the equally relevant responses of other price-comparison sites to low positions in the page.

Actions like this come under the heading of civil rather than criminal law: there was no danger that the directors of Alphabet might find themselves in prison. Competition laws are

complicated, and they do include some criminal law. (For instance, if the people running a set of firms which are nominally one another's competitors were secretly to agree among themselves to raise prices and avoid undercutting one another, that would be called a *cartel*, which certainly is a criminal offence that regularly leads to prison sentences.) But the criminal aspect is only a minor element of competition law as a whole.

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

We know that Britain will soon be leaving the EU. Readers might well think "Why is he bothering to tell us about European law? In a few months' time it will be irrelevant". But things are not that simple, for two reasons.

In the first place, one of the first things that Parliament is going to do in anticipation of our leaving the EU is to pass a law called the *Great Repeal Bill* (Caird 2017).[8] What this will repeal is the 1972 *European Communities Act* which gave European law supremacy over English law. But at the same time as doing that, the Great Repeal Bill will turn much of the specific content of European legislation into English laws – the laws will be the same, though in future they will apply because our Parliament says so rather than because the EU says so.

That might sound crazy. We are leaving the EU because our population dislikes being governed by European laws, so we begin by adopting those laws wholesale. Where is the sense in that?

But if it were not done, there would be large gaps in the law – areas which at present are governed by European laws would fall outside any legal framework, which for businessmen in particular would be a fairly horrifying prospect. Once Brexit has happened, we shall be free to change or repeal any specific European laws that don't suit us. But changing laws is a complicated, long-drawn-out process, in which many parties with different interests need to be consulted. To try to come up with a full set of UK-friendly alternatives to EU laws

in the months before we leave would be like rebuilding a ship from keel up in mid-ocean: quite impractical. So we shall begin by retaining European laws, and then change those that need changing at our leisure.

The other point is that even after Brexit we may want to agree to the EU retaining some influence over specific, limited areas of our law. At the time when I am writing, nobody yet knows what kind of bargain British negotiators are going to strike with their EU counterparts. But it seems quite possible that the Europeans might say something like "We can offer you favourable access terms to the Single Market after Brexit, but only provided you accept EU control over this or that aspect of commercial law, to ensure that your traders and ours are still competing on a level playing field" – and that could be a bargain that the British side was willing to accept.

The second of these points is uncertain – even if we are offered that type of bargain, our government could decide that it is not worth accepting. But the first is definite, indeed by the time you are reading this the Great Repeal Bill will very likely already be an Act. Hence it is still highly relevant in a book like this to say a little about EU law, which is very different in kind from traditional English law.

(Incidentally, some commentators see the task of disentangling Britain from EU legislation as so problematic that we might have done better to vote Remain for that reason alone, independently of any other considerations.[9] It is hard to take that too seriously, just as I am sure that no-one would have taken very seriously any Americans in 1776, or Irishmen in 1916, who argued that independence from Britain might be nice but separating the legal frameworks made it just too difficult to proceed with. But the fact that anyone could think like that underlines the point that even as we head towards the Brexit door, we still need to know something about EU law.)

So what exactly is the relationship between European and English law?

Before the UK joined what is now the European Union in 1973, 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 to which Parliament delegated certain limited law-making powers. Joining the EU 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, while we remain in the EU the European law takes precedence. By recent years a large proportion of all new legislation has been 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 mainly 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 mainly be Acts of the Westminster Parliament, but Acts introduced in response to EU Directives rather than on Parliament's own initiative.

(It might sound as though repealing the European Communities Act ought not to affect these Acts, since they were passed by our Parliament. In fact repeal will undercut them too, for reasons having to do with the distinction between so-called *secondary* and *primary* legislation which are too technical to enter into in this book.)

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 has sometimes been 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 have been coming into English law, we shall see that this contrast has sometimes led to practical difficulties for English courts, which have to interpret legislation in a manner that conflicts with their training. The European dimension has led to compromises in legal "styles" (on both sides – the English approach has influenced 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 has been a factor making for more unpredictability in our business law than it might otherwise contain.

It remains to be seen how far these innovations in English legal style will continue to influence our legal régime after Brexit (the present generation of judges have spent their entire careers as EU citizens, after all), or whether English law will throw off European influences entirely and revert to operating in its traditional style.

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 (see Trakman 1983). 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.

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 a court in the place where it arose; their livelihood depended on keeping on the move, and next week they might be in some place whose courts would have no interest in the quarrel. 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. For instance, Thomas Schultz (2008) argues that phenomena such as the system for resolving disputes between buyers and sellers on eBay (which is independent of any state-enforced system), and the rules of ICANN (the body which ultimately controls the system of internet domain names, discussed in sec. 7.4.1 below), are clear cases of "law" in every sense of that word – even clearer, Schultz believes, than mediaeval law merchant – and require legal theorists to rethink how we define the concept of law. (See, too, Wiener 1999.)

That 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 specially 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 few 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 (2011), 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?

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." 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 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.)

Indeed, the plaintiff probably would have lost a more recent comparable case, *BSkyB v. EDS & ors* (2010), were it not for a problem about the defendant's evidence that had nothing to do with general issues about IT contracts. This case is worth discussing if only because it was one of the most expensive in English legal history (legal costs were estimated at £70 million) – and because the problem just mentioned was too amusing not to include here.

A consortium led by EDS contracted to supply BSkyB (the formal name for Sky television) with a "customer relationship management" system (on CRM software see e.g. Sampson 2008: 155–7). The contract specified that the system should be up and running within nine months, but in the event it took closer to five years. Sky sought over £700 million in damages, largely because unsatisfactory customer relationship management in the mean time had led, Sky claimed, to many customers terminating their subscriptions.

The contract specified a far lower limit to liability for breaches, and it included an entire agreement clause. The judge accepted that these elements of the contract were valid on their face. The only reason why he in fact found in favour of BSkyB (and the two sides settled on a damages figure of about £300 million) was that EDS was remarkably unfortunate – or foolish – in its choice of its main witness, a man who had been instrumental in persuading BSkyB to enter into the contract. This man's academic qualifications became an issue in the case; he claimed to have an MBA business degree, but BSkyB contended that this was bogus, saying that the organization which issued it did no teaching or assessment but was a scam selling certificates to anyone willing to pay for them. The witness went to considerable lengths to rebut this. But (quoting Lloyd 2017: 507) although he "presented what appeared to be a transcript of his class marks and a (glowing) letter of recommendation from the college principal", the impact of this was severely undercut when BSkyB's lawyer showed "that an application made on behalf of his dog [had] produced an MBA, an identically worded letter of recommendation, and a rather better set of class marks"! It was so clear that this witness had lied, at length and in detail, about his qualification that the judge felt bound to distrust the rest of his evidence, and consequently accepted BSkyB's contention that they had been cheated into agreeing the contract – which invalidated it.

So in this case too the client of the software house essentially won. But other firms which find themselves in dispute with software suppliers can hardly hope to face hostile witnesses who lay themselves open to such spectacular demolition.

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.

3.4 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".[10] 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").[11] But these general standards are only guidelines; they cannot in themselves produce a suitable SLA for a particular contract.[12]

3.5 CLOUD COMPUTING

One development which has given the details of service level agreements much greater significance for the IT profession than when the first edition of this book appeared is the growth of cloud computing, whereby data processing occurs not on a firm's own machines

but on machines belonging to a separate company and located elsewhere – indeed, the cloud service provider will often itself subcontract the work, so that it may in practice be quite impossible for the owner of data to know where in the world they are being stored or who is actually doing the processing.

For many companies, getting their computing needs executed "in the cloud" has large advantages, so that by 2013 it was reported that more than half of all American businesses were already using it.[13] Apart from the general advantage of not having to tie capital up in fast-depreciating assets, if a firm's processing needs vary widely from time to time (in some cases, from moment to moment) it can pay just for what it needs at any given time, rather than needing to provide permanently for peak demand. However, the fact that the client firm loses physical control inevitably means that tieing down the contractual details of the services to be provided becomes crucial.

Various chapters in Millard (2013) give a wealth of hard information on what kinds of term appear in current cloud contracts, and how the terms have tended to change in recent years as providers and clients have been gaining more insight into the technology and their respective bargaining positions. It is clear that cloud providers have their fair share of the ruthlessness which Jeremy Holt (in sec. 3.2) attributed to IT suppliers in general. On the basis of a large-scale survey of current practice, Kuan Hon et al. (2013) note that

> Providers' exclusion of liability, particularly for outages and data loss, was generally the biggest issue…providers usually state that liability is non-negotiable, and "everyone else accepts it". Even large users had difficulty getting providers to accept any monetary liability. One global user stated that generally it "had to lump it".

To be fair, providers may be forced to exclude liability for monetary losses, because "unlimited liability could put smaller providers out of business". But one might expect cloud providers to recognize that their users are themselves under various legal obligations about how they handle data, which the providers need to help their clients to fulfil. According to Kuan Hon et al., not so:

> A common theme was that many providers…would not consider that users have regulatory or other legal obligations, and that they may need to demonstrate compliance to regulators. Some users expressed frustration at providers' lack of empathy with their compliance obligations, especially in Europe. Some users addressed this issue by using cloud only in less highly regulated jurisdictions, for example certain Asian countries.

A special problem for cloud computing arises from the US *Patriot Act 2001*, passed in response to the 11th September Twin Towers attacks. Under this law American authorities can require to see any data located within the USA or within the control of an organization subject to US law, without the data owner's consent (or indeed knowledge). One issue with this is that if data relating to individuals are moved from the EU to the USA without consent, that violates EU data protection law (to be discussed in chapter 6). In 2011 Gordon Frazer, MD of Microsoft UK, acknowledged that companies like his, as subsidiaries of American firms, could not guarantee that data would not be transferred out of the EU under Patriot Act requirements. The data protection law is essentially about personal privacy. But the Patriot Act creates problems for business also: a firm will not want its confidential information passed out of its control. In 2011 the defence contractor BAE Systems decided it could not use Microsoft's Office 365, which uses cloud storage, partly for this reason.

3.6 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.

Here (and elsewhere in this book) I am assuming that the contract in question is written so as to be governed by English law. Nothing requires contracts executed in England to be governed by English law, though that is the default. Probably the law of a foreign country would be specified only in cases where one party to the contract has connexions with that country. But it is quite common for a contract to 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.

However, we shall be considering how contracts are interpreted under English law. We shall look at five areas:

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

3.6.1 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. (This was the kind of exclusion referred to in the quotations from Kuan Hon et al. in sec. 3.5. The loss of customers in the *BSkyB* case discussed in sec. 3.2 was a consequential loss.) If the IT industry is to flourish, it is often reasonable that consequential liabilities should be excluded. IT products are sometimes 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.

3.6.2 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 (of which I am one) – 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 decides to classify us with greengrocers rather than doctors, and accepts no excuses when software is unfit for purpose.

For many years, the question has been open with respect to English law: it simply was not settled which side of the goods/service boundary software falls, despite the potential importance of the issue for suppliers. (Antony Taubman, 2009: 42, discussed the fact that, internationally, the issue has been a bone of contention between the USA and EU, with America wanting to classify digital products with goods while Europe wanted to class them as services.) 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.

In a very different context (namely, keeping statistics on international trade), a United Nations department in 1998 recommended distinguishing software packages marketed to numerous customers from bespoke software developed for an individual client to execute a particular task: the former should count as goods, the latter as a service.[14] This recommendation of

course had no force in terms of the English law of liability, but for our profession it would serve well if the law were to adopt it as a criterion. The companies which market standard packages could live more easily than individual programmers with the risk of occasional liability claims arising from damaging program behaviour that could not reasonably have been foreseen. Until recently it was anyone's guess whether English law would in fact take this line. But in two recent cases (*Fern Computer Consultancy v. Intergraph*, 2014, and *The Software Incubator Ltd v. Computer Associates UK Ltd*, 2016) the respective judges stated very explicitly that packaged software should be seen as "goods", and that in the modern digital world one cannot maintain the traditional assumption that goods are tangible objects. (Another important feature of the 2016 decision was that it laid down that what is sold in the case of a standard package is the actual software, despite the fact that it is intangible and that software houses invariably assert that what they are selling is only a licence to use the package, not the software itself.)

By standard methods of legal interpretation a statement that packaged software in particular is "goods" might be taken to imply that bespoke software by contrast is a "service". So the outlook for our profession on this issue is reasonably optimistic.

3.6.3 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.

(Incidentally, the law provides a standard means for avoiding problems arising from software houses keeping source code secret, though perhaps it might not have been relevant in the specific circumstances of the Merant case. Commonly, the contract between software house and client will provide for a copy of the source code to be lodged with a trusted third party, so that if the software house goes out of business the source code can be released to the client – in legal language the code is said to be held *in escrow*. Leigh and Wood 2011 discuss the practicalities of this aspect of software contracts.)

Another common reason for adding an implied term to a contract 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 (2005: 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".

Courts have come to 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).[15]

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.

3.6.4 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.* (There is further, newer legislation relating to the special area of retail trade.)

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 manufacturer (it was later 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 was for a time so adverse to suppliers that by 2001 the profession was asking "Do the Courts have it in for the IT industry?" (Newton 2011b: 23 – later, Jeremy Newton began to detect signs that the tide may have turned somewhat in favour of suppliers).

3.6.5 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 (2005: 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.

3.7 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 involving personal injury, damage to property, or the like. Furthermore, so far as I am aware no significant cases of this kind have come before the courts. I found that surprising

when I wrote the first edition of this book; eight years later it still seems to be true, and is all the more surprising.

Injury and damage to property are not the only kinds of thing which the law calls "torts". Defamation – libel and slander – is another, and we shall be looking at defamation via the Web in sec. 7.5 below. But, leaving that aside for now, there just does not seem to be much to say, yet, about tort by computer. David Bainbridge (2007) had a chapter, chapter 23, on torts, but it is almost wholly about defamation. (He also discussed the possibility of causing harm through negligent misstatements of fact, which might of course be done via the Web but might equally be done over almost any other channel of communication – it is scarcely a specifically IT-related issue.)

There was a 2014–15 case, *Vidal-Hall & ors v. Google*, where the plaintiffs persuaded the Appeal Court that Google's use of information about their pattern of web visits (which Google obtained via cookies which they had tried to block) should be treated as a kind of tort, but this was not very similar to the things we usually mean by "tort", and the *Vidal-Hall* case was really about data protection and the right to privacy, matters that are normally handled via laws which this book will consider in detail later. Tort law came into the *Vidal-Hall* case only for technical reasons related to the fact that Google is a foreign firm.

So the upshot is that anything said about how existing tort law will be extended or changed to address "typical" torts that crucially involve IT can be only educated guesswork.

3.7.1 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 – the manufacturer. 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". Even if it were clear that software counts as "service" rather than "goods", it might at the same time count as "product".

Jane Stapleton (1991) suggested that the European legal system was 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. In the case of things bought by consumers, the issue is now settled by the *Consumer Rights Act 2015*, in part implementing another European directive, and Jane Stapleton was correct: software does count as a "product". (I am not aware whether the question has yet been settled for the case of business-to-business trading.)

If there is strict liability for damage caused by bugs, a further issue arises 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 (2005: 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. (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 occurred.) 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? We do not know.

3.7.2 "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"?[16] 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 recognizable 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, Ian Lloyd argued (2008: 569) 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.

3.8 THE RISE OF ARTIFICIAL INTELLIGENCE

The Therac episode involved a computer carrying out a purely mechanical task, though (as we all know) there can be bugs in programs to do the simplest things. Deeper legal issues are beginning to arise with artificial intelligence (AI) systems, which autonomously execute activities or take decisions that traditionally required human intelligence or discretion.

