

Software and the law



About this free course

This free course is an adapted extract from the Open University course M814 *Software Engineering* www.open.ac.uk/postgraduate/modules/m814.

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University –

www.open.edu/openlearn/science-maths-technology/software-and-the-law/content-section-0

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Copyright © 2016 The Open University

Intellectual property

Unless otherwise stated, this resource is released under the terms of the Creative Commons Licence v4.0 http://creativecommons.org/licenses/by-nc-sa/4.0/deed.en_GB. Within that The Open University interprets this licence in the following way:

www.open.edu/openlearn/about-openlearn/frequently-asked-questions-on-openlearn. Copyright and rights falling outside the terms of the Creative Commons Licence are retained or controlled by The Open University. Please read the full text before using any of the content.

We believe the primary barrier to accessing high-quality educational experiences is cost, which is why we aim to publish as much free content as possible under an open licence. If it proves difficult to release content under our preferred Creative Commons licence (e.g. because we can't afford or gain the clearances or find suitable alternatives), we will still release the materials for free under a personal end-user licence.

This is because the learning experience will always be the same high quality offering and that should always be seen as positive – even if at times the licensing is different to Creative Commons.

When using the content you must attribute us (The Open University) (the OU) and any identified author in accordance with the terms of the Creative Commons Licence.

The Acknowledgements section is used to list, amongst other things, third party (Proprietary), licensed content which is not subject to Creative Commons licensing. Proprietary content must be used (retained) intact and in context to the content at all times.

The Acknowledgements section is also used to bring to your attention any other Special Restrictions which may apply to the content. For example there may be times when the Creative Commons Non-Commercial Sharealike licence does not apply to any of the content even if owned by us (The Open University). In these instances, unless stated otherwise, the content may be used for personal and non-commercial use.

We have also identified as Proprietary other material included in the content which is not subject to Creative Commons Licence. These are OU logos, trading names and may extend to certain photographic and video images and sound recordings and any other material as may be brought to your attention.

Unauthorised use of any of the content may constitute a breach of the terms and conditions and/or intellectual property laws.

We reserve the right to alter, amend or bring to an end any terms and conditions provided here without notice.

All rights falling outside the terms of the Creative Commons licence are retained or controlled by The Open University.

Head of Intellectual Property, The Open University

Contents

Introduction	4
Learning Outcomes	5
1 Why law is necessary	6
2 Intellectual property (IP) rights	8
2.1 Motivations for IP laws	8
2.2 International cooperation on IP	10
3 IP rights: copyright, patents, marks and brands	13
3.1 Copyright	13
3.2 Patents: introduction	19
3.3 Patents and software in the EU	19
3.4 Patents and software in the US	22
3.5 Trade marks, service marks and brands	23
4 IP rights: Common and public goods	25
5 Contracts	27
5.1 Breach of contract	27
5.2 Contract analysis	28
6 Responsibilities to employees and the public	31
6.1 Data protection legislation	31
6.2 Data protection law in the UK	31
6.3 Libel and defamation	34
6.4 Product liability and negligence	34
6.5 Limiting liability	34
6.6 Health and safety	36
6.7 Best practice in health-and-safety regulations	36
7 External threats	39
7.1 Legislation on misuse	39
7.2 Virus propagation as misuse	40
Conclusion	41
Glossary	41
References	42
Acknowledgements	44

Introduction

This free course, *Software and the law*, explores the laws relevant to software and its use – taking a global perspective, since the trade in software is international and information made available on the web can be viewed globally.

A major part of this course is devoted to intellectual-property law – the issue of who owns software and digital content and how that ownership can be protected by the law. You'll learn about copyright and patents, and international agreements aimed at harmonising laws in this area. We will look at how the laws aimed at protecting public goods can also be exploited to protect the public good.

Software is acquired or developed for a specific purpose, with the relationship between purchaser and supplier governed by some sort of contract. What should such a contract cover?

Software can do people harm in a number of ways – including by making public information that should be kept private, by defamation, or by supplying false information that leads people into error. Who should be held liable? How can the law protect you?

We shall illustrate our account of the law with examples from around the world – we want to enable you to explore the laws of your own country to understand their scope in your context.

This OpenLearn course is an adapted extract from the Open University postgraduate computing course, [M814 Software Engineering](#).

Learning Outcomes

After studying this course, you should be able to:

- explain the differences between various types of intellectual property and the legal frameworks that apply to each type
- understand the issues that arise when drawing up contracts relating to acquiring or developing software
- explore the legal frameworks relating to software systems in a specific context.

1 Why law is necessary

Computers have become embedded in society, making certain transactions between people or organisations affecting other people – what economists call ‘externalities’. Sometimes these externalities are generally positive and good, but lead to the ‘free-rider’ problem. In other cases the effects can be negative and bad – and even the seemingly beneficial free ride can also have negative effects, as when software can be easily copied (a free ride), with the consequence that invention and production ceases.

Negative effects raise questions of ethics and morality, which can be addressed by embedding ethical principles in professional codes of conduct. By formulating regulations in the form of technical standards, it is possible to help technology and people to work together more effectively.

While these voluntary approaches to counteracting negative effects work in many situations, sometimes we need the full might of the state in order to ensure that harm is not done and that society and the economy operate in the way intended. The mechanisms used by the state are the law, and law enforcement. Look at Case study 1.

Case study 1: Fonts and software in South Asia

Personal computers have been in use in South Asian countries (such as India and Pakistan) since the 1980s. While the hardware needed clearly has to be bought, the ease of copying software has meant that it’s seldom the case that software has also been bought. In the case of basic software such as operating systems this has meant a loss of revenue for major suppliers such as Microsoft, but has also meant there’s been little incentive to produce software locally. Because most computer use takes place using English, and pirated software has met local needs, the exception has been software for working in local languages – which use a variety of non-Roman scripts.

Since the 1980s and the arrival of desktop computers, various individuals have created fonts to facilitate desktop publishing in local languages. Producing such fonts may take months or even years of effort – but as soon as a font is produced it gets freely copied and distributed, and companies that assemble computers locally will typically include such fonts so as to enhance their product’s appeal. For example, in Nepal a typing tutor based on the traditional tale *The Ramayana* was commissioned by a pioneering local IT company, written by a local expert, then shamelessly copied by local distributors.

Thus fonts for local languages and software that works in those languages using those fonts have produced little income for their originators – suggesting that such work is undertaken more out of attachment to local languages than for reasons of financial return.

