8 Regulatory compliance

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

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

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

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

8.1 Sarbanes–Oxley and after

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

By 2006 the lawyer George Gardiner was more forthright:

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

But some regulators have large and painful sticks.

8.2 Accessibility

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

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

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

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

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

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

Maguire won his case and the Olympics Committee was fined A$20,000. As a precedent this case is not straightforward, though. Because the plaintiff was himself in the assistive-technology business, he wanted a great deal of technical information that would be irrelevant for most blind site visitors, and which the Olympics Committee resisted handing over because it was commercially-sensitive intellectual property belonging to themselves and their IT contractor, IBM. Another problem seems to have been that some of those involved in the legal dispute were not technically competent; at one point the Committee stated that because of commercial confidentiality it would not release the HTML source code for pages it had already put up on the Web – whoever drafted that statement evidently did not know how the World Wide Web works! Rather than being heard in an ordinary law court, *Maguire* was decided by a "Human Rights and Equal Opportunity Commission". Reading their judgement makes it difficult to avoid the suspicion that they were swayed more than an ordinary judge would be by bias in favour of the disabled.

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

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

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

8.3 E-discovery

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.4 Conclusion

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

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

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