Ever since the 1950s, the prospect of artificial intelligence has fascinated many computer experts, who saw it as coming just a few years round the corner – but for decade after decade it continued to be just round the corner, so that some of us concluded it probably always would be. Suddenly, though, in the last few years AI has become a reality in many areas of everyday life. Robot workers have come to pose such a threat to future human employment that in 2017 Bill Gates argued for taxing robots like human employees, to level the playing field and provide funds to ease the humans' transition into new careers,[17] and the European Parliament considered (but rejected) a proposal to do just that.

Surprisingly, most discussion of relationships between law and AI has been about the possibility of AI systems doing lawyers' work, for instance automatically establishing how a complex set of laws apply to the details of a specific case. (The idea that AI may make many lawyers redundant is a live issue among that profession – see Susskind 2008. The *Artificial Lawyer* website, <www.artificiallawyer.com>, carries many news items about applications of AI in the legal profession.) More relevant for us are issues about the legal implications of allowing intelligent decisions (in any sphere of activity) to be taken independently of human control. These issues have been very little discussed to date. (For instance, the Wikipedia article on "Artificial intelligence and the law" which I accessed in March 2017 was entirely about the former and did not mention the latter issues.)

One area which has, understandably, attracted a lot of attention is autonomous weapon systems. Already we have drones firing lethal weapons in the Middle East under the control of operators thousands of miles away in the safety of the USA, which itself raises very worrying ethical issues. But the obvious next step, probably not all that large a step technically, is to equip the drones with AI software that identifies targets and decides to attack without any human intervention.

This would create massive ethical questions, whatever one might feel about the rights and wrongs of a particular conflict. (These grave questions are discussed e.g. by Russell 2015. In Britain they ceased to be merely hypothetical in 2017, when the defence contractor BAE Systems announced plans for a "robot tank" system, "Ironclad".[18]) But while the ethical situation is so unclear it may be premature to discuss legalities. Law cannot be wholly based on moral principles but it certainly needs to reflect them where it can. (And in any case warfare and law never sit comfortably together.) Let us consider instead an area where new technology has not noticeably challenged our existing moral intuitions, but where there are large questions about how law should respond to it.

Self-driving motor vehicles are already travelling on public roads, and many commentators predict that they will fairly soon replace a large proportion of human-driven traffic, perhaps eventually all of it. In May 2016 in Florida they produced their first fatality. Joshua Brown, the driver in a Tesla Model S (to date, at least, every self-driving vehicle has a human at the wheel who can override the software in emergencies), was killed when a trick of the light led the Tesla software to fail to recognize an 18-wheel articulated lorry crossing the highway, so that the Model S ploughed into it at speed.

The Tesla company pointed out that this tragic accident still left their self-driving vehicles safer, in terms of the ratio of deaths to miles driven, than conventional vehicles. Indeed, the prospect is that when the roads are full of self-driving vehicles there should be fewer accidents than today. Furthermore, without making light of the tragedy one might argue that Joshua Brown knew the risks he had chosen to take on (he was a Tesla enthusiast and owner of a new-technology firm). Nobody expects that self-driving technology will be abandoned just because perfect safety has not been achieved.

But what will happen, when a self-driving car injures or kills someone in another car, or a pedestrian – as is surely inevitable sooner or later? How will the law share out responsibility between the suppliers of the software, and the driver who failed to override it in an emergency situation? It is unrealistic to expect those in charge of self-driving vehicles to maintain the same attentiveness as drivers of conventional vehicles; in 2017 a House of Lords Science and Technology Committee report found that "In simulated emergencies, up to a third of drivers of automated vehicles did not recover the situation, whereas almost all drivers of manual vehicles in the same situation were able to do so."[19] (Perhaps a share of responsibility should go to the owner of the vehicle: conceivably there will need to be a duty on firms which use fleets of self-driving vehicles to satisfy themselves that the software is reliable, though for most transport companies discharging such a duty would be very difficult.) Can these open questions be resolved by extending existing laws to cover the new phenomena case by case, or will new statutes need to be enacted to address them? And bear in mind that self-driving vehicles are only one practical application of AI. Plenty of others are in the pipeline, and many of those will surely create their own, equally novel, legal problems.

There are even some who argue semi-seriously that if AI systems are "intelligent" they should be treated as legal persons who can be prosecuted in their own right, though I do not believe that idea is worth pursuing very far.

At the time I am writing, the law has barely begun to respond to the challenge of AI.[20] (The House of Commons Science and Technology Committee broached the issue of how British law might do so in the report of its enquiry into "Robotics and artificial intelligence", published in October 2016.) So I can only point to questions, not describe any answers. But it seems sure that those who are computing students today will witness large and important legal developments in this area.

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.[21]

What Brown was saying was that most property of the "top companies" is now intellectual property; and it is largely IT which has brought about this change. Likewise, a 2016 report (Manyika et al. 2016) finds that while international trade in goods and finance has been slowing, cross-border digital flows have grown so rapidly, from almost nothing at the start of the century, that they now have more impact than the trade in tangible goods on overall GDP. These changes naturally mean 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 (or fairly clear at least, though see Murray 2016: 51–4); 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 those involved do not care whether their activity is legal, provided they feel safe from detection! In civilized societies, most companies 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 might be

hard for a business to flourish, 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 (2007: 328):

> 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.

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 applies 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. According to Michele Boldrin and David Levine (2013), there is plenty of evidence that patent law has failed in its nominal purpose of promoting useful innovation. And in connexion with copyright, 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 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.

Particularly in the IT domain, one special problem about patents is the rise of so-called *patent trolls* – people or companies which buy up little-used patents not in order to execute the processes they cover but in order to issue legal threats to parties who, they claim, are infringing the patents. The lawyer Alistair Maughan explains that "They're mostly based in

the US, as the damages are set by jury and can get very large… If you're prepared to enforce aggressively, people will pay you to go away."[23] In 2013 a new American law, the *Innovation Act*, attempted to address the most blatant abuses (and, perhaps as a consequence, in 2015 it was claimed[24] that the trolls are now migrating to Britain). But comparable behaviour is not confined to fly-by-night outfits. Hamadoun Touré, secretary-general of the International Telecommunications Union, complained in 2012 that "We are seeing an unwelcome trend in today's marketplace to use standards-essential patents to block markets. There needs to be an urgent review…patents are meant to encourage innovation, not stifle it."[25] (The context was the "smartphone wars" between Apple, Samsung, and others over the iPhone and its rivals.)

Another view accepts that there is a need for intellectual-property laws in our field, but holds 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. Those who take this view 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.

(It is worth adding briefly that one technology commentator, Jaron Lanier (2014), argues that the continuation of free and democratic society requires a massive *expansion* of something like copyright law to cover the value of the data which at present is freely surrendered by ordinary individuals through their interactions with Facebook, Google, and other major internet players. Lanier's book is not an easy read, but he is the only thinker I have come across to identify and outline a possible solution to what is becoming a very serious social problem created by the internet. However, discussing Lanier's theme would take us too far away from the topic of the present book.)

4.4 COPYRIGHT FOR SOFTWARE

One question for our industry is whether copyright applies to 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 licence 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.

(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. This was confirmed by the decision in a 2010 case (*SAS Institute v. World Programming Ltd*), and Andrew Murray's summary (2016: 255) is that "it is difficult to think of an occasion where non-literal copying would be upheld [as being a breach of copyright] now".

Incidentally, discussions of this area in law textbooks often confuse two different kinds of similarity between programs. After Apple commercialized the first 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. Already in 1997 a Department of Trade and Industry minister said:

> 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.[26]

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, and databases are now protected by new legal rules independent of both the copyright and the patent régimes.

(Not everything that you or I might think of as a "database" counts as one for the purpose of the European Directive. In *Football Dataco & ors v. Brittens Pools & ors*, 2010, the data in question were fixture lists of English and Scottish football associations. A football fixture list is not merely a mechanical assembly of pre-existing data-points, like a phone directory; drawing it up involves skill in balancing various requirements – for instance, a town will not want a home match to clash with some other big event in that town. This put it outside the scope of the Directive, and the case was decided in terms of ordinary English copyright law.)

Unfortunately, in cases where they do apply 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 more than half of all databases in the EU.

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 has changed
- 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 HAS CHANGED

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. Developments such as SaaS (software as a service) have been accelerating this trend. (For "SaaS" see e.g. Sampson 2008: 106–7.)

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 – as yet there is no such thing as a single Europe-wide patent, though a unitary EU-wide patent is likely to become available soon.) 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, at least 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 it as meaningless and empty – even if it is. Cases are being fought out to give it a meaning. The trend of the decisions has been towards increasing willingness to grant patents for software. Unfortunately, the trend has also turned 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.

PBS Partnership/controlling pension benefits system (1995)[27]

In 1995, PBS 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.)

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 Ian Lloyd remarked (2008: 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".

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 (2007: 296) commented "The reasoning of the [EPO] Board in finding (as they did) technical content in the *Sohei* case is at times impenetrable".

The situation became 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 was impossible to follow EPO precedents, because the EPO was not following its own precedents consistently. Over the period 2007–10 the British authorities made repeated attempts to ask the EPO to resolve the problem, but the EPO simply repeatedly denied that it had been inconsistent.

(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 became 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.

(Most authorities associate the beginning of American software patents with the *State Street Bank* decision, but Daniel Tysver traces it earlier, to a 1981 case, *Diamond v. Diehr*.[28])

This expansion of American patent law is being amplified by a separate development, independent of IT: excessive workload has been 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 was 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.

(Interestingly, since 2009 the US patent office has been addressing the excessive-workload problem by opening up the claim examination process to the public in a "Peer to Patent" scheme described by Wikipedia as "the first social-software project directly linked to decision-making by the federal government". The UK patent office ran a six-month trial of this approach in 2011–12, but appears not to have taken it further.)

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 tightly bound together as they are nowadays, for their patent régimes to be far 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 was 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 to some extent reined in the patentability of business methods and software programs – but in 2010 that decision was partly overturned by the US Supreme Court, and at the time of writing the American situation, too, is fairly murky. (The most relevant recent Supreme Court decision, in *Alice v. CLS Bank* (2014), has been described by one observer, Gene Quinn, as boiling down to deciding that software is not patentable but business methods are, which Quinn finds "bizarre and inconsistent".[29])

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!

4.13 INTELLECTUAL PROPERTY IN WEB CONTENT

So much, then, as far as intellectual property in software is concerned. But what about the content of websites? Much more obviously than software, the wording and graphics contained in webpages are exactly the kinds of thing that copyright law is designed to protect.

There is something logically odd about copyright law applied to Web content. With traditional printing, all the copying was done by the copyright-owner or someone working for him; but any act of downloading a webpage involves copying a file onto one's own machine from a master file on the rights-owner's server. On the face of it this might imply that anyone who browses the internet is repeatedly breaching copyright law. That would obviously be an absurd situation (after all, people normally put material on the Web with the intention of enabling others to download copies), and the common-sense position must be that there is a difference between copying a file to the extent needed to view it in a browser, and taking a copy to distribute to others. Perhaps remarkably, only in 2014 (in the case *Public Relations Consultants Association v. The Newspaper Licensing Agency Ltd & ors*) was it settled that English law agrees with common sense in this respect: visiting a webpage is not breaching copyright.

On the other hand, someone who incorporated into his own website passages of prose, or graphic material, originated by some other rights-holder and having economic value, would be clearly breaching that other's copyright, just like someone who printed off and sold copies of Harry Potter books independently of J.K. Rowling and her publisher.

But that is not the kind of issue which typically arises. More commonly, someone (let us say 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 A 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.

(There have been repeated attempts by a number of Continental countries to legislate to force Google, and other internet companies which copy snippets from print newspapers into their websites, to pay the copyright owners. At the time of writing the EU is considering proposals for European copyright reform which would include such a feature.[30])

Perhaps more clearcut than the Shetland case 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, 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 (Bodard et al. 2004) 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".

("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. Anthony Misquitta, of the distinguished London law firm Farrers, believed 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.[31] But he 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!

What about a situation where website A links to website B, and B breaches C's copyright? Is A also in breach?

This question was answered, for EU law, by a 2016 Dutch case, *GS Media BV v. Sanoma Media Netherlands BV & ors*, which established that in EU law linking for financial gain to material which appears on another site in breach of copyright is itself a breach. Sanoma, the publisher of *Playboy*, commissioned nude pictures of a young lady called Britt Dekker for publication in the magazine, and somehow copies of the photos found their way onto an Australian content-distribution website. GS Media is a Dutch news website which included a link to the pictures in Australia, despite Sanoma asking it not to. The question was whether this amounted to a "communication to the public" in the sense of the EU *Copyright in the Information Society Directive*, and the decision was that it did, and hence GS Media (and not just the Australian site, which was outside the reach of EU law) was in breach.

So this last issue is now settled in a clearcut way. But more generally the law on intellectual property in Web content seems at present far from settled. I shall leave the last word to a judge, Mr Justice Arnold, who in a 2014 academic lecture on intellectual property said of the current English copyright law that

> Amendments have repeatedly been made to earlier amendments. To call the result a patchwork quilt would be an insult to the art of quilting…the [Copyright] Act lacks coherence…the law is inaccessible to creators, exploiters and users of copyright works, which is to say, everyone in the UK.[32]

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. Squeamish readers need not fear: we shall not be looking at the fleshy realities of porn at all, only at the laws which try to control those realities and the technologies to which the laws have to adapt. 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.

5.1 FILM VERSUS VIDEO

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*.

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 technological development 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),[33] 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 two 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, 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 – hence point (3).

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. (The name for this particular principle of legal interpretation is *eiusdem generis*, Latin for "of the same kind".) 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.

(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 would override the Common Law.)

The defendants in this particular case were acquitted and there could be no question of reopening that issue. But when the Attorney General (the officer in overall charge of criminal prosecutions) believes that an acquittal may have been wrong 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, (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. (Though newer plasma-screen technology does not, so that

argument might not work today.) 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 have supposed 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 PORN 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 fact 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. Jenny Kleeman notes that:

> Online pornography pushed the growth of the internet, transforming it from a military invention used by geeks and academics to a global phenomenon. Pornography was the motivator behind the development of streaming video, the innovation of online credit card transactions and the drive for greater bandwidth.[34]

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 (1995). 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 their 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 a later 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 some ten years after the Act was passed.

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 twenty years since Manchester was writing, and the pace of innovation in IT has probably been even faster over this period than it was before.

5.6 *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 (Manchester 1996). 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.

5.7 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 found that it had. The judge did not make explicit *how* any of these words applied in the case of files downloaded over the internet, but Manchester felt that this gap in the Crown Court judgement could be filled in from wording elsewhere in the document.

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.

5.8 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, and the reason why the Crown Court judge was not explicit about it in connexion with the Obscene Publications Act was that he had already covered it, discussing the "key to the library" analogy, in connexion with the Protection of Children Act. But this latter act offered further possibilities for defeating the prosecution.

The Protection of Children 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, *might* be a "copy of a photograph" (if a copy of a copy of X is legally equivalent to a copy of X); but a set of 0s and 1s on a hard disc 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 implied 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 A and B, and A is capable of being understood either in a broad sense which would include B as a special case, or alternatively in a narrow sense in which it contrasts with B, then the legal rule is that the mention of B will be a reason for taking A in the narrow sense – otherwise it would be redundant to mention B. If we set A = "copy of a photograph" and B = "data stored on a computer disc", it might look as though the reference to B requires us to interpret A 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 B in that statute might impose a narrow interpretation on wording A 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.