Only in the first decade of the 21st century was serious software for South Asian languages produced, following the adoption of open-source methods. One reason for the move to open-source has been to gain the freedom to localise in whatever language is desired, unfettered by market considerations. But the shift also tacitly recognises the realities of the market: that without intellectual-property law and its enforcement, fonts and software will effectively be public goods.

We'll look at several areas where most legislation has been created, starting with an extended account of intellectual-property law. Our treatments will necessarily be brief and focus on principles, independently of any particular legal jurisdiction and its laws, statutes and legal precedents. Many books have been written on how the law affects software and what special measures have been introduced for new problems created by software – the main sources used for this course were Edwards et al. (2000), and Holt and Newton (2004). The new problems may sometimes be made more complex when older laws, drafted before software and the internet existed, get reinterpreted for this new context.

The internet in particular has caused the law to become more international – for when crimes are committed on the internet, it is frequently not clear where, geographically, the crime has occurred.

Normally the place where a crime is committed determines the jurisdiction – the place where a particular set of laws should be applied. But, for example, when someone in North America posts information on an internet site in Asia that may be illegal somewhere in Europe, where did the alleged crime take place? There needs to be international law to cover such cases. In any particular case the advice of an appropriate specialist lawyer should always be sought.

2 Intellectual property (IP) rights

Software can be expensive to produce. A substantial piece of software such as a database management or operating system will take several hundred person-years of effort to produce, and after that a large team of engineers will be required to maintain and evolve the software. How will this be paid for?

Developments in technology have made the need to protect intellectual property even more urgent. With software and now books, music and film available digitally, replication and distribution is both easy and cheap, and the financial barriers to copying no longer apply.

When considering the general concepts of property, the difference between private property and public goods is an important distinction. Here a key issue is the economic conditions surrounding the production of goods, and whether production should be based on markets and an economic return acquired through sales of the goods. An important issue in enabling a market to function was seen to be **excludability** – people who don't pay should not be able to use the goods.

Software and electronic data are extremely easy to copy and distribute – which is sometimes beneficial, since this enlarges the community of practice for that software or information, and the community within which data can be exchanged.

One way to ensure excludability is to use technical measures, like encryption and licence codes, along with the internet to check that people are properly licensed.

The other measure in wide use is the law – a public good created to protect private goods. We shall look in detail at the use of the law based on private goods and markets. Later we shall return to consider software and information as a public good, and what is being done to use the law to protect this approach – the most common manifestation of this public goods view is the free/libre and open-source (FLOSS) movement, as you will see again below.

2.1 Motivations for IP laws

Over the past 200 years two different legal approaches have developed: **copyright**, to protect written works and music and similar, and **patents**, to protect inventions and their subsequent exploitation in manufacture. Copyright protects the expression of an idea, while patents protect the physical manifestation of that idea. Different countries may have enacted slightly different laws, but generally these kinds of laws have been thought beneficial and have been widely adopted, and have become the subject of international agreements. Activity 1 explores the different motivations for intellectual property laws.

Activity 1: Why have intellectual-property laws?

Why do people in the developed world regard intellectual property law as so important? And why might people in Asia or Africa take a different view?

Discussion

The usual Western response is to treat software and information works like other property. The idea of property rights, where the property involved is physical in nature – as with a house, motor vehicle or television set – is well established. It would generally be agreed that such objects can be owned by a person or an organisation for

their exclusive use, and that the owner is free to sell the object, or hire it out, or profit financially from it in other ways. This economic activity would be seen as a fair recompense for the labour involved in building the house or other goods or the capital outlay in purchasing the house, motor vehicle, television set, or other goods. Most people in the developed world would agree that the law should protect the owner's right to undertake this economic activity and prevent the theft of such property, but also that the law should regulate the activity – for example, to limit monopolistic and extortionate activity.

What about the fruits of creative activity – as with the composition and performance of music, the writing of a novel, the invention of some new device, or the writing of software? These intangibles are known as intellectual property – property that has resulted from the work of the intellect. Most people in the West now agree that these have tangible value that needs to be protected and regulated. The argument is that if we did not do this, people would stop producing intangibles such as these although there are a number of counterarguments to this view.

However, elsewhere in the world – in Africa and most of Asia – people might think differently. The idea of property being private might be challenged, for example some cultures may well be collectivist and wish to see goods that can be shared as public goods. In such communities we might expect open-source software to be popular, not because of its low cost but because it aligns better with cultural beliefs.

There are arguments in favour of intellectual property rights (IPR) and that all countries should enact and enforce laws to protect them. If a country did enact IPR law to protect the intellectual property of other countries, this would also protect rights of intellectual property generated within the country, helping them in export sales and also in obtaining foreign investment. Investors would want the protection of the law for the products they produce in a particular country, for without that a return on their investment would not be realised (see, for example, Zavin and Martin, 1997). In the short term there might seem to be benefits from avoiding copyright, particularly on material that would otherwise have to be imported at great cost. However, in the long term a country is likely to benefit from respecting copyright and from other countries implementing copyright so that all exports could in turn generate income.

Intellectual property has tangible value and needs the protection of the law, particularly if copying is easy and cheap. This protection needs to be international.

However, there are also strong arguments against the protection of intellectual property in specific situations. These are based on ideas of common good which should not be withheld – for example, if an invention protected by IPR could save a life, should it be withheld? To some, the protection of IPR, particularly for technology and science, by more developed societies mitigates too strongly against less developed societies. Software products may be covered by copyright and patents in some countries. However, Richard Stallman and others (see Stallman, 2002) have argued against software idea patents – now a reality in the US – and this is currently an issue of much debate.

If a software enterprise is seeking to operate internationally it is important that intellectual property issues and the different views about intellectual property in different countries be taken into account. We start by looking at international bodies and agreements, to

establish concepts and set a context within which copyright, patents, and other aspects of IPR can be described and discussed.

2.2 International cooperation on IP

There are two major forms of legal system: common law, based on argument from previous cases made by knowledgeable and powerful independent judges; and civil code (introduced by Napoleon), based on carefully formulated laws that can form bases for judgement by magistrates. The legal systems of England and the US epitomise common law, while those of France and Germany epitomise civil code. These two systems now form the basis for legal systems around the world, having been spread by the European colonial activities during the 15th to 19th centuries.