5.9 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.

Since the Acts referred to above there has been new legislation – notably sections of the *Criminal Justice and Immigration Act 2008*, the *Coroners and Justice Act 2009*, and the *Criminal Justice and Courts Act 2015* which aim to deal with "extreme pornography", child pornography, and the new problem of "revenge porn" respectively. But the purpose of this chapter has not been to inform the reader about the current state of the law, rather it has been to use a case study so as to give the reader a feel for the difficulties law has with the imprecision of language and with fast-changing technologies. The most recent legislation seems not yet to have thrown up interestingly problematic cases, so I shall not discuss it.

5.10 THE WIDER IMPLICATIONS

One 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. An 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 parallel 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. While Britain has been 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 does make 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 connecting 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 (1998) has called a "transparent society", where no-one any longer has a side of their life which is private. 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 are supervised by a civil servant called the Information Commissioner, who decides how in detail the statutes should be interpreted, promotes compliance with them, takes 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. Both areas 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.)

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.

Sometimes it is clear that there is no public interest in making a given category of data available, but it has to be handed over anyway. In 2011 Kingston University received a Freedom of Information request for a list of university e-mail addresses of all employees who had them. It was manifest that the applicant's purpose was to use the addresses for mass marketing (i.e. spam), and the University tried to refuse; but the applicant appealed to the Information Commissioner, who told the University that the law required it to comply, except in any cases of individuals who might experience "potential serious harassment from estranged family members or partners". (How the University was expected to filter out those cases was not clear.)

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 decision was 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 & 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 then 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 could not 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.)

On the other hand, a public body is to some extent expected to run its affairs so as to make complying with Freedom of Information applications not too burdensome for itself. In my experience as a university don, my colleagues and I would file our e-mails in individualistic, not to say chaotic ways. If it were necessary to comb through this material to produce a response to some freedom of information application (and e-mails are within the ambit of the Act), the university could very easily have put its hand on its heart and said that this would take far more than three man-days. But, legally speaking, this answer might not have been satisfactory. A statutory code on records management has been issued under the Act, which

> requires all public bodies to treat the records management function "as a specific corporate programme". The Code emphasises that electronic records, such as emails, should be managed with the same care accorded to manual records, and that the records management programme, "should bring together responsibilities for records in all formats, including electronic records, throughout their life cycle, from planning and creation through to ultimate disposal."[36]

The only adequate solution might be "a state-of-the-art e-mail storage facility with enhanced retrieval and management capabilities".

It is clear that the Act does create a large drain on public resources. By 2012 the Ministry of Justice was arguing that it was wrong for so much taxpayers' resource to be diverted into

a system that mainly benefited journalists and private-sector companies. That problem might be addressed by imposing a small fee for information requests. (When Ireland did that with their similar law, the volume of applications fell by three-quarters.) But, more significant, the Ministry report also suggested that the Act might be working counterproductively. Officials can only be asked to reveal records where written records exist, so the Act was encouraging civil servants to avoid writing things down (and hence was making the processes of government even more opaque than they had been). In the memoirs he published after ceasing to be prime minister, Tony Blair had described the Act his government had brought in as "dangerous" and himself as a "nincompoop" for sponsoring it. However, the select committee of MPs which considered these issues later in 2012 recommended no major changes to the law, and in 2016 a government minister announced that the idea of charging would not be taken up.

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 an 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 was a Brighton journalist and MD of John Connor Associates; 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 the responding body is not allowed to impose any duty of confidentiality on the applicant, so 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, which chose to introduce the Act, has been aggressive in claiming exemptions for its own data.

For instance, at the period when the Act came into force there was a political controversy about the proposed introduction of a nationwide system of identity cards. Many people objected to this on several separate grounds. It was seen as a threat to civil liberty; it was 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. (Eventually, after a change of government, the project was abandoned.)

In 2006, while the identity card project was live, the Office of Government Commerce refused a freedom-of-information application for information about the outcome of Gateway Reviews of the project. (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.) The identity card project looked like just the kind

of thing which motivated the introduction of the Act: it was publicly funded, and many members of the public had 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 of young people to expose their personal lives on social networking sites like Facebook and YouTube. Those of us who were young fifty 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. To many older people, the millennial generation appears to be rushing eagerly towards a dystopia of the kind portrayed in Dave Eggers' novel *The Circle*.

(Lilian Edwards, 2009b: 47–8, quoted evidence from both Britain and America which seemed to show that the problem is partly that young people simply do not realize the extent to which their use of social media is exposing them before the public, and that when they do grasp this they are as unhappy about it as their elders would be. As she said, this seems surprising when one considers how much savvier about technology "digital natives" are said to be than their parents' generation.)

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 individual customers than they might imagine.) This will surely become better understood with time; in 2003 David Manasian suggested 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 recognized 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 own 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.

England has long had laws against defamation (libel and slander), of course, which aim to protect individuals from words that would lower their reputation in other people's eyes. We shall look at defamation in sec. 7.5. But the concept of personal privacy, which laws in various Continental countries protect, is not the same thing. In 2008 the film actor Olivier Martinez was awarded damages by a French court for breach of his privacy by a news website, Fuzz.fr, which had posted a link to a story on another site saying that he was in a romantic relationship with Kylie Minogue; Fuzz.fr closed down. I am not sure how many Englishmen who are single (as Martinez then was) would have considered a report of an affair with Kylie harmful to their reputation. Furthermore, an English court will not find that you have libelled someone, if you can show that what you wrote was true. In France it seemed to be the very fact that Martinez and Kylie had indeed been an item that made the Fuzz.fr story a breach of his privacy.

An important case for privacy in England 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 Court of Human Rights, 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 Court of Human Rights found that the logged details are themselves part of what the Convention guarantees privacy for. Lynette Copland was awarded damages.

(The European Court of Human Rights, which heard the *Copland* case, is quite separate from the European Court of Justice, which has been mentioned in earlier sections. The ECJ is in effect the Supreme Court of the European Union. The Court of Human Rights has nothing to do with the EU. It was set up to oversee the European Convention on Human Rights, which dates back to a time before the foundation of what became the EU. Almost all European countries are signatories to the Convention, including countries like Russia which have never been EU members.)

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. We shall see that 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.

Countries that are Convention signatories are expected to modify their laws if these prove inconsistent with the Convention, but this expectation is looser than the clear legal obligation on EU members to treat ECJ decisions as overriding their national laws. 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 was 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 Act protecting freedom of expression.

Since these two principles are stated in broad, general terms which are more or less mutually contradictory, in the past English courts might have been expected to resolve the contradiction in line with established English 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 a significant sum 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 in 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 (see e.g. Edwards 2009b: 475–6), 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.

In the following sections I shall describe the 1998 Act in some detail; at the time of writing it remains current law. However, it has now been overtaken by an EU *General Data Protection Regulation*, to come into force in 2018; and at the time of writing Parliament has begun considering a new Data Protection Bill which will match the requirements of that Regulation, and will survive Brexit. (Normally, EU "Regulations" – as opposed to Directives – have direct effect without needing to be transposed into national law, but the General Data Protection Regulation is an exception which in part must be implemented by national parliaments.) The new rules do not abolish any requirements of the 1998 Act, so far as I am aware – they only tighten the requirements further and add new ones; so time spent learning about that Act will not be wasted. In the course of describing it, I shall briefly mention some of the main respects in which its provisions are set to be strengthened soon. (For the sake of clarity I shall refer to the new law as the "2018 law".) But at the time of writing, 2018 lies in the future, so I cannot be as specific about it as about law which has been applied and tested over a period of years.

6.9 THE DATA PROTECTION ACT IN OUTLINE

Although the 1998 English 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 organization might well have wanted to do, and which many people might see as *not objectionable*.

To English lawyers, the Act was a strange piece of legislation; one lawyer used the word "unprecedented" (Aldhouse 1991 – he was referring to the 1984 Act, but this was already heavily moulded by Continental patterns of legal thought). This is partly because it took 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[38] 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 EU 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".[39] Americans tend to regard Europe as having an excessive appetite for regulation – and many in Britain have seen the EU approach as failing to appreciate

that placing excessive burdens on enterprise, however laudable the reasons, risks damaging the prosperity on which everyone depends.

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[40] 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. (Ian Lloyd, 2017: 60, 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 reported 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…[41]

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 have normally played 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."[42] Indeed, British decisions in some relevant cases 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 even if Britain were happy with a lax privacy régime, that will soon be irrelevant in view of the new EU Regulation – and, this time, Parliament may be reluctant to temper the impact of the 2018 law on business by implementing it in a mild form, because business wants Europe to continue to see Britain as an acceptable place to process European data after Brexit.

6.11 STRENGTH THROUGH VAGUENESS

In practice, laws like the Data Protection Act, which seek to control a significant aspect of life through rules which are somewhat vague, affect society – and business – not just through what they actually forbid but also by creating an atmosphere in which anything that *might*

conceivably trigger legal difficulties is avoided. Stewart Room's opinion just quoted was only that – an opinion. Administrators concerned with data protection in an organization will often require their colleagues to refrain from actions which seem even less likely than those of a hypothetical British Bodil Lindqvist to fall foul of the law.

Before I retired from teaching in 2009, our university administrators were preventing us from learning how well individual students were doing on other teachers' courses, and forbidding us to send e-mails to students taking our course in ways that would reveal the names of various students on the course to one another. We protested that we needed to do these things in order to teach well. (If a student, say, proposes an unusually ambitious final-year project, a good teacher needs to take a view on whether the student is likely to be up to it or should be advised to choose something easier. Encouraging the students on a course to meld together as a community helps to create an enthusiastic, learning-promoting ambience.) But the answer was that the remote risk of Data Protection issues was the only thing that mattered.

Jane Kelly was a volunteer hospital visitor, offering friendship to patients with no family to visit them. In 2017 she described how "Hospitals are putting NHS data-protection policies above simple humanity":

> A neighbour broke her leg. When I arrived at the hospital, it proved impossible to see her. "If you don't know which ward she's on we are not allowed to tell you," said a woman on the front desk.… A man of 95 was being discharged. There was no one at home waiting for him, he said, and he'd like a visitor. He told me he belonged to a local church and so, at his request, I contacted them and asked someone from their pastoral team to visit him. That was strictly against the rules as well, I was told. I gave up the hospital job.[43]

Administrators in organizations like hospitals and universities, who have the ultimate say-so on issues like this, are often more interested in "covering their backs" than in furthering the aims of the institutions. They know that if patients suffer, or students fail to acquire a love of learning, it will be the medical staff or the teachers who are blamed, not the administrators who may have been interfering with how they do their jobs. And thus laws which are wide-reaching but somewhat vague can have social implications which go far beyond what the legislators perhaps intended.

6.12 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.

6.12.1 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 offers 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 (and in the 2018 law that is explicit). The new Regulation adds more categories;

it applies to an EU resident's personal data, "whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an e-mail address, bank details, posts on social networking websites, medical information, or a computer's IP address".[44]

This sounds, then, as though any file whatever which briefly mentions an identifiable person, in whatever context, will be hit. For many years the leading British case was *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 represented 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 required. (This is a main reason why I noted above that the gap between British and Continental data protection régimes has been widening.) Indeed, in 2004 the European Commission announced an investigation of the UK data protection régime, to see whether it adequately implements the Directive, though nothing seemed to come of this.

In a more recent case, *Edem v. Information Commissioner & Financial Services Authority* (2014), the Court of Appeal found a way of partly revoking its *Durant* decision without explicitly contradicting itself. Simplifying a complex judgement, a file which mentions a person by name is now covered by the Act, unless the file fails to identify an individual uniquely because the name is common and other information does not fix the reference.

6.12.2 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. 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.

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 (2017: 82) 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.

The consent requirement will be considerably tightened up under the 2018 law. "Opting in" has sometimes been managed in a fairly minimalist fashion, but the new law will strengthen the requirement, aiming to avoid data subjects being lulled into agreeing absent-mindedly. Data subjects will be able to withdraw consent at any time, in which case everything relating to them must be deleted.

6.12.3 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.[45] 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!)

6.12.4 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, for Data Protection Act purposes the act of anonymizing data *itself* counts as processing the data. So it may only be done if the Act allows it (e.g. because the data subject gave consent for their data being used for research purposes) – though, once the material has been adequately anonymized, the Act no longer applies and anyone can do anything they like with it.

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.

6.12.5 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, the 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, initially, the UK Information Commissioner (unlike counterparts in other EU countries) lacked any power of audit. Comparable supervisory bodies, such as the Health and Safety Executive or the Financial Conduct Authority (previously 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. It is questionable whether the EU Directive is adequately implemented if the Commissioner lacks the power of audit; in 2009 he was given the power to audit public bodies, though not private-sector organizations. (With the financial crisis which began in 2007 at its height, it was presumably felt desirable to avoid throwing extra burdens on business, though the minister denied that this was the main consideration.)

Under the 2018 law, any organization which gathers or processes personal data must be able to demonstrate that it has systems in place to ensure that the data are well protected in specified ways, including replacing individuals' real names by pseudonyms at an early stage. For anyone to re-identify individuals from pseudonymized or anonymized data becomes a crime.

6.12.6 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 very 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 past credit problems to home 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 Data Protection Tribunal upheld the Registrar's veto.

The judgement made the "fairness" aspect particularly explicit. The tribunal chairman 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 is imposing a relatively strong sense.

Our second example of "unfairness" for the purposes of the Data Protection Act was never tested in a formal hearing, 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.

6.12.7 RIGHT TO SEE AND CORRECT DATA, AND OBJECT TO PROCESSING

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, under the current law 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. Another is processing for purposes of making automated decisions, which 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.

One feature introduced by the 2018 law which is quite novel is that decisions like this which are made purely algorithmically will be subject to legal challenge: an individual denied

credit by a credit-scoring program, for instance, can demand an explanation of how the decision was reached, and can try to get it reversed by court action. (How this might work in practice seems very unclear, considering that much software used for tasks like credit scoring is of the neural-network type, so that even the software engineers responsible for it can hardly identify an explicit set of rules on which decisions are based.)

6.12.8 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 kinds of thing that are forbidden can be illustrated by two cases where the Information Commissioner found organizations in breach of the Act in 2007: the telecomms firm Orange, because staff were sharing usernames and passwords to get their work done conveniently (creating the possibility of staff members seeing personal data which they were not entitled to see), and Marks & Spencer, for allowing 26,000 employees' details to be held on a laptop without encryption.

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 observers, though, the most noteworthy point about this proviso is that the British Government, which was responsible for introducing the Data Protection Act, became 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, just over the year to April 2008 government officials were reported as losing details relating to more than 300,000 individuals each 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".

In 2004, the Nationwide Building Society was fined almost a million pounds after a laptop containing confidential customer information was stolen from an employee's house. Yet, 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 2008, forcing the site to be suspended, the Prime Minister asked the country to accept that losses of sensitive data were inevitable.[46] If such errors are truly inevitable, how can anyone be punished for committing them?

(The British government's problems with the principles of data protection are not limited to the safe storage issue. In 2009 the Joseph Rowntree Reform Trust commissioned a report on public sector databases, which concluded that one in four of them were illegal under data protection or human rights law, and another six out of ten were problematic and possibly illegal. Ross Anderson of Cambridge University, one of the experts responsible for the report, commented that "Britain's database state has become a financial, ethical and administrative disaster which is penalizing some of the most vulnerable members of our society."[47])

6.12.9 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. Even after we regain our independence, we shall have to maintain data protection rules similar to those of the EU if we want to keep that type of business.

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 only a handful of non-EU countries are judged to have laws guaranteeing adequate data protection, and while some of these, such as Switzerland, may be significant locations for data processing, others, such as the Faeroes, are perhaps not. The countries judged to provide inadequate protection notably include the USA.

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

"Safe Harbour" had 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. The system achieved nothing unless US firms chose to sign up, and for years the numbers doing so were not large. And on the other hand there was doubt in Europe about whether the Safe Harbour safeguards were strong enough. These doubts led in 2013–15 to a case, *Max Schrems v. Data Protection Commissioner*, which began in Ireland and was referred to the European Court of Justice. (It concerned transfers of data about EU citizens to US servers by Facebook, which had signed up to Safe Harbour.) The ECJ's decision effectively struck down the Safe Harbour arrangement as not compatible with the Data Protection Directive.

In 2016 a replacement system, Privacy Shield, was negotiated between EU and USA. But various legal challenges to it were soon launched, and at the time of writing it is not at all sure whether Privacy Shield will be more successful than Safe Harbour.

6.13 THE RIGHT TO BE FORGOTTEN

One important aspect of data protection which was not spelled out explicitly in the EU Directive or the 1998 Act, but which the Directive has since been interpreted as guaranteeing, is the so-called "right to be forgotten" on the Web.

This originally arose through a 2014 case at the European Court of Justice, *Google Spain v. Spanish Data Protection Agency & Mario Costeja*. A Spanish newspaper had in 1998 published information about social security debtors, including Costeja, and the newspaper was later uploaded to the Web, so that people Googling for Costeja's name were shown this adverse information about him which was sixteen years old and, Costeja argued, had lost its relevance. There was no dispute that the facts had been reported accurately. But, cutting through a complex judgement, the Court decided that the EU Data Protection Directive controlled the right to process "inadequate, irrelevant, or excessive" data, accurate or not, and that unless an individual is prominent in public life, his right to be forgotten overrides "not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information [via a search on the individual's name]". (Because the Directive did not explicitly spell out a "right to be forgotten", the 2014 decision was actually made in terms of the clause in the European Charter of Fundamental Rights about respect for private and family life. But the Court was influenced by knowing that the new EU General Data Protection Regulation was on the way, and was going to make the right to be forgotten explicit. For a detailed discussion of this case see Rowland et al. 2017: 361–5.)

The consequence of this decision was that Google instituted a system in Europe whereby people can apply to have webpages about them deleted from search results, though the publishers of the respective pages are notified and can object. This facility is heavily used; on its first day of operation more than twelve thousand deletion requests were received. (Readers will have seen the note that Google now displays with a page of search results, "Some results may have been removed under data protection law in Europe.") At present the decision is implemented only within the EU, but as I write we are waiting for a decision by the European Court of Justice on whether the EU will require Google to delete this material globally (on pain of heavy fines if it fails to do so).

Under the new law coming in 2018, the right to be forgotten will be strengthened in other ways. For instance, anyone will be able to demand that social networks delete everything he or she posted before turning 18 years old.

Like the Yahoo!/Nazi case discussed in sec. 2.1, the right to be forgotten underlines the different attitudes on either side of the Atlantic towards how the balance should be drawn between freedom of expression and arguments for limiting that freedom. Americans give greater weight to freedom of expression, and it seems quite unlikely that Americans would ever introduce a right to be forgotten. Some influential Americans have been scathing about attempts to protect privacy. Scott McNealy, chief executive of Sun Microsystems, commented in 1999 "You have zero privacy anyway…Get over it."[48] On the other hand, for

some Continental Europeans freedom of expression is not a high priority. In 2004, in the case *von Hannover v. Germany*, the European Court of Human Rights found that German publishers of coffee-table magazines had violated the European Convention on Human Rights when they printed a set of (harmless, non-embarrassing) paparazzo photographs of Princess Caroline of Monaco in her daily life, riding a horse, playing tennis, and so forth. A judge serving on the court, Bostjan Zupančič of Slovenia, wrote "I believe that the courts have to some extent and under American influence made a fetish of the freedom of the press. It is time that the pendulum swung back to a different kind of balance between what is private…and what is public".

It is understandable if people feel that the Web has created a new need for controls. Before the internet it was simply not practical to dredge up everything that might have been written somewhere about some private person years earlier with no current relevance, so this kind of threat to privacy did not exist. When a new technology creates a possibility of doing something that during most of human history was impossible, it is perhaps difficult to see how doing that thing can possibly be a basic human right.

On the other hand, the array of privacy laws on this side of the Atlantic are becoming stronger to an extent that some find worrying. Much modern history writing ultimately

depends for its basis of hard evidence on newspaper reports, which used to be archived as roomsful of yellowing paper copies. Recently these have largely been replaced by electronic archives, which it is physically possible to alter. Ian Lloyd (2017: 154) believes it is "certain" that already under the 1998 Act a data subject would be entitled to require errors in such archives to be corrected – and not just that, but any editorial opinions based on the incorrect facts to be rewritten. True, changing prose to make it more accurate is different from suppressing facts, or representing them as other than they actually were. But once the principle of changing the historical record is accepted, it is not clear how easy it will be to maintain that crucial distinction. Understandably, Lloyd sees this implication of the 1998 Act as Orwellian.

(In George Orwell's novel *1984*, the protagonist Winston Smith was employed by the dictatorial government's Ministry of Truth to change records of the past so as to bring them into line with how the past "ought" to have been in order to serve the dictatorship's changing propaganda goals. Orwell intended this as a dystopian vision, and readers have seen it as such – certainly not as something we ought to be using technology to realize. On the other hand, if Lloyd is correct in predicting that this is how the law would be interpreted, it is perhaps surprising that – so far as I know – there has not yet been a relevant case.)

6.14 IS THE LAW ALREADY OUTDATED?

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. Ian Lloyd comments (2017: 74):

> 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 et al. (2017: 384) 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:

> How should the original data protection legislation designed to deal with a much more static situation be applied to the dynamic environment of the internet? How could, for example, the restriction on transborder data flows be applied? Can there be any guarantees of appropriate safeguards? How can the originator of the material know in

> which jurisdiction the resultant data might be used? If the information is made available by an individual on, for example, a social networking site, does that mean that the processing attracts an exemption on the grounds of personal and domestic use? In short, can the original 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 (and it is not clear that the 2018 reform of data protection legislation will do much to answer them – Lloyd, 2017: 55, describes it as "reluctant…to accept that the computer world has moved on from the 1970s").

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. We know that an economy tends to be more prosperous if the agents interacting within it tend to trust one another, and it has long been recognized that information technology, which replaces personal relationships by impersonal online interactions, is dissolving trust to a worrying extent. (Cf. Sampson 2008: 71–2.) 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. We saw in sec. 3.5 that the IT industry is currently moving 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. Some industry leaders have called for "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.

6.15 IS DATA PROTECTION LAW WORKABLE?

I described the 1998 Act as a tough law, but the régime coming in 2018 is certainly tougher in many ways – it might be called draconian. Perhaps the most striking thing about it is the level of penalties it defines for breaches, which are far higher than under the current legislation: up to four per cent of a firm's annual worldwide turnover, or twenty million euros, whichever is greater. These are admittedly maxima, but they are huge sums. To lose four per cent of turnover would often be quite enough to turn a profitable company into a loss-maker, and the €20 million alternative would surely wipe many small firms out.

Since the new régime has not yet begun, it is too soon to know how it will work out in practice. It is very possible to doubt that organizations will be capable of, for instance, locating and deleting all the items of data it holds within any set of files relating to an individual who has withdrawn consent for data to be held, or with respect to whom the purpose of holding the data has expired, or who requires deletion of his postings made before the age of eighteen. A YouGov survey reported in June 2017 that, with less than a year to go, fewer than three in ten UK firms had begun preparing to meet the detailed requirements of the Regulation for how companies must organize responsibility for handling personal data. (And quite a number of firms which had put plans in hand had later abandoned the effort in view of Brexit, although this was evidently a miscalculation.) Indeed, a few months earlier

the Information Commissioner's office had reported that "nearly half of all companies are struggling to comply with existing data protection laws, let alone the GDPR reforms". Two-thirds of firms surveyed by YouGov did not believe they could rely on being able to report a data breach within the mandatory three-day deadline.

Interesting times ahead!

7 WEB LAW

7.1 CHANGING SOCIAL ATTITUDES TO INTERNET FIRMS

7.1.1 CAN LAW CONTROL THE INTERNET?

It is interesting to reflect that, when the World Wide Web was young, its independence of geographical boundaries led many people to imagine that it was destined to become a domain where states and their laws would simply not hold sway: in the 1990s a widely-held view was that "government *could not* regulate cyberspace, that cyberspace was essentially, and unavoidably, free" (Lessig 1999: 4). David Johnson and David Post (1996) saw the rise of the internet as "throw[ing] the law into disarray by creating entirely new phenomena…that cannot be governed, satisfactorily, by any current territorially based sovereign". The American poet, musician, and political activist John Perry Barlow published a famous "Declaration of the Independence of Cyberspace" in 1996, beginning:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[49]

Stirring stuff, but naive. Only three years later, the academic lawyer Lawrence Lessig was arguing, correctly, that in reality the extent to which visitors to "cyberspace" could escape the control of national laws depended entirely on the technical details of how the internet was implemented; and Lessig saw it as inevitable that, unless societies began to make political decisions about internet architecture which they showed little sign of doing, cyberspace was bound to evolve soon into a domain of much *less* personal liberty than his home country, the USA. "Left to itself, cyberspace will become a perfect tool of control" (Lessig 1999: 6).

Two decades on, Lessig seems almost as naive as Barlow. Lessig was right, of course, to say that internet technology could in principle be modified so as to give states close control over individuals' activities when using it, but in practice most states have had a very limited appetite for doing so. (China is one exception: see Murray 2016: 82–3.) One of the developments Lessig saw coming was systems to ensure that any data moving over the internet could reliably and easily be traced back to their individual originator. Lessig saw this as a fearsome prospect. To me it seems a highly desirable change, because it would end overnight the vicious trolling that is driving some vulnerable youngsters to suicide and

severely damaging the quality of life of many others. In the physical world, it has long been generally understood that writing anonymous letters is a disgusting practice, yet in internet forums and the like contributors are actually encouraged to use pseudonyms, which can sometimes be penetrated when authorities need to do so, but often cannot. I agree with Lessig that free speech is a principle well worth defending, but there is little to be said in favour of anonymous free speech. Yet our governments have been wringing their hands and asking schools to try to teach children resilience to trolling, rather than addressing the root of the problem by modifying internet architecture.

Until very recently the British and other governments have been remarkably willing to go along with John Perry Barlow's attitude that internet companies are somehow above the law. People commonly put the astonishing, world-beating commercial success of Silicon Valley down to a lucky confluence in California of accumulations of capital and a highly-educated workforce; but Anupam Chandler (2014) argues that a more important factor has been a kind of huge implicit subsidy by the US government, in that it has exempted online businesses from many different legal burdens which apply to business offline. In Britain, consider for instance the scandal that developed from 2012 onwards about American companies which were paying little or no UK tax on large profits generated in Britain. (The firms mainly complained about included Google and Amazon, but also Starbucks, which is not an

internet company.) The ways in which these firms were organizing their businesses to avoid tax were of course perfectly legal under the existing tax rules – but, usually, when firms or individuals discover and exploit massive loopholes in tax law, the law is changed to block the loopholes. What happened in response to a growing chorus of popular resentment in this case was rather different. For instance, in January 2016 Google decided for the sake of its reputation to offer voluntarily to pay "back taxes" of £130 million to cover the previous ten years. Some commentators saw this as derisory: the tax avoidance expert Prem Sikka reckoned it equated to a tax rate of less than three per cent for a decade during which the normal rate of corporation tax averaged about 25 per cent. Yet the then Chancellor, George Osborne, greeted it as a triumph: "This is a major success of our tax policy…a really positive step – I think it's a big step forward and a victory for the government."[50]

To anyone familiar with the relations between the authorities and ordinary commercial or individual taxpayers, this deferential attitude sounded extraordinary. If I make a modest profit from writing this book, nobody will greet my offer to pay tax on it as a welcome act of generosity. I shall receive a demand to pay at the full applicable rate, and to be prompt about it. That is the way taxation normally works, and must work. But internet firms in particular were seen as somehow different, in connexion not just with taxation but with all kinds of social obligations. (This was about the time when Google formally abandoned its previous company motto, "Don't be evil".)

7.1.2 GROWING DISENCHANTMENT

Very recently, attitudes on the part of societies and governments have begun to change. When the internet was new, it was seen as a mysterious goose laying golden eggs; governments were frightened to interfere with it, in case interference somehow interrupted the egg supply. (Indeed, to question the wisdom of letting information technology take over any and every sphere of human activity was seen as saying no to the future, and the less detailed knowledge individuals had of how the technology worked, the more convinced they seemed to be that it could only be beneficial.) But by now the mystery is largely dissipated and the internet has come to be seen as just one everyday aspect of social life, open to criticism like any other.[51]

One early sign of legal hostility towards the internet came in the summer of 2011, when serious, destructive riots and looting broke out in the London suburb of Tottenham and rapidly spread to other parts of London and many other British cities. To a large extent the rioting was organized via messages on Facebook and other social media platforms, so that some Parliamentarians urged government to close the social media networks down

temporarily. Andrew Murray points out (2016: 163) that when those involved were prosecuted, individuals who posted messages proposing local riots that never took place seem to have been given prison sentences several times longer than individuals who actually participated in the orgies of theft and destruction (but did not post social-media messages).

It is hard to know whether or not Murray is correct to analyse this as indicating a general hostility towards technology on the part of the legal system, because happily the 2011 episode has so far been a one-off. More recently, though, changing attitudes towards the internet, internationally and on the part of society more widely, have been unmistakable.[52]

One factor was growing concern about "fake news" websites, which came to the fore in connexion with Donald Trump's presidential election campaign in 2016. In the 2017 MacTaggart Lecture, Jon Snow argued in connexion with fake news that Mark Zuckerberg and Facebook pose a "vast threat to democracy".[53] Providers of internet service wanted to be seen as comparable to the postal service, with no responsibility for the contents of the sites to which they provide access, but sections of the public began to feel that this was not good enough. Then in 2017 Google found itself losing advertising revenue: major advertisers, including leading high-street brands such as Marks & Spencer, McDonald's, and L'Oréal, major banks, and many others, were withdrawing their custom because the Google subsidiary YouTube was displaying their banner ads alongside Islamist and other hate videos.

Google seemed to feel that it could not be expected to find the resources needed for thorough monitoring of video which was being uploaded to YouTube at the rate of 400 hours per minute.[54] But people would laugh if an ink-on-paper publisher pleaded that it had not got enough editorial staff to keep itself legal. No organization has a God-given right to set up a system which it cannot control.