With the coming of digital media and software, and digital communication networks facilitating cross-border flows, the need for international harmonisation and agreement has become ever more pressing. Without an international authority with jurisdiction across countries, commercial parties could exploit the variations in national laws or they could attempt to flout the law altogether through the uncertainty as to where exactly an illegal copy was being held. The idea of **cyberspace** as a territory in which the law should operate has become established.

This need for international agreement led in the 19th century to the Berne Convention on copyright, and then to subsequent conventions to further elaborate and refine the Berne Convention. Other conventions addressing other aspects of intellectual property law followed. The European Union as a collaboration between countries with advanced, linked economies but different legal systems has been important in movements towards international agreements.

The next three subsections below provide a brief summary of the international agreements and organisations, with current debates and open issues highlighted.

The Berne Convention

The original Berne Convention was agreed in 1886 and focused on protecting 'Literary and Artistic Works'. The agreement was reviewed in Paris in 1896 and again in Berlin in 1908, before being ratified in Berne in 1914. A further review was held in Rome in 1928, with others in Brussels in 1948, Stockholm in 1967, and Paris in 1971. The most recent amendment was in 1979.

Countries sign up to this agreement, but may choose to implement only parts of it. So, for example, Canada signed up to the Rome version, and then moved on to the more exacting 1971 Paris version. Some 120 countries have now signed up – the US was very late in doing so, having only signed on 1 March 1989.

The Berne agreement lays down three basic principles and a minimum level of protection that its signatories must provide. The principles are that:

1. The protection given to an original work in one Berne country must also be given in all other Berne countries.
2. Protection should be automatic and not contingent upon any formalities such as marking the work as copyright using the special copyright symbol '©'.
3. The protection given in a Berne country should not depend upon that same protection existing in the country of origin.

Because many important countries (including the US and various Latin American and Asian nations) did not adopt the Berne Convention until very late, the Universal Copyright Convention (UCC) was created in 1952 to build a bridge between the copyright systems of these countries and Berne members. When the US signed up to Berne in 1989, the importance of the UCC diminished.

GATT and TRIPS

The General Agreement on Tariffs and Trade (GATT) was made after the Second World War in a bid to regulate world trade. In 1995 this agreement was replaced by provisions made by the World Trade Organization (WTO). The GATT and WTO process has involved regular negotiations – in a series of meetings called ‘rounds’ – so as to reach agreement on areas of world trade. Various rounds have addressed intellectual property rights.

The Uruguay Round of GATT (1986–94) – which led to the establishment of the WTO – developed its own view of copyright, extending the Berne Convention in significant ways. This view has now become enshrined in the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), administered by the WTO.

TRIPS introduces a most-favoured-nation (MFN) requirement on copyright, so that any one GATT/WTO member must be given as good copyright treatment as any other member. GATT-style dispute settlement and enforcement procedures are introduced. TRIPS is generally seen to favour developed rather than developing countries in increasing protection, with the only accommodation being that developing countries could take five years instead of one year to move to the TRIPS agreement.

More recent WTO meetings, notably that in Doha (Qatar) in 2001, have focused on pharmaceuticals. We anticipate that future meetings will focus on software.

WIPO

The World Intellectual Property Organization (WIPO) acts as the secretariat for the major intellectual property conventions, including the Berne Convention, and the more specialised Brussels, Geneva and Rome Conventions. WIPO’s role is to provide its members with information on and assistance with intellectual property, to ensure that international and regional agencies cooperate on intellectual property issues, and to help developing countries protect their own intellectual property and obtain developed countries’ intellectual property on favourable terms.

On 20 December 1996 the members of WIPO adopted two new treaties – the [WIPO Copyright Treaty](#) for the protection of authors, and the [WIPO Performance and Phonograms Treaty](#). The Copyright Treaty updates the Berne Convention of 1971 to cover digitisation and, in particular, the availability of work online, but no agreement on reproduction rights in this environment was reached.

At WIPO’s general assembly meeting in Geneva in September 2004 a proposal from Argentina and Brazil that economic development depends upon a freer use of intellectual property than normal IPR regulation expects was accepted. A very strong and cogent argument supporting the Argentinian and Brazilian ‘Friends of Development’ proposal was given by India – as seen in Case study 2. This important area clearly will develop over the coming decades.

Case study 2: The imbalance of IPR protection: the pharmaceuticals example

Consider the following, from Alsegård (2004).

When considering the differences between developed and developing countries in terms of IPRs, one of the most important areas has been pharmaceutical patents. On one side are the pharmaceutical companies, claiming their right to own their patents and to benefit from them with high prices, considering the high risks and costs of their research and development (R&D). On the other side are developing countries, claiming their rights to buy or manufacture existing medicines at low prices to prevent diseases and to help their people. These interests not only conflict, but it is also unclear how either one is best protected. Not everyone believes that strong IPR protection benefits the pharmaceutical industry, and weak protection is not necessarily good for the users of the drugs. Nevertheless, the general view is that the TRIPS Agreement helps the pharmaceutical industry but, with regard to medicines, makes the situation worse for many developing countries.

[...]

The general complaint made from developing countries regarding IP is that it has shifted too far in favour of producers. In the case of drugs this means that IPRs have shifted too far towards the protection of the pharmaceutical patents owners. According to the critics, IPRs are not inherent, natural rights and should not be treated as such. This debate revolves around the general issue of the monopoly and private rights granted through patents, as opposed to the public interest and social benefits deriving from science and technology. Due to this conflict, patent laws that are strong for protecting private interest are thus weak for protecting the public interest, at least initially.

The protection of intellectual property rights by law may not be in the wider social interest.

3 IP rights: copyright, patents, marks and brands

Intellectual property rights include copyright, patents, and trademarks and service marks, the latter two being of relevance to brands. First, let's look at copyright.

3.1 Copyright

Copyright has been of central importance in the field of publishing for 200 years, and now is as important in the field of software and the internet. Copyright gives the right to the 'originator [of a work], or his or her assignee, for a fixed number of years, to print, publish, perform, film, or record literary, artistic, or musical material, and to authorize others to do the same' (*Concise Oxford Dictionary*, 9th edition).

It is important to note that copyright law does not protect the ideas underlying the work, but only the expression of those ideas. This means that having examined a work, or a number of works, an author is free to create a new work through the re-expression of the ideas underlying those other works. However, this does not mean that simple re-keying of text with small changes or redrawing a diagram or re-implementation an animation is permitted.

Compilations and databases are explicitly protected as intellectual property.

When software first became an area of concern in the second half of the 20th century, copyright was used for its protection. In 1991 the European Union issued a directive requiring all member states to use copyright law for protecting software, spelling out the rights and exceptions (European Union, 1991); in 2000 it reported on the success of this initiative (European Community, 2000). Nevertheless copyright has not proved adequate (not everyone agrees here!), since it only protects the way the software is written and not the underlying algorithms; in consequence, software is increasingly being protected by patents (see next subsection). In computing, copyright is now much more important for the protection of internet websites and for documentation.

Traditionally, different kinds of artistic work have been protected by different pieces of legislation – so music has been protected separately from literature and separately from film, and so on. However, there is a move to 'convergence' as everything becomes digitised and intermixed within multimedia products. Digitisation raised new problems, with the need to protect works against new actions. Thus the treatment of all rights under the general heading of intellectual property right, or at least general copyright, is today the only reasonable way forward. Further, the ability to distribute digital material over the internet makes intellectual property rights a global problem that requires international agreement – as you saw earlier in this course.

In copyright, the author or originator of the intellectual property is given a number of legal 'rights'. These circumscribe what the owner can do and in some cases cannot do, and what other people can do with the intellectual property.

The detail of how the right is claimed and what it gives the owner of the IPR varies between legal jurisdictions. In some cases the right has to be explicitly claimed or

registered, as was the case in the US before 1989, while elsewhere, as in the UK, the very act of creating the work automatically gave the creator the rights. The move is now towards the latter, through decisions taken as part of various international agreements described earlier – the Berne Convention, the Uruguay Round of GATT and TRIPS. Even though it may not be necessary to place a copyright line on the work, it is still advisable. The actual right given is exclusive use for the lifetime of the creator plus 70 years. The US and others had previously limited rights for life plus 50 years, but shifted to life plus 70 years to match European practice as part of the process of harmonising copyright law internationally.

There are exceptions to granting of exclusive rights recognised by the law that will be covered in greater detail later. Where exceptions are made, this is to protect the public interest. What is allowed varies – for example, in the US a teacher can read from a work in the classroom but cannot distribute copies, while in the UK a researcher can make a copy of part of a work for personal use. Very limited quotation from works is accepted as ‘fair dealing’.

All other use requires reference to the copyright owner for permission, and may involve paying a fee. Finding out who rights owners are can be very complex – even a simple diagram in a text can involve more copyright owners than you might imagine. Rights can be assigned to other persons or legal entities – in fact, this is common. In some jurisdictions, such as the US, all rights can be assigned, while in others such as France some rights are inalienable, such as the ‘look-and-feel’ of an artistic work.

Copyright protects the expression of an idea, but not the idea itself.

Any breach of an intellectual property right can be viewed as theft, just as most people would consider taking someone else’s physical property to be theft. Yet the kinds of works protected by copyright laws are seen as different, and the introduction of new technologies is making breach of copyright easier.

How breaches of copyright are dealt with varies between jurisdictions. In some places, such as the US, breaches are largely handled through the civil courts using statutory damages: copyright owners group together in societies and together make random checks to see if copyright is being breached, and if it is, take joint action to recover money lost and punish the offender. In the US the music industry associations conduct some 500 lawsuits a year in a bid to enforce their members’ copyright interests (see Saffer, 1997). In other countries enforcement might be through criminal law, which is necessary to deter major and systematic infringers.

The increasing use of internet services that allow sharing of audio and video content (e.g., YouTube) has made it harder for copyright holders to keep track of how their content might be shared in breach of copyright. This has required internet service providers to develop policies and procedures to help copyright holders assert their intellectual property rights and penalise users who infringe copyright by sharing content to which they have no rights. Technological developments such as peer-to-peer file-sharing (as with, for example, BitTorrent) distribute content by putting portions of files across many computers located all over the world. Such developments make it even harder to address the problem of jurisdiction.

Copyright in the courts

Read Case study 3.

Case study 3: Copyright in the courts

Between 1970 and the present, court cases have set a variety of precedents. The following four examples, adapted from David Bainbridge's *Software Copyright Law* (Bainbridge, 2004), illustrate some of the judgements given.

1. *Digital Communications Associates v Softklone Distributing Corporation*. [659 F Supp 449 (ND Ga 1987)]

The plaintiff (DCA) designed a screen display for a communications program which showed a list of commands with the first two letters highlighted and in block capitals; the user selected a command by entering its first two letters. The defendant (SDC) developed another communications program with a similar display. The court upheld protection of the screen display, saying that the idea was the concept of such a screen (and therefore not copyrightable), and the expression (that is, the use of highlighting and capital letters, and the organisation of the command) was the means to communicate the idea (and hence was protected by copyright).

2. *Broderbund Software v Unison World*. [648 F Supp 1127 (ND Cal 1986)]

This case also concerned screen displays. In this instance, it was argued by the defendant (UW) that there was only one way to structure the screens and input, thus they were part of the idea, and not simply expression. In fact, other versions of the screens were produced as evidence, and it was ruled that the screen displays were indeed part of the expression used by BS, and thus copyrightable.

3. *Ibcos Computers Ltd v Barclays Mercantile Highland Finance Ltd (UK)*. [1994. FSR 275]

A programmer had worked on an accounts package for the plaintiff (Ibcos), and subsequently marketed a competing accounts package for the defendant (BM). Copyright was held to subsist in the individual program and in the entire software package as a compilation. This case showed that, as well as individual computer programs being protected by copyright, the way they are linked together (structured) may, in some cases, also be protected. In other words, depending on the skill and judgement involved in selecting and arranging the individual programs, copying structural and design features may infringe copyright.

4. *Lotus Development Corporation v Paperback Software International*. [740 F Supp 37 (D Mass 1990)]

This case showed that overall organisation and structure, the content and structure of commands, and the user interface (choice of words or symbols) are protected by copyright, but the judge in this case said that it does not follow automatically that every expression of an idea is protected by copyright. He listed four things that must be considered:

- originality – the expression must originate from the author
- functionality – if the expression simply embodies functional elements of an idea, it is not copyrightable
- obviousness – if the expression is inseparable from the idea, it is not protected
- merger – if the particular expression is one of a quite limited number of expressions, then it is not copyrightable.