In Britain a turning-point came in March 2017 when the jihadi Adrian Ajao, alias Khalid Masood, murdered four people and injured fifty on Westminster Bridge and in the grounds of Parliament, and the instant-messaging service WhatsApp (a Facebook subsidiary) declined to show the police the content of messages he had sent immediately beforehand, explaining that their system of "end-to-end" encryption meant that even WhatsApp staff had no way of reading the unencrypted text.[55]

WhatsApp had boasted of its encryption as a system which ensured users' privacy, but Government and many individuals felt that in such cases the need of the security services to investigate crime ought to override privacy rights. WhatsApp claimed to be an internet platform with no control over the messages it carried, and it had some existing law on its side. In 2012–13 a student and Conservative local-election candidate, Payam Tamiz, had sued

Google for defaming him by carrying a blog which labelled him, without any justification, as a drug dealer and thief. Google disclaimed responsibility for the contents of users' blogs, describing itself as a "neutral service provider". Tamiz argued that Google was functioning as a publisher, making it liable for distributing defamatory content, but the judge sided with Google. Someone who owns a wall which gets daubed with offensive graffiti should not be treated as publisher of those graffiti, the judge ruled, and likewise Google "should not be regarded as a publisher, or even as one who authorized publication".[56] (We shall look at the specific issue of internet defamation in more detail in sec. 7.5 below.)

After the 2017 Ajao atrocity, though, the Home Secretary, Amber Rudd, said that the Government did consider firms like WhatsApp to be "publishing companies", like broadcasters and newspapers, which certainly do have elements of legal liability for what they publish; end-to-end encryption was "completely unacceptable". She presumably envisaged bringing in new law to override the precedent set by *Tamiz v. Google*. And then later that year she stressed that internet companies "need to go further and faster to remove terrorist content from their websites", after a home-made bomb was exploded on the London Underground and it emerged that Amazon was listing various things used to make bombs under a convenient "frequently bought together" tab.[57]

Major internet companies have just begun to accept other kinds of social responsibility. For years the music and film industries had complained that search engines were encouraging users to damage their revenues by leading users to sites offering pirated songs and films. In 2017 the British government finally persuaded Google and Microsoft to install systems to eliminate pirate sites from the first page of search results.[58]

The fact that internet users commonly live in countries other than those hosting the sites they are visiting obviously makes legal control harder than when everything is contained within a single jurisdiction. The UK legal system would be powerless to close WhatsApp down, for instance. But it could require British internet service providers to block access to it. That might sound like a "nuclear option", and it is the kind of thing that people and governments in the past saw as out of the question: hence the appearance that internet companies were above the law. But at the time when I am writing, we seem to have reached a turning of the tide of public opinion. In November 2017 the very sober, well-informed *Economist* magazine ran a cover story arguing that "Once considered a boon to democracy, social media have started to look like its nemesis". Consequently tough action of various kinds against internet companies is becoming less unthinkable.

Law tends to reflect changing social attitudes, admittedly often with a time-lag. Very likely, in five or ten years' time there will be a great deal more to say about Web law than there is today.

7.1.3 THE "AMAZON PARADOX"

I should say that John Perry Barlow's idea that national laws simply cannot survive within cyberspace does not, even today, seem to some commentators as dead as it seems to me. Chris Reed (2012) argues that the global nature of the Web is beginning to force those who make laws to think in terms of what rules internet users are prepared to accept as applying to them, rather than what rules a state decides to impose on them. Offline, the communities we belong to are largely determined by geography, but online we choose which communities we join, and we accept laws if we see them as applying to our communities. For instance, Reed points to what he calls "the Amazon Paradox". Amazon UK, the firm which owns the amazon.co.uk site, is obviously oriented to selling into the United Kingdom, but physically it is based in Luxemburg; yet the amazon.co.uk site

> complies with UK advertising regulation and other legal requirements which would only be applicable to it if it were a UK corporation. It is clear that Amazon UK invests substantial time and effort in understanding UK law and ensuring that its amazon.co.uk

> website complies with it…some rules of UK law have authority for Amazon UK simply because they are part of UK law. The fact that the UK authorities have no power to enforce those laws against Amazon is simply not a relevant consideration.

To my mind this is naive. One problem with Reed's view is that it seems to ignore the difference between legal behaviour, and "good behaviour". We all, individuals and commercial firms, refrain from doing many things which would not actually be illegal, because we have been brought up to behave ourselves. We could make a habit of speaking rudely to everyone we meet, and the law would have nothing to say about it; but in practice most of us try to be at least minimally polite, whether because we fear losing our friends or because we see gratuitous rudeness as morally wrong (or both). Amazon UK wants to be seen in its target market as a decent company which respectable people will be happy to deal with, rather than one which takes advantage of any legal loophole it can squeeze through, so it constrains its behaviour in ways that go beyond the demands of Luxemburg law. Offline companies constrain their behaviour for similar reasons. Some people behave better than others, and perhaps Amazon is an unusually "well-behaved" company in this respect, but (for individuals and for businesses) avoiding illegal behaviour is only a bare minimum requirement: there is nothing "paradoxical" about rising above the minimum.

Reed's idea of cyberspace as an arena in which communities voluntarily decide which laws they are prepared to accept grossly understates the role of enforcement. Reed says, rightly, that if some foreign country, let's call it Ruritania, were to bring in a law which purported to impose low speed limits on roads everywhere in the world, and were to issue summonses to drivers who exceeded the Ruritanian limits on British roads, British drivers would just scoff at the summonses. And he says that laws affecting internet behaviour are often like this: nothing in the laws as worded explicitly limits their application to individuals (or commercial agents) residing in the particular country whose laws they are, but people and firms elsewhere just ignore those laws. However, that does not mean that laws can only work if a community voluntarily accepts them. Perhaps the Ruritanian traffic law failed to spell out in so many words that it applied only within Ruritania, but it did not need to, because the rest of us know very well that Ruritania has no power to punish us for exceeding its limits in our own country, and hence that the Ruritanian law is irrelevant here.

On the other hand, in the business domain the USA quite often makes laws applying to foreigners in their own countries. One example is FATCA, the *Foreign Account Tax Compliance Act 2010*. FATCA requires foreign bankers to search their files to identify any clients with a US connexion, and to report on such individuals' finances to the US Treasury. British and other non-American bankers comply, because the world's financial relationships are so interdependent, and the USA accounts for such a large portion of the network, that the

American authorities easily can – and will – take actions that seriously damage the business of a non-compliant bank, even though it owes the United States no fealty.

Ruritania cannot enforce its traffic laws in Britain, the USA can enforce its financial laws. It is enforceability which matters – not voluntary acceptance. Where laws are enforceable, they often function successfully to influence the behaviour of communities which strongly disagree with them. Very many British car drivers and passengers were vociferously hostile to the seat-belt law which came in in 1983, but people who failed to wear their seat-belts were often caught and fined, and nowadays people do usually buckle up.

It is true that there have been some cases where a country (or, in the case quoted by Chris Reed, the EU) has brought in a law which explicitly purports to control behaviour by internet users outside its own territory. Reed's example was an attempt in 2002 to require non-EU suppliers of online services to charge value added tax to EU consumers at the consumers' respective national VAT rates, and to pay over the tax received for distribution among the EU member states. This would have been a quite onerous requirement for non-EU suppliers to obey, and most of them ignored it. Reed is correct to say that they did not see it as applicable to them. But the reason was that the EU had no way of enforcing it against them – and they knew that.

So I continue to believe that the international character of internet relationships, though it is novel, is not a central issue for our present purposes. But there are many ways in which the Web does create special legal issues. We shall look at four topics:

- contract formation in internet trading
- the right to make links
- trademarks and domain names
- Web 2.0, defamation, and "hate speech"

7.2 THE INTERNET AND CONTRACT

7.2.1 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 Continental, Civil-law 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, though for Civil-law countries this turns out not to have been very successful (see Reed 2012: 135–7). 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 Common 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 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 (though see Bainbridge 2007: 269–71). 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.

7.2.2 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 retail 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 can 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 1993, when the vacuum cleaner manufacturer Hoover ran a sales promotion which offered free flights to America with purchases over £100, budgeting £2 million as the cost of the promotion. Hoover did not anticipate how popular this offer would be. Many people bought two vacuum cleaners just to get access to the flights, and 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; it ended up paying out at least £50 million, including compensation to disappointed applicants, and 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 1993, 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 etailing, 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 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.[59] (Jane Winn and Benjamin Wright, 2005, reported that the terms and conditions on the United Airlines website still did not provide protection against the type of error that occurred in its case, several months *after* the mistake was discovered!)

7.2.3 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 (2005: 274) pointed out that in 1971 Lord Denning would not have envisaged cases where the machine processes customers' orders in complex ways – they saw 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.

Some enthusiasts envisage automation invading the market process at a deeper level, so that contracts between firms might be not merely fulfilled and enforced, but perhaps even negotiated, without human intervention – a world of so-called *smart contracts*. The human population might be able to sit back and watch firms contracting new relationships with one another and trade flourishing and expanding, all as an automatic process. A platform for smart contracts, Ethereum, was launched in 2015 using blockchain technology.[60] But (whether one sees it as attractive or the reverse) this concept seems at present too futuristic to examine in detail.

7.2.4 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 go into further.

7.2.5 FREE SERVICES

Another issue which raises an interesting question of contract law is the prevalence nowadays of free services over the internet, such as the benefits associated with use of social media. Some economists have commented that countries' growth rates may well currently be systematically underestimated, because so many services whose nearest equivalent, a few years ago, would have been paid for are now offered gratis online (and consequently tend to be invisible in economic statistics).

If a service is truly free, of course, it cannot be governed by contract law. We have seen that a contract must involve a swap: each party must agree to give something in exchange for what it gets. But the "consideration" does not have to be money: it can be anything of value. Alan Cunningham and Chris Reed (2013: 347) look at this in connexion with the common-law obligation on anyone who contracts to supply a service to carry the service out with "reasonable care and skill". They point out that many "free" digital services do involve users parting at least with information about themselves which has value to the service provider, by increasing what they can charge to advertisers. (Why would the services be provided without charge, if the service providers were getting nothing in return?) In view of this, Cunningham and Reed argue that the services are contractual, so that their users do have a legal right to exercise of care and skill in delivery of the service.

One can easily imagine circumstances in which the question whether or not this legal right existed would matter a great deal. And it is not clear that suppliers of "free" services are always aware of the possibility that they might be liable in this way. However, at present it is a possibility only – so far as I know, no case has yet tested the question in a court.

7.3 THE RIGHT TO LINK

One area that was a matter of legal controversy when the World Wide Web was young can be passed over briefly here, because it has faded away as an issue. When the Web and HTML were created, they were designed in such a way that to link from Site A to Site B requires action only by the Site A webmaster – Site B responds to any and every request to serve up its pages. In its early days the Web was an affair mainly for academics, who want nothing better than publicity for their writings: the more links into their webpages the better. But the structure of cyberspace is defined by links between webpages, and once the Web was commercialized in the 1990s, firms wanted to reside in salubrious "cyber-neighbourhoods". An upmarket boutique would prefer not to be next-door in the physical world to a betting shop or a tattoo parlour, and similarly firms began objecting to incoming links from sites

they did not want to be associated with. The problem was not just about "brand image": many commercial websites were expecting visitors to "enter through the front door", landing first on their home page, and they were liable to lose advertising revenue if people arrived via "deep links" into pages far from the home page, bypassing advertising material.

Initially, firms often tried to control incoming links. At one time, for example, National Public Radio in the USA was asking people to submit lengthy request forms for permission to link to its site. 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 was not clear to American legal commentators whether it could actually force anyone to remove a link to its site.

One case in Germany about "deep linking" (*Verlagsgruppe Handelsblatt v. Paperboy*, 2003) was lost by the plaintiff, with the judge pointing out that an organization which really wants others to link only to its home page can perfectly well ensure that by technical means. So by now I believe the legal "right to link" is no longer open to question.

7.4 TRADEMARKS AND DOMAIN NAMES

7.4.1 ICANN AND THE MULTI-STAKEHOLDER MODEL

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 put 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][61]

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. (On the "DNS Wars", see e.g. Litman 2000.)

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 sophisticated, formal processes for arbitrating disputes over ownership of lower-level domains, which those who buy domain names have to sign up to. 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.

Before ICANN adopted its "Uniform Domain Name Dispute Resolution Policy" in 1999, disputes over domain names had been settled in ordinary national law courts. If a state-backed court decided to override the ICANN system, Nominet or its counterpart in some other country would have little choice but to obey. However, in practice state courts have acknowledged the authority of ICANN and do not interfere. (In a 2012 case, *Toth v. Emirates*, the plaintiff argued that Nominet had misapplied the ICANN policy and the court should require a name which had been transferred away from him to be returned, and initially he won; but on appeal to a higher court the final decision was that English law had no basis for second-guessing the Nominet decision.)

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. Despite some US resistance to internationalizing internet governance (Taubman 2009: 16–17), ICANN was established in 1998, largely in line with a memorandum published in the name of the "Internet Community"; the US government transferred responsibility for domain name allocation to ICANN. Until 2016 ICANN was still operating under a light-touch contract with the US government, but authority over it was formally transferred in that year to a so-called "multi-stakeholder community" in which national governments have no special rights.[62] On the whole the world seems to see this multi-stakeholder model of governance as a success, though there have been dissenting voices – both from some national governments who felt that more control was needed,[63] and from individuals who fear that "multistakeholder consultation" sometimes in practice boils down to one key ICANN member "chatt[ing] with a few of her mates and they decide[…] amongst themselves".[64]

The result is that to anyone steeped in traditional legal thinking, the internet domain name system can appear a mysterious and ungraspable phenomenon. Ian Lloyd (2017: 443) 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 important 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. By 2006, Martin Veitch was commenting that premium domain names which would once have been deemed highly valuable were failing to sell for high prices, and that "firms with strong URLs frequently lose out [in commercial competition] to sites with less obvious names".[65] So this is not an area of computing law which I would expect to develop to any great extent in future. (Though large sums do sometimes continue to be paid for attractive domain names. In 2015 the Chinese security software maker Qihoo bought the domain 360.com from Vodafone for $17 million.)

7.4.2 INTERFLORA V. MARKS & SPENCER

Another way in which the Web is creating new legal problems for trademarks, though, is a very live issue and likely to remain so. This relates to Google's AdWords facility.

As many readers will know, AdWords is a system by which traders can bid on particular words, so that the winner's website is displayed as a "sponsored advertisement" when that word is input to the Google search box. (Currently, sponsored adverts appear at the top

of the first page returned by Google, distinguished from the results retrieved by Google's ordinary relevance algorithm by a television-screen symbol containing the word "Ad".) Interflora is an organization which links a nationwide network of florists, so that someone wanting to send flowers to a distant friend can use it to arrange delivery from a shop local to the friend. Because Interflora is long-established and very well known, customers wanting to send flowers often type its name into the search box.

But Interflora is not the only organization offering a similar service. Marks & Spencer also deliver flowers via their own national retail chain. The legal problem arose after M&S successfully bid for "interflora" as an AdWord, so that people searching on that word were shown an M&S website (which did not, itself, contain the name "Interflora"). In 2009 Interflora began a case for trademark infringement which has become an immensely complex legal saga, including hearings at the High Court (twice), the Court of Appeal, and the European Court of Justice. It is not yet finally resolved.

One might have supposed that using a competitor's trademark in this way is clearly not cricket; but legally there would be no objection, so long as customers seeing a sponsored advert are not confused about the identity of the advertiser. Apparently it is routine for advertisers to bid for other firms' trademarks in this way. The problem in this case is that, because Interflora is a network of independent florists, someone searching for "Interflora" and seeing an M&S site could easily imagine that M&S is a member of the Interflora network – which it is not.