(adapted from Bainbridge, 1994, pp. 50, 58–9, 92–3, 96–7)

There are a number of quite distinct rights, and in the following subsections you'll look at each kind of right in turn, focusing on some of the specific problems and issues raised by each right. Because this is an evolving area, particularly with regard to digitised material, it is always advisable to seek expert legal advice when considering intellectual property rights in general and copyright in particular.

Moral rights

Moral rights are concerned with the artistic integrity of the intellectual property and the right of its creator to be acknowledged. In Anglo-American law these moral rights have in the past been neglected, with emphasis placed on the economic or pecuniary rights, but this has now changed. Moral rights may be waivable, but they are never assignable.

The moral right of attribution is clear – if any authorship is to be attributed, this must be to the originator (though the originator may choose to remain anonymous). In some jurisdictions, such as France, this right is inalienable. In others it may be waived – so in the UK the originator has to positively declare this right of 'paternity', otherwise a publisher could in principle (though in fact never would) drop the author's name from the work; however, the publisher must not substitute any other person's name. When an intellectual property is created under contract, attribution may often be dropped.

It is common practice to credit computer-game developers, but this occurs less commonly in the case of software – for example, for the Eudora email package there is developer attribution, but Microsoft's policy is not to have this (though for some Microsoft products you can find the developers' names if you know how to do so – see Cooper, 1995).

The position on integrity is less clear. The most common breach of integrity occurs in television and film, where colourisation or aspect ratio may be changed. A celebrated case in Canada involved a sculpture of swans draped in red ribbons which led the sculptor, no longer the owner, to sue for damaged reputation. Again, in France this right is inalienable, while elsewhere it may be waivable. There is a strong case for waivability – for example, to handle cases where a publisher might want to edit an author's work or a film might be distributed in a range of countries in some of which particular colours might have particular cultural significance. For internet sites it might be desirable that properties such as font size and picture resolution can be changed.

Economic rights

The most fundamental economic right is that of control over reproduction of the work. When publishing a work via a third party, it is important to license the publisher to print (and distribute) the work; this is done either by assigning (transferring) copyright to the publisher, or by giving the publisher a licence to print and distribute the work as part of the publishing contract. Once a work has been printed, the publisher may assume a 'typographical right' in the printed material – generally for a shorter period than the copyright itself.

Reproduction using computers may now also cover the initial digitisation of the work, and uploading or downloading of the work.

All of these acts of reproduction may only be carried out with the permission of the owner of the copyright, who may also require the payment of some suitable fee.

The point at which people most commonly encounter copyrighting of text is in photocopying, for which in principle a licence is always required. Recovery of fees from photocopying is an important source of income for copyright holders.

The rights protected by copyright law include the moral right to be known as the author, and the right to economic benefit.

Distribution and communication of copies

The right to distribute also belongs exclusively to the owner of the intellectual property rights, and distribution and communication have a broad interpretation covering anything that enables members of the public to access the intellectual property at a time and place of their own choosing.

Thus distribution and communication includes the performance of plays, the reading of poetry, and the on-demand transmission of film and audio across communication networks. But it also includes the display of material where the public can access it, particularly on the internet.

'Communication to the public' is a new right under the Geneva Convention and is contained in the EU harmonisation directive, though it may not yet be incorporated into law. This complicated right includes concepts such as 'performance' and 'broadcasting' and is inconsistent or incomplete with regard to electronic publishing.

The exercise of the right of distribution and communication may involve, but does not require, sale or hire. It also includes the right to prohibit unauthorised distribution and communication. These rights normally cannot be 'exhausted' except by transfer of the ownership of the right to some other party. The concept of exhaustion – whereby some particular action by the owner then terminates his or her right – has existed in certain jurisdictions.

In linking from one website to another it is very easy to embed material from some other site within your site, and pass this off as part of your own site; however, to do this would be a breach of copyright.

The usual advice is to make any such links to the home page of the site being linked to. This may make the link much less useful, since you then have to find the part of the site you need, but it does avoid breaching distribution and communication rights.

Exceptions and exemptions

It is recognised that certain exceptions to owners' intellectual property rights need to exist, for various reasons: to serve the wider public interest, because of market failure, and to support the exercising of licences granted by some previous copyright holder.

It is clear what we mean by making copies of printed and other physical, creative works, and it is widely though not universally accepted that you may make single copies for purposes of research, private study, criticism and review, and reporting current events. The latter is termed 'fair dealing' in the UK and 'fair use' in the US. In such cases it would be argued that copying is in the wider public interest, since doing this facilitates education and the development of society. However, in many European countries the idea of fair dealing is not accepted and still hotly debated. Where fair dealing is referred to in national laws it tends not to be very explicit, and publishers and users have had to resort to drawing up consensus guidelines for actual day-to-day practice.

Things are even less clear with regard to copying digital works – there are no guidelines yet for the electronic environment, with really no clear agreement on what the digital equivalent of fair dealing might be.

Exceptions may be taken further in various ways. It may be permissible to make copies of audio and audio-visual materials for personal use – so-called ‘private copying’. In some jurisdictions it may even be permitted to use materials transmitted on TV for educational purposes, though normally this would require a licence. The EU directive on use of copyright for software included exemptions for making back-up copies and for limited decompilation of software at the interface to facilitate the interoperability of the software with other software. Software is usually delivered as an ‘executable’, with guidance on how to connect to this at particular points in particular ways. To be able to make this connection effectively, it may be helpful to know what the original programming language code of the software was, and particularly of those parts being connected to. This source code can be abstracted from the executable via decompilation or reverse engineering.

Libraries may also be exempt from copyright constraints in the case of particular actions such as archiving – this is called ‘library privilege’ in the UK, and is not part of fair dealing. Libraries do make extensive use of fair dealing when supplying copies of items to scholars, particularly via other libraries – in the UK this is an aspect of the interlibrary loan system. It is not clear what the equivalent of an interlibrary loan would be in the digital world, and remote delivery of library services in digital libraries would not be exempt from copyright constraints.

In many technical processes involving digitised copies, temporary intermediate copies are inevitably produced, and legislation has been proposed to exempt these. However, the making of copies for the purposes of security or back-up may not be exempt – though typically a licence would also grant this right while prohibiting the making of any other copies.

It is clearly unwise to assume an exemption exists; when in doubt you should seek a licence. In the UK the [Copyright Licensing Agency](#) can provide, for a fee, the right to use ‘extracts from print and digital publications on behalf of the copyright owners – authors, publishers and visual artists’.

Berne and TRIPS

TRIPS adopts the Berne principles and requires countries to adopt Articles 1 to 21 of the Paris 1971 protocol, with the notable exception of Article 6 on the moral rights of paternity and integrity. TRIPS extends copyright coverage to computer programs (as literary works) and to databases, and requires that a rental right is established for computer programs and for recordings.

The minimum protection required for all literary, artistic and scientific works is:

- the rights including translation, adaptations and adjustments, public performance and recital, reproduction, communication and broadcast
- moral rights of paternity and integrity
- a minimum duration of protection.

Multimedia rights

Now complete Activity 2.

Activity 2: Multimedia rights

Imagine you've been teaching mathematics for several years and have developed your own individual way to explain the key concepts of set theory, involving the students playing a game. You now decide to publish your method of teaching and the game as a multimedia product with an accompanying book. You will write the book but need to hire a developer to produce the multimedia component, to your specification. You plan to sell the combined product via a well-known publisher. What rights should you have? What rights should the multimedia developer and publisher have?

Discussion

Since the basic ideas are yours, it would seem sensible to retain these. As the employer of the multimedia developer you may well automatically own the actual multimedia software produced and the employee would gain no rights over the software – but it would be wise to spell this out in the contract of employment.

When entering into the agreement with the publisher, all you need grant are the copying and distribution rights, retaining all other rights for yourself. Standard publishers' agreements are very likely to demand assignment of copyright to the publisher, but this is not necessary and some publishers are happy not to demand this.

3.2 Patents: introduction

In contrast to copyright, patents are explicitly intended to protect ideas or inventions. In the UK patents go back to the Statute of Monopolies of 1623, while in the US the first patent law was enacted in 1790. Since then the need to protect inventions and similar creations has been recognised worldwide – first in national legislation and now in global agreements, as with GATT.

US patent legislation (United States Code Title 35, Section 101) describes the position very well:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvements thereof, may obtain a patent, subject to the conditions and requirements of this title.

USPTO (2014)

3.3 Patents and software in the EU

The following videos present excerpts from an interview with Dr Maria Fernández-Ferreira, a patent examiner at the European Patent Office, in which she discusses different aspects of patents and their applicability to software inventions. Video 1 explains what a patent is and how patents are relevant to software engineers.

Video content is not available in this format.

[Video 1 Patents and their relevance to software engineers](#)



For another excellent discussion of patents see Thomas Gordon and Arthur Cookfair's *Patent Fundamentals for Scientists and Engineers* (2000). A lot of this advice is relevant to software engineers – except that the book predates recent developments that make software patentable.

To be patentable an invention must be novel. Previously existing inventions are known as 'prior art' and would have been disclosed and made public, perhaps by means of publication or embodiment in a product or earlier patent. If novel, the invention must not be obvious 'to one of ordinary skill in the art', and though it may resemble some pre-existing invention it must contain non-obvious new features. Furthermore, the invention must be both useful and operable.

Patent laws usually circumscribe what can be patented. Historically this has constituted inventions and discoveries, human-made products, compositions of matter, and processing methods. To this have been added designs (in the sense of ornamental appearance) and, more recently, plants, following developments in genetic engineering. Software was initially explicitly excluded, as were methods of doing business, and 'mere printed matter'. However, following initiatives in the US and then in Europe, software is now becoming patentable. In the next interview excerpt, Video 2, Dr Fernández-Ferreira explains how software can be patented and how requirements differ across the world.

Video content is not available in this format.

[Video 2 Patenting software](#)



Gaining copyright requires no particular action by an author or creator – the very act of creation is sufficient, though it is advisable to include a copyright statement (as is commonly seen at the front of books). In contrast, acquiring a patent can be a lengthy and expensive procedure. However, immediate protection can be obtained by filing a provisional patent application. An alternative to filing a patent, if the cost makes the investment unacceptable, is disclosing it; this stops others patenting the same idea. It has become standard practice in many major industrial companies to have a ‘technical disclosure’ publication specifically for this purpose.

A patent is applied for by the inventor at the national patent office, following procedures and regulations laid down by national or international law. The invention needs to be specified in sufficient detail – including any appropriate drawings – that anyone in the technological area would be able to build the invention. One means of actually constructing the invention also needs to be provided. The invention’s actual novelty needs to be claimed explicitly, and this is what will be examined during the registration process. Thus, in order to establish a patent, an extensive search must be made of prior art in order to establish novelty. In the final excerpt, Video 3, Dr Fernández-Ferreira describes how the patents process works in the European Union.

Video content is not available in this format.

[Video 3 The patents process in the European Union](#)



If the application is successful a patent will be granted to the owner for a period of 20 years from date of filing. During this period the patent holder has the exclusive right to exploit the patent commercially – to make, use or sell the invention. For an overview of the patent process see the [European Patent Office website](#).

Software patents slowly became established as court rulings attempted to decide on what was and was not patentable.

3.4 Patents and software in the US

Patenting of software in the US was regularised in 1996. There are now many thousands of software patents, including the well-known GIF compression patent – the algorithm for reducing the size of images encoded in the GIF manner. But software patents remain controversial, and at the time of writing many trivial and, in the US, obvious algorithms have been given patent protection. Nevertheless, in many areas of the software industry, particularly outside the US, there is concern that access to much obvious and useful software could be prevented due to claims of patent infringement.

Now complete Activity 3.

Activity 3: America Invents Act

In 2011, US President Barack Obama signed the America Invents Act (AIA) into law. A key change resulting from this law was that the US patent system shifted from a 'first-to-invent' to a 'first-inventor-to-file' system. The change is explained in four short videos produced by the US Patent and Trademark Office. Watch the videos, then briefly explain what 'first inventor to file' means.

You can access the videos at:

- [First Inventor to File, Video #1](#)
- [First Inventor to File, Video #2](#)
- [First Inventor to File, Video #3](#)

- [First Inventor to File, Video #4](#)

You can also find them at [AIA Informational Videos](#).

Don't worry about understanding all the legal terms – focus on the explanations given. Why might the 'first-inventor-to-file' approach to granting patents be unfair to some inventors?

Provide your answer...