Since the case continues, one cannot say what the overall legal situation will turn out to be. But already the various hearings have established a number of principles which sometimes seem quite surprising.[66] For instance, AdWords includes a "negative matching" facility. Someone who markets ski-ing holidays and bids for the word "ski" will not want his site to be shown in response to a search on "water ski", so he can specify that searches including "water" should be ignored. To market their service, M&S had also bid on "generic flower-related terms" (words like "roses" or "flowers", presumably), and because Google's algorithm uses data on relationships between different words, bidding e.g. for "roses" increased the probability that a customer searching on "interflora" would be shown an M&S site. It has emerged from the hearings to date that bidding for generic words like "roses", while failing to specify "interflora" as a negative term, *in itself* counts legally speaking as a use of the Interflora trademark, though we do not yet know whether it is a legitimate use.

Sponsored advertising is a growth area, and the underlying algorithms are becoming increasingly subtle. So in this area we are very likely to see further legal development, even after the *Interflora* case is done and dusted.

7.5 WEB 2.0, DEFAMATION, AND "HATE SPEECH"

7.5.1 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 (and indeed slander cases rarely come to court nowadays). Emails, tweets, 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, here it has been 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 used in new ways now. We have heard a great deal 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 – have ceased to be outlets for one-way communication exclusively, and have often turned 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. And this has been reinforced by the rise of social media such as Twitter and Facebook.

There are several business reasons why the "virtual communities" fostered by interactive websites and social media 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 all 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.

7.5.2 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 – an issue that we looked at briefly in sec. 7.1.2. 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. Lilian Edwards (2009: 53) noted that, both in Britain and in America, there used to be "a general rule of thumb that an ISP or host should exercise as little editorial control as possible over content provided by third parties, lest they be…held legally responsible for it". However, this danger appears now to have been removed in England by the *Defamation Act 2013*, which among other things specifically

lays down that moderating a website will not in itself make the moderator responsible for defamatory material which appears on the site nevertheless, and that the operator of a site will not be held responsible for defamatory material posted by others, provided the person defamed can identify who posted it.

We saw in sec. 7.1.2 that English law has classified Google with distributors rather than with publishers (in the *Tamiz* case), but the current May government wants to change this. However, the motive for that is fighting terrorism. It is easy to imagine that a government might aim to force internet companies to co-operate in the battle against jihadism, without necessarily wanting to give them responsibility for defamatory posts by their users. (We do not know at the time of writing what specific legislation might be proposed in order to make good on Amber Rudd's threat quoted in sec. 7.1.2, so we do not know whether it will be limited in that way.)

At the European level, there has been a great deal of legal interest in a case which was referred in 2013 from Estonia to the European Court of Human Rights, where it was listed as *Delfi AS v. Estonia*. It suggested that internet companies might be held culpable for users' unmoderated comments even if no-one at the company had spotted them. (The case is discussed in some detail by Andrew Murray, 2016: 205–10.) An internet news portal, Delfi, had run a story about a ferry company which allegedly prevented a winter "ice road" being made between some Estonian islands and the mainland, and the comments box below the story filled up with hostile posts about the ferry company. (These were heated and unpleasant, but if the examples quoted by Murray are representative they do not seem to have been damaging in the sense of alleging crooked dealings or dangerous practices. A widely-quoted judgement in an English case, *Nigel Smith v. ADVFN* (2008), pointed out that internet posts often comprise "mere vulgar abuse" which in context no-one would take for serious statements of fact, so that they could not be a basis for libel actions. "Mere vulgar abuse" sounds like an accurate description of the Delfi comments.) After several weeks a representative of the ferry company complained, and Delfi immediately deleted the posts, but the Estonian court held that it ought to have done so without needing the complaint to be made – "it was contrary to the principle of good faith to place the burden of monitoring the comments on their potential victims"; and the Court of Human Rights essentially agreed with this. (On the European legal concept of "good faith" see e.g. Riefa and Hörnle 2009: 112.) If internet companies were going to be punished just for failing to notice users being (very) rude, their position would become extremely difficult. However, Murray (2016: 205–10) believes that the practical legal impact of the *Delfi* decision may be narrower than one might suppose.

In the USA (although its libel law is far milder than the English law) the 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. (It is one of the special favours for online business which Anupam Chander sees as responsible for the success of Silicon Valley, cf. sec. 7.1.1.)

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.

What of the position in England? English law has contained 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. In 2000 the EU brought in an *E-Commerce Directive*, transposed into UK law as the *Electronic Commerce (EC Directive) Regulations 2002*, which seems to have aimed at an effect broadly similar to the American §230. However, Lilian Edwards (2009a: 71–2) explained that in practice member states have often managed to get round this Directive and classify websites as publishers rather than as passive intermediaries.

(There were of course other aspects to this Directive, not all of which were favourable to internet trade. For instance, in a 2008 case, *Bundesverband v. Deutsche Internet Versicherung AG*, the European Court of Justice decided that the Directive required internet traders to publish a phone number where users can contact them 24/7. Christine Riefa and Julia Hörnle, 2009: 114, pointed out that for a small trader hoping to interact with customers by Web only, this creates a large extra financial burden.)

7.5.3 *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 lucrative hobby out 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.

(Incidentally, Lilian Edwards, 2009a: 75, quoted American evidence that the majority of requests at that period to delete items from the material returned by Google were coming in from commercial competitors of the firms which they sought to make invisible!)

British ISPs have sometimes been censoring material even 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."[67] Legal commentators saw NetBenefit's attitude as entirely understandable given English law as it stood.

7.5.4 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 when the E-Commerce Directive was already in force.

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. Under the E-Commerce Directive, Mumsnet should not have been required to do that: the Directive explicitly forbade member states to make internet companies check postings before putting them up. But the Directive did make Web 2.0 sites immune from prosecution only provided they removed legally-objectionable posts "expeditiously" after

receiving a complaint, and Mumsnet was unsure whether a 24-hour delay, the minimum they could be sure of achieving, would count as "expeditious". Lilian Edwards (2009a: 66) believed that if Mumsnet had resisted Gina Ford in court it could have won, but it gave up the fight and settled out of court. 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".[68] 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 to flourish). 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.

A Law Commission report looked at the Electronic Commerce Regulations and concluded that they did not clearly offer an ISP any greater protection in practice than it had under the 1996 Defamation Act. Although the EU never formally repealed the E-Commerce Directive from which those Regulations stemmed, it seems fair to say that parts of it became virtually a dead letter.

7.5.5 PROTECTION DISMANTLED

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.

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.

However, events of the last couple of years have led many people to see even this level of protection for distributors of electronic communications as too strong. We have seen that the 2016 US election campaign triggered a moral panic about "fake news"; and in 2015

Angela Merkel's announcement that Germany would accept unlimited numbers of immigrants from Syria and elsewhere had sparked an avalanche of "hate speech" on Facebook and other social networks (as well as physical attacks on migrants, doubtless encouraged in part by the social media posts). In 2017 the British lawyer Magnus Boyd commented that social media had for years been claiming to be mere passive "aggregators" of communications, but in view of the dominant role they have now achieved within society this was arguably no longer realistic, so that they ought to be treated like newspaper publishers, which routinely have to moderate news stories before they appear rather than waiting for complaints after they go to print.[69]

Social media began responding to this growing change of public mood by putting more effort into deleting objectionable posts. The first Western country to change its law significantly was Germany, in June 2017. The new German law obviously does not apply in Britain, but it is worth mentioning because it may be a straw in the wind showing which way the law internationally is likely to move – namely, further away from the spirit of the US Telecommunications Act mentioned in sec. 7.5.2. It imposes heavy fines, up to €50 million, on social media firms which fail to take down legally-unacceptable posts within 24 hours or seven days of notification, depending on how obvious their illegality is. Facebook had been evading problems with existing German law by basing staff responsible for platform content

outside Germany, but the new law requires social media firms to have designated responsible executives within that country. The law does not go as far as requiring moderation before publication, though both civil-liberties groups and representatives of social media firms argued that, without that, the short deadlines for deleting postings would be impossible to meet. Bernhard Rohleder, head of Bitkom, the German digital trade association, was quoted as saying that

> the requirement to delete posts within 24 hours on platforms that carry up to 1bn posts a day "is utterly impossible to implement in operational terms" and would create a "permanent mechanism of censorship".[70]

Perhaps more significantly, there were indications that the European Commission sees the German law as incompatible with the EU E-Commerce Directive (see above), which worries it not so much for free-speech as for economic reasons: it creates a danger of fragmenting the single European digital market. But Germany happened to be in the middle of a national election campaign, which made it hard for the Commission to object publicly for fear of being seen as interfering in a member state's internal politics. Meanwhile, plenty of commentators were complaining that the new law does not go far enough.

Whether the German law-change will in due course turn out to be a harbinger of wider legal developments, rather than an isolated over-reaction to a temporary moral panic, and whether on the other hand the 2013 Defamation Act will turn out to do more than the E-Commerce Directive to strengthen the legal position of organizations like Mumsnet, are at the time of writing open questions.

7.5.6 LIBELLOUS TWEETS

Exchanges on social media are so chatty and spontaneous that participants have often assumed that they themselves (as opposed to the organizations which provide the channel of communication) are no more likely to be held to account legally for their remarks than in the case of conversation among friends across a coffee-shop table. If people use pseudonyms to post, anonymity may seem to make them safe – but English courts can certainly require a social-media platform to identify the person behind an anonymous post, if the platform is itself within the reach of English law. (And, interestingly, in 2017 a legal precedent was set when a judge agreed to issue an injunction – a court order to desist from specified activity – against "persons unknown".[71] A British businessman, whose name was not revealed, had found that someone was defaming him anonymously on social media. He was able

to discover an e-mail address linked to the defamatory postings, and when the court sent a copy of the injunction to that address with a receipt request, the recipient's pressing the "message received" button was accepted as enough for the injunction to have been duly served. The defamatory posts ceased, before they had gone viral, so we do not know how the court would have attempted to deal with disobedience.)

However, if anyone assumed that the casual nature of social-media comments was itself enough to keep them safe from legal comebacks, the falsity of that assumption was dramatically exposed by the *McAlpine v. Bercow* case in 2013.

Late the previous year, a BBC Newsnight programme and Channel 4 News both announced that a boy in a scandal-hit Wrexham care home had been raped by "a former senior Conservative official from the Thatcher era". The man the programme-makers had in mind was Lord McAlpine, who had been party treasurer; the alleged victim had named him to one of their sources. Newsnight and Channel 4 did not broadcast the name, but the Twittersphere was alive with speculation. The clues provided were enough for many tweets to assert that the programmes had been referring to McAlpine; they gloated over the apparent downfall of one of the mighty.

A few days later, though, the young man in question (reported by the official enquiry into the care-home scandal to be an "unreliable witness") was shown a photo of Lord McAlpine and admitted that he had made a mistake. He went on Newsnight himself to say "Humble apologies to Lord McAlpine. That certainly is not the man that abused me."

It is hard to imagine a more horrible allegation against an innocent man. Lord McAlpine had no choice but to use the means offered by the law to restore his reputation. He sued the television companies, which paid £310,000 in damages between them. But the dissemination of the libel via Twitter tweets and retweets had been on such a massive scale (estimated to have involved more than ten thousand British Twitter users) that he needed to tackle that too.

Lord McAlpine went about this in a subtle way. It would not have been practical to take each individual tweeter to court, so he announced that he would take no action against Twitter users with fewer than 500 followers, provided they tweeted an apology and gave a donation to the BBC Children in Need charity. That left a limited number of higher-profile individuals who were required to make amends on a larger scale: the comedian Alan Davies paid damages of £15,000, and the journalist George Monbiot undertook charitable work to the value of £25,000. But one famous figure insisted that her tweet (to 56,000 followers, many of whom retweeted it) had been innocent, and refused to settle on McAlpine's terms;

so she had to appear in court. This was Sally Bercow, wife of the "First Commoner of the Land" (that is, the Speaker of the House of Commons), and seen by many as something of a loose cannon.

Sally Bercow's tweet ran: "Why is Lord McAlpine trending? *innocent face*". Mrs Bercow claimed that this was no more than a straightforward request for information. But the judge saw the *innocent face* part as amounting to a knowing nudge and wink that pointed readers towards the child-abuse scandal which was raging on social media (and how could anyone sensitive to social nuance disagree?) Mrs Bercow had to apologize publicly and pay damages and Lord McAlpine's costs; the total was not revealed but is estimated at roughly £100,000 (about £15,000 per tweeted word!)

This is a useful lesson to all of us about the dangers of treating an informal channel of communication too casually. In the context of this book, though, the McAlpine case is perhaps less central than those discussed earlier. We are chiefly concerned with law as it impinges on IT professionals in their working lives, rather than on individuals in their private lives. The lesson from those earlier cases is that companies need to be cautious when setting out to reap the commercial advantages envisaged by enthusiasts for "Web 2.0" and social media.

8 REGULATORY COMPLIANCE

8.1 IS SOFT LAW DAMAGING?

When people think about "law", they are usually thinking about the traditional kinds of laws which are laid down in detail by Parliament or EU legislative bodies and enforced through criminal or civil actions in the courts. They tend not to think about delegated or regulatory law – "soft law", as it is sometimes called. We have looked at two examples of regulatory law in chapter 6, the Freedom of Information Act and the Data Protection Act. Both are interpreted in detail and enforced by a civil servant (the Information Commissioner) and a tribunal, rather than through the ordinary legal mechanisms of judges, Crown Prosecution Service, and courts. The Data Protection Act in particular has such huge impact on the IT industry that it merited most of a chapter to itself. But there is far more regulatory law than just these two Acts, and indeed they are not very typical. They focus mainly on the rights of individuals, whereas much regulatory law governs the behaviour of organizations, including businesses, and sometimes does not impinge on people in their private lives at all. The quantity of it is enormous, and so are its consequences for the IT profession.

Regulation of business is necessary, of course, and complaints about excessive red tape are an age-old phenomenon. But in quantitative terms what we have now really is unprecedented. Just to quote one example (not related to IT) that I happened to encounter while drafting this section, Tracy Blackwell and David Pitt-Watson tell us that "in 1990 there were 3,000 pages of regulation covering pensions. Today [i.e. in 2017] there are 166,000."[72] (And incidentally, Blackwell and Pitt-Watson go on to suggest that the pension industry is not actually functioning better now than in 1990.) In this chapter I shall outline a handful of examples of soft law, other than those already discussed, to give a flavour of how organizations are affected; but readers should bear in mind that these are only sample buckets drawn from an ocean.

One point that needs to be made is that, in many people's eyes, regulatory law tends not to be very good law.

When we talk about "good law" and "bad law", most commonly we are thinking about whether or not we agree with the effect that the law is aiming to achieve. But an area of law can be good or bad in another, functional sense, depending whether it works well: those to whom it applies can understand what it requires, it can be enforced, and complying with

it is not unreasonably burdensome. In this functional sense, it is fair to say that delegated law has something of a reputation as inferior to law enacted directly by Parliament.

One problem is consistency. The Parliamentary officers responsible for drafting English statutes are rather good at making sure that one new law does not contradict another. When the task of fixing the details of new law is delegated to different regulatory agencies, this kind of harmony becomes harder to maintain. By now this is not merely a hypothetical risk. Contradictions do indeed exist, such that one law requires people to do something which another law forbids them to do. By 2003 Michael Fabricant, then shadow e-commerce minister, was moved to say 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."[73]

Furthermore, even if there are no contradictions between regulations, the fact that they are made by a multiplicity of agencies rather than all having to squeeze through a single Parliamentary bottleneck means that regulations proliferate, to the point where firms are scarcely capable of keeping track of all the rules they are expected to obey. The lawyer George Gardiner wrote "Nobody can comply with every law; it's a question of prioritising business interests and watching out for which regulator has the big stick."[74] It hardly needs saying that this is a highly undesirable situation, but it seems inherent in the system of delegating powers to make and to enforce laws.

Another frequent problem with regulatory laws is that they can involve a large element of human discretion, and hence unpredictability. Often, the statutes which form the basis of regulation give less detail about what is required than the Data Protection Act does, leaving more interpretation to be done by regulators.

We saw in sec. 2.4.6 that an issue which is particularly subject to regulation in our industry is monopolistic behaviour, and I gave the example of the fine levied in 2017 by the European Commission on Google, which it regarded as abusing a monopoly position. But a difficulty is that deciding whether a monopoly exists, and, if so, whether it is being abused, involves judgements which are unavoidably subjective. Google is not the only internet search engine: Microsoft's Bing, for instance, is only "one click away", so people could use that instead (but mostly they don't). People nowadays often use Amazon to compare prices, but the European Commission did not count Amazon as a "search engine" and hence as a competitor to Google. Furthermore, even if we accept that Google had an effective monopoly, was its action in promoting its Shopping site an abuse of that position, or simply a wise and proper commercial decision? Determining that competition law has been violated depends on considerations of economic theory and perhaps even of philosophy, whereas in other areas of life we expect the

law to tell us what it requires in a blunter, more impersonal and black-and-white fashion. One commentator[75] claims that the 2017 decision went against Alphabet only because the previous EU competition commissioner happened to be succeeded in January that year by Margrethe Vestager, a lady with a notably aggressive personality – in her Brussels office she keeps a statuette of a hand giving the finger. (The US Federal Trade Commission had looked at the same issue but decided to take no action, and indeed there have been a whole series of cases since the turn of the millennium in which the EU has taken a tough line against American technology firms for behaviour that the US authorities found acceptable. For a while, many Americans were indignant about Europeans forcing US companies to change their working practices, though lately they seem to have become more used to it.)

Economists all agree that, as a general rule, monopolies are a bad thing. But quite a number of economically-literate observers argue that it is counterproductive to attack the particular kinds of monopoly which arise from IT network effects. While the EU was still considering the Google case, Matthew Lynn wrote

> …an open search engine such as Google promotes far more competition than it will ever stifle. Millions of new and small businesses have been able to tap into a huge and instant market because they can publicise products through the web so easily. Banks, insurers

> and retailers can't get away with expensive, poor-quality products anymore… Second, the tech companies are furiously innovative. Google is pouring $10bn a year into research and development…What does it say about the way the EU is run that it wants to punish a company spending the equivalent of the GDP of a small nation on R&D every year?[76]

The fact that regulatory law often seems to give regulators more discretion in choosing how to apply their rules than ordinary law gives to judges is one reason why it is seen as a questionable kind of law, but it is by no means the only reason. Another is that regulation has become so pervasive that it can distract businesses from their proper task of searching for ways to wring more value out of finite resources. *The Economist* comments that regulators are "making it harder for bosses to look beyond quarterly earnings. Boards are devoting less time to strategy and more to enforcing regulations."[77]

Some observers object to the growth of regulatory law in strong terms. Innovation is the lifeblood of economic growth in any society, but Sir Richard Lapthorne, chairman of Cable & Wireless, quotes the government's Chief Scientific Adviser as having "concluded that the growth in so-called 'Soft Law' in the UK…is killing innovation."[78] And he quotes an unnamed senior London lawyer as

> explain[ing] that you can never fight regulators: "If they believe they are losing in a line of attack they can just change the rules to favour their evidence…" This [Sir Richard continues] sounds like the type of behaviour pursued by the most oppressive regimes around the world, past and present – dictatorships…that function as prosecutor, judge and jury in persecuting their citizens.
>
> One might believe this could never happen in the UK. The truth is that it does – except that most examples happen in private and people often feel under pressure to condone it.

Are Sir Richard's comments over the top? I am not sure.

In our role as citizens, we should perhaps consider whether this feature of present-day society needs to be challenged. However, this book is addressed to readers in their role as potential or actual members of the IT profession, and we are concerned with understanding the present-day realities of law as it applies to our industry. Whether we like it or not, the fact is that regulatory law has become a very powerful factor indeed.

8.2 A MEDIUM OF REGULATION

There is plenty of business regulation that has nothing in particular to do with IT, of course. But a great deal of it has. Increasingly, regulators are using IT as a medium of regulation.

In earlier chapters, most of the time 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 in the 21st century, when 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 "this is how you must use computers", or "you must do P, Q, and R", where P, Q, and R are things that could not have been achieved at all without computers.

(Many of these things, while important to business, are remote from the private consumer's point of view – but not all. For instance, under a recent EU regulation, every new car sold in Europe from 2018 will have to be part of the "internet of things": cars and other motor vehicles must be fitted with "e-call" technology which automatically contacts emergency services in the case of a crash.)

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 has been starting to demand are things at the very edge of what we are capable of doing, 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.

8.3 SARBANES-OXLEY AND AFTER

Regulation of business IT has stepped up to a higher gear in the 21st century, 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 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.[79]

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.

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. (In 2018 it is due to be replaced by a new and more stringent *MiFID II* régime.) *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 financial crises of that year 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. (Again, a more stringent *Basel III* is coming shortly.) 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. The total annual cost of regulatory compliance to British business by 2005 was estimated by the National Audit Office (2007) at just under £20 billion – and this was just direct costs: one body representing small and medium-sized businesses suggested in 2014 that the time taken to understand and implement regulatory changes was costing firms twice as much, in terms of lost opportunities, as the direct costs of compliance.[80] (A manager who spends a day dealing with some aspect of regulation is not spending that day finding or progressing new revenue-earning business.)

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.[81]

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, expected it to 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.[82]

It would be hard to exaggerate the impact on business of the recent growth of regulation. According to Richard Lumb of Accenture, writing in 2017, since the financial crisis "a single large global bank might have 20,000-plus people working solely in [the] area [of regulatory

compliance]".[83] And, as Lumb points out, it is likely that this large new area of work will only successfully be addressed via innovative applications of information technology – Lumb sees this as "One of the greatest potential applications of AI…where there is a persistent skills shortage".

It is worth noticing, incidentally, that increasing business regulation, apart from its obvious costs, has a large hidden cost in terms of reducing trust. We saw in sec. 6.14 that this is a large problem for electronic business. New regulation is being introduced to try to compensate for reduced trust levels, but this is a vicious circle in which increased regulation reduces trust even further. An anonymous non-executive director of a FTSE 100 firm commented in 2011:

> instead of people relying on integrity and trust, businesses think "If we're in a regulator's rules, I'll play by those rules" and then there's a temptation to game those rules or push them to the wire because it's a rule and it's different from a trust based system.[84]

However, our concern in this book is with what the law is, not whether it is good or bad law. Regulation versus trust is an issue that should concern us seriously as citizens, but it is not one we can pursue further here.

8.4 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 various later laws culminating in the *Equality Act 2010*. 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. (For a brief summary, see Picton 2007: 182.) 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 legal case about Web accessibility in Britain,[85] though the Royal National Institute for the Blind 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! The disability discrimination regulations being delegated law, *Maguire* was decided by a "Human Rights and Equal Opportunity Commission" rather than a law court. Reading the Commission's 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 ours, 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". For instance, 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."[86] In 2017 one survey reported that fewer than one in three of local authority websites meet accessibility requirements.

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

8.5 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. As said in sec. 6.3, many people file e-mails chaotically. 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 enormous 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 has become a large problem in lesser cases. In a linked pair of New Jersey cases, *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, it was reported while the cases were still ongoing in 2008 that the company was demanding

> 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.[87]

(The pair of cases were settled in the plaintiffs' favour in 2009.) Rebecca Love Kourlis, formerly a judge and now director of the academic Institute for the Advancement of the

American Legal System, anticipated 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.

In 2007 Malcolm Wheeler described e-discovery as "the single most significant change to the legal system" in his forty years as an American business lawyer.[88] American companies have had 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 English rules on discovery (or "disclosure") are different 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 (Blair and Maron 1985). Consequently, lawyers have been turning to artificial-intelligence-based "machine learning" techniques such as *predictive coding*, first approved by a UK court for use in e-disclosure in 2016. A British judge was quoted in 2015 as expecting such techniques to become the norm quite soon.[89]

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 discussed 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.[90]

By contrast, Dale discussed the advantages of one of the systems being 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.

It is widely claimed that AI techniques can already outperform humans at e-discovery tasks (as well, obviously, as being far cheaper), and no doubt future AI research will improve performance further.

8.6 PUNISHED FOR MISFORTUNE?

In the summer of 2017 Britain experienced a series of IT breakdowns in companies providing infrastructure services such as transport. An IT collapse, never satisfactorily explained, at British Airways over a bank holiday weekend left thousands of passengers stranded, often separated from their luggage. Shortly before, a ransomware program called WannaCry had attacked many NHS computer systems (as well as various systems in other countries), bringing the Service to its knees temporarily, with doctors in many regions unable to access patients' records, surgical operations cancelled, and so forth; the attack was only halted through an almost chance intervention by an amateur.

The response by the Digital Minister, Matthew Hancock, in August was to announce plans to force organizations providing "essential services" – transport companies, energy and water providers, hospitals, and internet companies – to protect their systems better, by enabling regulators to impose huge fines for such breakdowns; figures mentioned were up to £17 million or four per cent of global turnover. And a similar government plan, announced a little earlier in the same year, related to the prospect of cars becoming part of the "internet of things", mentioned in sec. 8.2 above: car manufacturers will be required to step up the protection they provide against hackers.

At the time of writing we do not yet know how laws to achieve these goals will be framed, but it seems that they will have to involve regulations of an unusual kind. We are used to firms being fined for providing harmful services, but not for getting into situations where they are unable to provide services (apart from cases where the services are provided under contracts that specify penalties for non-performance). It is routine for hackers to be punished if they are caught, but punishment for "hackees" appears to break new ground.

Sceptically, one can wonder how successful such a regulatory régime can hope to be. After the loss of about £10 billion of public money on a failed project to equip the NHS with a unified national computing infrastructure (the world's largest-ever non-military IT project), which a competent IT professional should have been able to predict could never succeed, I pointed out (Sampson 2012: 42) that the domains of government and computing

> are founded on contrary assumptions. In the government world, it is a given that sufficient authority will elicit any desired action. In the world of informatics, authority is impotent. Bring as much pressure as you like to bear on a flawed software system, and what you will get is a worse-flawed system.

The shift from a "world of atoms" to a "world of bits" has undermined a number of fundamental assumptions which had served so well for so many centuries that they came to seem axiomatic – and most people who are not themselves IT professionals, certainly including our political leaders, have not yet got their minds round the downfall of those assumptions (Sampson 2017). The professionally responsible attitude, I would argue, should be that it is reasonable and desirable to debate whether the risk of some complex software system misbehaving is worth the gains from replacing manual systems in that function with automatic systems, but it is not reasonable to expect the system never to misbehave. It is

in the nature of computer software that there *will* be unpredictable breakdowns, however much care is put into avoiding them. (Some software systems may function as expected indefinitely, but we cannot know in advance which ones will fail or how they will fail.)

From this point of view, the proposed new category of IT regulation looks a little like punishing people for getting ill. If people were punished severely for illness, probably the incidence of illness would fall a little – people would put even more effort into avoiding infections, exercising, and so forth. But it is hard to believe that the reduction would be great, because nobody wants to get ill anyway. So, quite apart from the moral oddity of punishing people for misfortune, doing so would be a silly, ineffective policy. We shall have to see whether the new regulatory proposals turn out to make better sense. At the time of writing, we do not know how it would be decided whether a given IT breakdown is culpable, or whether the organization which suffered it should not be blamed because it had taken all expected precautions even though these proved not to be enough. (It is easy to imagine that such nebulous decisions might be influenced in practice by whether or not the organization happens to be popular with the regulators, or with society at large.)

But, as ever, the silver lining to the cloud is that greater incentives to avoid any possibility of computer breakdowns are sure to create more work, and interesting work, for computing graduates.

8.7 CONCLUSION

With that glimpse into the future, our brief survey of some aspects of law which matter to the IT profession is complete.

It has necessarily been selective. There are a number of subjects I could have chosen to write about, if I had wanted to make this book longer than it is. Here, for instance, are a few topics I have left undiscussed:

- employment law – the rise of the IT-mediated "gig economy" has created contentious legal issues about whether people working for organizations like Uber or Deliveroo should be entitled to the sickness and holiday benefits of employees
- computer fraud
- taxation of internet business – there are many complexities, for instance under British VAT rules the "place of supply" of an e-publication has to be decided in terms of whether the contents are predominantly fiction or non-fiction (Taubman 2009: 23n63)

- electronic money such as Bitcoin, and other applications of blockchain technology
    - law in "virtual worlds" like Second Life or World of Warcraft (South Korea has been taxing the incomes players earn in virtual worlds since 2007).

I chose to leave these things out, because to me they seem less central than the topics I have covered – but the point is arguable. Even the subjects I have included could be discussed here in only the barest outline. But, for readers planning careers as computing professionals rather than lawyers, I hope what I have written may be enough to give them the necessary general awareness of the legal framework within which their working lives will proceed.

It only remains for me to wish readers all possible success, good fortune, and fun, in their careers in our industry.

REFERENCES

Aldhouse, Francis, 1991. "UK data protection – where are we in 1991?", *Yearbook of Law Computers and Technology*, 5.180–7.

Bainbridge, David, 2007. *Introduction to Information Technology Law*, 6th edn. Pearson Longman.

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

Bodard, Katia, Bruno de Vuyst, and Gunther Meyer, 2004. "Deep linking, framing, inlining and extension of copyrights: recent cases in Common Law jurisdictions", *Murdoch University Electronic Journal of Law*, March 2004.

Boldrin, Michele, and David Levine, 2013. "The case against patents", *Journal of Economic Perspectives*, 27.3–22.

Brin, David, 1998. *The Transparent Society: will technology force us to choose between privacy and freedom?* Perseus Books (Reading, Mass.).

Chandler, Anupam, 2014. "How law made Silicon Valley", *Emory Law Journal*, 63.639–94.

Cunningham, Alan, and Chris Reed, 2013. "Consumer protection in cloud environments". In Millard 2013.

Edwards, Lilian, 2009a. "The fall and rise of intermediary liability online". In Edwards and Waelde 2009.

Edwards, Lilian, 2009b. "Privacy and data protection online: the laws don't work?" In Edwards and Waelde 2009.

Edwards, Lilian, and Charlotte Waelde, eds, 2009. *Law and the Internet*, 3rd edn. Hart Publishing (Oxford).

Elliott, Catherine, and Frances Quinn, 2017. *English Legal System*, 18th edn. Pearson.

Holt, Jeremy, 2011. "IT contracts". In Holt and Newton 2011.

Holt, Jeremy, and Jeremy Newton, eds, 2011. *A Manager's Guide to IT Law*, 2nd edn. British Computer Society.

Hörnle, Julia, 2009. "The jurisdictional challenge of the internet". In Edwards and Waelde 2009.

Hunter, Dan, 2003. "Cyberspace as place and the tragedy of the digital anticommons", *California Law Review*, 91.439–519.

Johnson, David, and David Post, 1996. "Law and borders – the rise of law in cyberspace", *Stanford Law Review*, 48.1367–1402.

Kuan Hon, W., Christopher Millard, and Ian Walden, 2013. "Negotiated contracts for cloud services". In Millard 2013.

Lanier, Jaron, 2014. *Who Owns the Future?* Penguin.

Leigh, Jon, and Graham Wood, 2011. "Software escrow". In Holt and Newton 2011.

Lessig, Lawrence, 1999. *Code and Other Laws of Cyberspace*. Basic Books (New York).