Discussion

Under new US law a patent will be granted only if the invention being claimed has not been made known to the public before the date on which the patent application was filed – the 'effective filing date'. As long as the claimed invention is something new and unknown to the world, the patent will be granted to the inventor who first files a patent application. It is no longer possible to file an application for an invention if there is another patent application for an invention considered to be same, that has an earlier effective filing date.

The new law raises the possibility that an inventor may not be able to get a patent on his or her invention if someone else files a patent for it first. This could happen, say, because the inventor writes an article about his or her invention before applying for a patent, which prompts someone else to develop the invention and patent it. However, the new law addresses this issue by specifying a 'grace period' that allows up to one year between publication of the invention and the filing of the patent application.

Patents protect ideas themselves, and are now applicable to software. This is controversial.

3.5 Trade marks, service marks and brands

Brands have become an important aspect of commercial activity, being used to identify and represent the quality of a product or service. International brands such as Nike™ and Coca-Cola® are instantly recognisable and attract customers. Trademarks are indicated by the ™ superscript, and registered trademarks by the ® symbol.

Brands are recognised in law as 'marks', for which special protection is given. According to the US Patent and Trademark Office:

A trademark includes any word, name, symbol, or device, or any combination, used, or intended to be used, in commerce to identify and distinguish the goods of one manufacturer or seller from goods manufactured or sold by others, and to indicate the source of the goods. In short, a trademark is a brand name.

USPTO (2013)

This definition clearly identifies trademarks with brands.

Service marks are like trademarks, but identify and distinguish the services of a particular provider. The US also recognises two further marks: collective marks for societies, and certification marks to indicate that products conform to particular standards.

International agreement on trademarks was reached in April 2002 under the Madrid Protocol, managed by WIPO. The US contracted into this treaty in November 2003.

Brands and their associated marks need to be managed, through advertising and refreshing them by means of suitable changes. All this makes sense commercially, but is also necessary from the trademark perspective. For a trademark to remain protected it needs to be maintained and in active use, otherwise some other body will become authorised to use it.

Now complete Activity 4.

Activity 4: Patents, trademarks and market distortion

To what extent does using patents and trademarks distort the market?

Provide your answer...

Discussion

Patents actually are intended to distort the market, creating a monopoly for the patent's owner for the life of that patent. This means the price of any goods based on the patent might be inflated, but the counterargument is that this might be necessary to recover the costs of developing the product and patent, and to support research that will lead to more inventions for future exploitation. Once the patent has lapsed the market could revert to its normal competitive state.

People don't buy goods solely on the basis of price; quality and trust are also important, and brands and trademarks support this. So overall, trademarks help the market rather than distort it.

4 IP rights: Common and public goods

An alternative approach to the one described in the previous section – based on private property and market forces, with protection in the form of both copyrights and patents – is that software and information should be viewed as public goods and be freely available. You saw how this works in general economic terms, but how does it work out legally?

The idea would be to freely distribute software for anyone's use, with no requirement to pay fees and no constraints on what the software can be used for. However, this free distribution would be taking place in an environment in which software copyright and patents are already established and in active use. The free distribution of software could still run into problems as people attempted to take ownership of that software as private property and used the law to give themselves exclusive rights to the intellectual property. Thus it has become common practice to use intellectual property law to protect 'free software', which is software as a public good. This turns out to be desirable anyway, since there may be some basic rights, like moral rights, that you would always want to protect – so that for those jurisdictions that do not treat such rights as inalienable, these rights have to be respected anyway. These protections are set out in standard licensing agreements, of which two are in increasingly widespread use within the free and open-source movement.

- The GNU General Public License and the Free Documentation License were established by the Free Software Foundation for software and documentation respectively. The intention is to ensure everyone is free to copy and redistribute the work with or without modification and commercially or non-commercially, while crediting the original authors without making them responsible for any modifications. These are the original public goods licences, though they have evolved over the years. These licences contain a number of specific stipulations that must be adhered to. For more on GNU licenses, see [The GNU Operating System](#).
- The Creative Commons License for a copyrighted work is somewhat less restrictive than the GNU licences, but it is gaining considerable popularity. This licence enables you to reproduce and distribute the work, incorporate the work into a larger collection, and create and reproduce and distribute derivative works. This can be done in any medium. The Creative Commons License must be passed on to recipients of the distributed work, without any further imposed conditions. The original copyright notice must be passed on intact, in particular to identify the original creator of the work. The distribution of a work should not be one primarily for commercial gain, and where such gain is made the licensor retains the right to collect royalties. For more on this topic see the [Creative Commons Legal Code](#).

Software as public goods can be protected by intellectual property law.

The use of GNU and Creative Commons licences has been a source of dispute between the commercial software development industry and the open-source movement. It has been claimed that the conditions laid down are infringements of human rights. The debate over public goods led to interest in the United Nations, where it is believed that many services, including education and the use of the internet, should be viewed as public goods. This will clearly be an area of change and growth in the decades ahead.

Fortunately you will be able to track those changes via the internet, where so much valuable information is posted as a public good.

5 Contracts

Contracts are very frequently entered into as part of software management – for example, as an aspect of employing personnel and hiring consultants, purchasing hardware and software, software development, and hardware and software maintenance. Contracts are agreements between two or more parties that are legally binding. If one of the parties should fail to fulfil its agreement then the other party can obtain redress through the courts. The central importance of contracting in computing can be seen in the British Computer Society monograph *A Manager's Guide to IT Law* (Holt and Newton, 2004), which devotes more than half its pages to contracting issues. It gives much useful, detailed guidance, with the central message being: when in doubt, seek expert legal advice.

The contract needs to set out what the parties to the contract will do and when they will do it. Typically this involves payment of money in return for supply of goods and services. We need to make sure that our contracts are well formulated so that we do not find ourselves in difficulty later; some of the issues that need to be addressed in any contract are described below.

The goods to be supplied might be computer and communications hardware as part of some major development of the IT infrastructure of your organisation. In such a case it would be normal to specify delivery dates, and include procedures for commissioning and acceptance of the new equipment. The supplier might depend upon us to ready our premises for receipt of the new hardware systems. Alternatively the goods might take the form of software, from off-the-shelf products to bespoke development. Software which involves customisation of some pre-existing software or the bespoke development of other, new software is notoriously difficult to specify precisely enough for a simple contract to suffice.