Litman, Jessica, 2000. "The DNS Wars: trademarks and the internet domain name system", *Journal of Small and Emerging Business Law*, 4.149–66.

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

Lloyd, Ian J., 2017. *Information Technology Law*, 8th edn. Oxford University Press.

Macdonald, Elizabeth, 2005. "Bugs and breaches", *International Journal of Law and IT*, 13.118–38.

Manchester, Colin, 1995. "Computer pornography", *Criminal Law Review*, July 1995, pp. 546–55.

Manchester, Colin, 1996. "More about computer pornography", *Criminal Law Review*, September 1996, pp. 645–9.

Manchester, Colin, and David Salter, 2006. *Exploring the Law: the dynamics of precedent and statutory interpretation*, 3rd edn. Sweet & Maxwell.

Manyika, James, et al., 2016. *Digital Globalization: the new era of global flows*. McKinsey Global Institute (New York).

Millard, Christopher, ed., 2013. *Cloud Computing Law*. Oxford University Press.

Murray, Andrew, 2016. *Information Technology Law*, 3rd edn. Oxford University Press.

National Audit Office, 2007. *Reducing the Cost of Complying with Regulations*. HMSO.

Newton, Jeremy, 2011a. "Systems procurement contracts". In Holt and Newton 2011.

Newton, Jeremy, 2011b. "System supply contracts". In Reed 2011.

Picton, Vivian, 2007. "Accessibility and information security". In Jon Fell et al., *IT Law: an ISEB foundation*. British Computer Society.

Pitt-Payne, Timothy, 2011. "Access to electronic information". In Reed 2011.

Press, Tim, 2007. "Patent protection for computer-related inventions". In Chris Reed and John Angel, eds, *Computer Law: the law and regulation of information technology*, 6th edn. Oxford University Press.

Reed, Chris, ed., 2011. *Computer Law*, 7th edn. Oxford University Press.

Reed, Chris, 2012. *Making Laws for Cyberspace*. Oxford University Press.

Riefa, Christine, and Julia Hörnle, 2009. "The changing face of electronic consumer contracts in the twenty-first century: fit for purpose?" In Edwards and Waelde 2009.

Rowland, Diane, Uta Kohl, and Andrew Charlesworth, 2017. *Information Technology Law*, 5th edn. Routledge.

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

Russell, Stuart, 2015. "Take a stand on AI weapons", *Nature*, 521(7553), 28 May 2015.

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

Sampson, Geoffrey, 2012. "Whistleblowing for health", *Journal of Biological Physics and Chemistry*, 12.37–43. <www.grsampson.net/AWfh.pdf>.

Sampson, Geoffrey, 2017. "Obsolete assumptions", *Nanotechnology Perceptions*, 13.132–6. <www.grsampson.net/AOass.pdf>.

Schultz, Thomas, 2008. "Private legal systems: what cyberspace might teach legal theorists", *Yale Journal of Law and Technology*, vol. 10, issue 1, article 5. <digitalcommons.law.yale.edu/yjolt/vol10/iss1/5>.

Stapleton, Jane, 1991. "Three problems with the new product liability". In P. Cane and Jane Stapleton, eds, *Essays for Patrick Atiyah*, Oxford University Press.

Susskind, Richard, 2008. *The End of Lawyers? Rethinking the nature of legal services*. Oxford University Press.

Taubman, Antony, 2009. "International governance and the internet". In Edwards and Waelde 2009.

Trakman, Leon E., 1983. *The Law Merchant: the evolution of commercial law*. Fred B. Rothman & Co. (Littleton, Colorado).

Ward, Richard, and Amanda Akhtar, 2011. *Walker & Walker's English Legal System*, 11th edn. Oxford University Press.

Ward, Richard, and Amanda Wragg, 2005. *Walker & Walker's English Legal System*, 9th edn. Oxford University Press.

Wiener, Jarrod, 1999. *Globalization and the Harmonization of Law*. Pinter.

Winn, Jane, and Benjamin Wright, 2005. *The Law of Electronic Commerce*, 4th edn. Aspen Publishers (New York).

ENDNOTES

1. Adapted from a remark by Dave Bailey, "Why IT failure comes easily to government", *Computing*, 20 Aug 2009.
2. Ian Campbell, "The new skillseekers", *Computing*, 13 Sep 2007.
3. Quoted by Ben Wright and Ben Marlow in the *Daily Telegraph*, 23 Jan 2017.
4. Lawyers often write *judgment*, with no central E. This could be a useful convention to distinguish the technical legal sense discussed here from the everyday sense of the word (e.g. "She is a woman of sound judgement"), but in practice lawyers do not observe that distinction: they often use their special spelling for the everyday sense too. So it seems simpler in this book to use the ordinary spelling throughout.
5. In 1999 the ancient term *plaintiff*, for the party who initiates a lawsuit, 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 to a non-lawyer seems both more familiar and less ambiguous than "claimant" in this sense, so this book will continue to use the word "plaintiff".
6. On this phenomenon see "Fuel of the future", *The Economist*, 6 May 2017.
7. See "We'll see you, anon", *The Economist*, 15 Aug 2015.
8. Jack Simson Caird, "Legislating for Brexit: the Great Repeal Bill", House of Commons Briefing Paper 7793, 23 Feb 2017. The formal name is now "European Union (Withdrawal) Bill".
9. See e.g. Adam Bienkov, "Theresa May's Great Repeal Bill will be the biggest political power grab of modern times", *Business Insider UK*, 7 Mar 2017. <uk.businessinsider.com>.
10. <www.axelos.com/best-practice-solutions/itil>
11. <www.isoiec20000certification.com>
12. For more about SLAs, see Holt (2011: 10–11); and for detailed discussion of the art of drafting successful IT contracts, see particularly Newton (2011a).
13. Reuven Cohen, "The cloud hits the mainstream: more than half of U.S. businesses now use cloud computing", *Forbes*, 16 Apr 2013.
14. UN Department of Economic and Social Affairs, *International Merchandise Trade Statistics: concepts and definitions*, 1998. <unstats.un.org/unsd/publication/SeriesM/SeriesM_52rev2E.pdf>.
15. Elizabeth Macdonald (2005) discusses the question of when bugs amount to breach of a software contract.
16. *Product Liability Directive*, article 7(e).
17. See Kevin Delaney, "Why Bill Gates would tax robots", *Quartz*, 17 Feb 2017. <qz.com/911968>.
18. Alan Tovey, "Warning shots fired over BAE's robot tank plans", *Daily Telegraph*, 11 Sep 2017.
19. Reported in *Daily Telegraph*, 15 Mar 2017.
20. For an academic discussion see Abel Castilla and Jeremy Elman, "Artificial intelligence and the law", *TechCrunch*, 28 Jan 2017. <techcrunch.com/2017/01/28/artificial-intelligence-and-the-law>.
21. Reported in the *Daily Telegraph*, 7 Dec 2006.
22. Quoted by Brian Runciman, "Berners-Lee visits key web issues", *Computing*, 6 Apr 2006.
23. Quoted by Stuart Sumner, "UK aims to break curse of the patent trolls", *Computing*, 2 Aug 2012.

24. Roy Schestowitz, "With software patents in Europe […] patent trolls now come to Europe, attack Android/Linux", *Techrights*, 10 May 2015. <techrights.org/2015/10/05/patent-trolls-in-london>.
25. Quoted in "ITU holds patent roundtable", *The Guardian*, 10 Oct 2012. A *standard-essential patent* is one covering a process that has become part of a formal industrial standard, so that any firm engaged in that industry must use it. The holder of such a patent is required to license it to all comers (including competitors), on "fair, reasonable, and non-discriminatory" terms, but this requirement leaves a lot of legal wiggle-room.
26. House of Commons, Fourth Standing Committee on Delegated Legislation, 3 Dec 1997.
27. Claims at the EPO are conventionally identified as *Applicant's name/nature of invention to be covered*.
28. See Tysver, "Are software and business methods still patentable after the Bilski decisions?", *BitLaw*, 2015. <www.bitlaw.com>.
29. Gene Quinn, "A software patent setback: Alice v. CLS Bank", *IPWatchdog*, 9 Jan 2015. <www.ipwatchdog.com>.
30. For a critical summary see Julia Reda, "Extra copyright for news sites". <juliareda.eu/eu-copyright-reform/extra-copyright-for-news-sites>.
31. Quoted from a piece "You've been framed" on the Farrer & Co. website and dated Spring 2001, since deleted.
32. Quoted in Lloyd (2017: 365).
33. 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".
34. "The race to build the world's first sex robot", *The Guardian*, 27 Apr 2017.
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. Pitt-Payne (2011: 668–72).
36. Jimmy Desai, "Email archiving: UK law, regulations and implications for business", MessageLabs (Gloucester), 2009.
37. "Digital dilemmas: a survey of the internet society", *The Economist*, 25 Jan 2003.
38. 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, and it is clearly that impact which is most relevant to the IT profession).
39. Quoting a November 2003 piece by Alan Raul et al., "EU privacy: European Court of Justice hands down landmark decision on EU Data Protection Directive", later deleted from the website of Sidley Austin LLP.
40. 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*.
41. David Scheer, "Europe's new high-tech role: playing privacy cop to world", *Wall Street Journal*, 10 Oct 2003.
42. Quoted from a 2005 piece "What's wrong with enforcement?" on a website *DPA Law* which is no longer extant.
43. "Rules for loneliness", *The Spectator*, 4 Feb 2017.
44. European Commission press release, January 2012. <europa.eu/rapid/press-release_IP-12-46_en.htm>.

45. SMSR Ltd, *Report on Information Commissioner's Office Annual Track 2006: Individuals*, p. 15. <foia.blogspot.co.uk/tracindivs2006.pdf>.
46. "Personal data will never be safe, says Brown", *Daily Telegraph*, 3 Nov 2008.
47. "A quarter of official databases fall foul of the law, say experts", *Daily Telegraph*, 23 Mar 2009.
48. Quoted by Polly Sprenger, "Sun on privacy: 'Get over it' ", *Wired*, 26 Jan 1999.
49. <www.eff.org/cyberspace-independence>
50. Quoted in Daniel Boffey and Jill Treanor, "George Osborne on Google tax deal vindicates government approach", *The Guardian*, 23 Jan 2016.
51. See e.g. "Eroding exceptionalism", *The Economist*, 11 Feb 2017.
52. See e.g. "Chaining giants", *The Economist*, 12 Aug 2017.
53. <www.channel4.com/news/by/jon-snow/blogs/mactaggart-lecture-edinburgh-2017>
54. Sam Dean and Hayley Dixon, "Apology is not enough to end hate row, Google told", *Daily Telegraph*, 21 Mar 2017.
55. On the history of IT companies' reluctance to co-operate with security services battling terrorism and other crime that is facilitated by those companies, see e.g. Madhumita Murgia, "Tim Cook's defiance of the FBI is something we should all support", *Daily Telegraph*, 19 Feb 2016, and "Fighting the cyber-jihadists", *The Economist*, 10 Jun 2017.
56. Quoted by Mark Hughes, "Google not liable for online claims, court rules", *Daily Telegraph*, 3 Mar 2012.
57. Kate McCann and Hayley Dixon, "Bomb ingredients sold together on Amazon", *Daily Telegraph*, 19 Sep 2017.
58. James Titcomb, "Microsoft and Google relent over piracy links with new pact", *Daily Telegraph*, 20 Feb 2017.
59. Quoted in "Argos in the clear over 49p TV e-commerce error", *ZDNet*, 2 Sep 2005. <www.zdnet.com>.
60. "Not-so-clever contracts", *The Economist*, 30 Jul 2016.
61. "IP: trademark & domain names", *Cybertelecom*, June 2006. <www.cybertelecom.org/dns/trademark.htm>.
62. On the "multi-stakeholder" model see Stuart N. Brotman, "Multistakeholder Internet governance: a pathway completed, the road ahead", July 2015. <www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf>.
63. See "A plaything of powerful nations", *The Economist*, 1 Oct 2011.
64. Michael Gurstein, "Multistakeholderism vs. democracy: my adventures in 'Stakeholderland'", 20 Mar 2013. <gurstein.wordpress.com>.
65. "Premium domain names lose appeal", *IT Week*, 6 Nov 2006.
66. See e.g. "When not using a competitor's trade mark might still infringe it – the curious case of negative matching", 3 Jul 2015. <www.fieldfisher.com/publications/2015/07/case-of-negative-matching>.
67. Statement of 6 Apr 2000 by Alison Sparshatt, MD of NetBenefit. <rosecottage.me.uk/OutRage-archives/2000d24outcast.htm>.
68. Quoted by Hugh Muir, "Childcare expert threatens to have website shut down", *The Guardian*, 8 Aug 2006.
69. Interview on BBC Radio 4 "Law in Action" programme, 21 Mar 2017.
70. Guy Chazan, "Rise of refugee 'fake news' rattles German politics", *Financial Times*, 15 Feb 2017.

71. See Monidipa Fouzder, "Success in 'fake news' injunction first", *Law Society Gazette*, 24 Jul 2017.
72. "Reform finance and we should all benefit", *Daily Telegraph*, 4 Aug 2017.
73. Quoted by Sarah Arnott and James Watson, *Computing*, 18 Sep 2003.
74. "Weighing up security and compliance", supplement to *IT Week*, 24 Apr 2006.
75. James Titcomb, "How Europe's chief regulator knitted a case against Google", *Daily Telegraph*, 28 Jun 2017.
76. "EU must leave Google alone and create its own tech giants", *Daily Telegraph*, 23 Jun 2015.
77. *The Economist*, "The big engine that couldn't", 19 May 2012.
78. Sir Richard Lapthorne, "Regulators are the new dictator class of our society", *Daily Telegraph*, 17 Jun 2015.
79. This and the Schrader quotation following are taken from Jason Compton, "Compliance: businesses will have to pull their SOX up", *Computing*, 31 Mar 2005.
80. Carina Perkins, "Money for nothing: SMEs in dire straits on compliance costs", *Hospitality News*, 7 Aug 2014. <www.bighospitality.co.uk>.
81. Quoted by James Watson, "Banks urged to stay ahead of the MiFID game", *Computing*, 2 Feb 2006.
82. Quoted by Dave Bailey, "How data rules will burden business", *IT Week*, 9 Oct 2006.
83. Richard Lumb, "Rise of the robots must be used as a means of enhancing humans' work", *Daily Telegraph*, 3 Apr 2017.
84. Quoted in *The Trust Deficit – Views from the Boardroom*, a 2011 report by Populus, commissioned by DLA Piper. <www.dlapiper.com>. On declining levels of trust in recent American business life see "Suspicious minds", *The Economist*, 12 Aug 2017.
85. With the exception of one rather unusual case in 2006–7 about an American company without a presence in the UK, which offered an exam for a professional qualification online to a blind candidate in Scotland.
86. <www.blether.com/archives/2006/05/dti_achieves_ne.php>
87. "The big data dump", *The Economist*, 30 Aug 2008.
88. Quoted in "Of bytes and briefs", *The Economist*, 19 May 2007.
89. Grania Langdon-Down, "E-disclosure: electric avenues", *Law Society Gazette*, 13 Jul 2015. See also Jonathan Maas, "Legal AI vs eDiscovery", *Artificial Lawyer*, 9 May 2017. <www.artificiallawyer.com>.
90. This and the following quotation are from a 2008 White Paper by Chris Dale, no longer available on the Web. For EnCase see <https://www.guidancesoftware.com/document?products=EnCase-eDiscovery>.