At the time of writing there has been a shift towards supplying computing systems as services that encompass both hardware and software – responding to a organisational need. Collectively known as **cloud computing**, these services range from:

- computing infrastructure as a service (IaaS), which provides networked computers and data storage that be configured as needed.
- platform as a service (PaaS), which provides configured computing platforms such as web servers or database systems for the client organisation
- software as a service (SaaS), which provides software such as distributed office productivity applications (e.g., Google Docs) or file-sharing systems (e.g., Dropbox).

In such cases it may be easier to set out what must be delivered and to identify failures under the contract, using key performance metrics that relate qualities such as availability, performance and security of the service.

5.1 Breach of contract

There have been cases of failure to deliver systems that have led to lawsuits over breach of contract – as exemplified in Case study 4.

Case study 4: Breach of contract

PeopleSoft charged with contract breach

By Alorie Gilbert, Staff Writer, CNET News.com

The state of Ohio has charged PeopleSoft and its consulting partner with fraud and breach of contract for their role in a software project at Cleveland State University.

The attorney general of Ohio, who filed suit Jan. 30 in Ohio state court, seeks combined compensatory and punitive damages in excess of \$130 million.

The suit alleges that PeopleSoft, based in Pleasanton, Calif., misrepresented the capabilities of its software and failed to provide promised features as the university embarked on a revamp of its student administration systems in 1996.

It also charges Kaludis Consulting Group, the Washington-based consulting firm the university hired to help install PeopleSoft's systems, with failing to fulfil its contractual duties.

In the suit, the university said certain features of PeopleSoft programs were 'little more than vaporware' and that the programs had trouble administering student financial aid, keeping student records in synch and running properly on the IBM DB/2 database.

PeopleSoft did not immediately respond to a request for comment.

PeopleSoft was the target of a similar suit several years ago, brought by textile manufacturer W. L. Gore. Yet suits brought by customers against PeopleSoft and competitors, including Lawson Software, Oracle and SAP, are increasingly uncommon.

A court date for the Ohio case has not yet been scheduled.

Gilbert (2004)

5.2 Contract analysis

When hardware is supplied it is usual for the purchaser to be the owner of that hardware, as with any other physical property. However when software is supplied the property rights to it may not be bought, merely licensed, with ownership remaining with the supplier or whatever other party supplied the software. Only in the case of bespoke development might the intellectual property become the purchaser's, though even then the agreement might entitle the supplier to further develop the software and sell it to other clients where this does not lead to loss of competitive advantage for the original purchaser. The details need to be spelled out in the contract.

Software or hardware would normally be given a warranty during the period of which any defect identified after delivery would be remedied free of charge. In the case of hardware the warranty period may be one year, but for software it may be significantly shorter. A

warranty period of just three months is far too short a time for many defects to have arisen (such as those related to large volumes of data that build up only over several years), let alone to be demonstrated unambiguously. Software supply contracts would usually be followed by maintenance contracts.

In any case involving the supply of goods or services there always is the danger that the supplier goes out of business, and the contract should include clauses about what would happen then. In the case of the supply of software – especially where this involves continued maintenance – or of licensing a useful fallback position would be to have access to the software's source code so that alternative developers and maintainers could be found. This can be arranged through an **escrow agreement**, whereby it is agreed that a copy of the source code will be held by some third party – perhaps a bank – and be released to you should certain conditions arise, such as bankruptcy of the supplier. The escrow clause would normally also require that the supplier place new releases in escrow so that the latest copy is always available should the need arise.

Payment for products or services under a contract are typically staged so that some initial payment is made, and followed by further payments at key **milestones** in the project, such as delivery of hardware and then its commissioning or, for software, at the time of agreement of functional requirements or of delivery of software into alpha trials. Payments may be for time and materials, covering costs, perhaps with a small allowance for profit in a 'cost-plus' contract. However, in order to avoid cost escalation the contract may specify a fixed or maximum acceptable cost as a 'limit of liability'. With fixed cost the supplier takes most of the risk relating to time or cost overruns, whereas with maximum acceptable costs the customer takes some of this risk, up to the 'limit of liability', with the supplier assuming the risk for any cost overruns beyond this limit.

Other standard clauses may also need to be included in the contract. You may need to declare that the only agreements in force are those in the contract – that the contract constitutes the **entire agreement**. Some things can go wrong for which the parties to the contract cannot be held responsible, such as flooding destroying the supplier's premises – a case of '**force majeure**' – and what happens in such a case needs to be covered in the contract. If dispute should ensue it is important to declare which legal system should apply – the **jurisdiction** for any settlement of a dispute. In some cases it might be appropriate to include a **restraint on trade** following the contract – for example, to prevent a supplier or employee working for a rival company for a specified number of years.

Because setting up a contract may take a considerable time, and work typically needs to start immediately, it is common practice for a purchaser of goods or services to issue a **letter of intent**, indicating that a contract will be issued but work can begin beforehand. However, it is important to make such work **subject to contract**, so that when the contract has been agreed and signed, this is the only document that counts.

Prior to the **letting of a contract** there is likely to have been a tendering stage, during which potential suppliers responding to the tender may have invested a considerable sum – perhaps as much as 10 per cent of the contract value – developing partial solutions to the requirements of the contract. It is important that if you are tendering you take steps to protect this investment – it has been known for designs proposed by one tenderer to be given to another tenderer for implementation in the contract, with the creator of the designs receiving no recompense.

Now complete Activity 5.

Activity 5: Contract analysis

Take any one of the contracts for supply of software or software-related services listed at [Red Hat Agreements](#), and analyse it in terms of the issues described above. Does your chosen example grant unreasonable powers of termination to the supplier? Is the purchaser of the software protected should the supplier go out of business?

Discussion

You can see some of the standard contract elements in the examples we have given in the case studies above. If you can, get hold of the complete contracts – you will find clauses about jurisdiction and entire agreement, and about termination of the contract from the supplier's end. However, you may not find any escrow protection or favourable clauses for termination by your side.

Contracts need to be carefully drawn up to protect the interests of all parties across a range of contingencies.

6 Responsibilities to employees and the public

In carrying out activities using IT, organisations have a responsibility of care towards their employee and customers, and the general public. While these responsibilities would be clear on the grounds of ethical argument, some aspects of them have been cast into law. Whenever any organisation sets out and gathers information about people, steps must be taken to ensure that, firstly, the information really is needed for a valid purpose, and then that if any information is collected, it's correct and is used appropriately. Data-protection legislation enacted in many jurisdictions requires all this, and, more generally, laws of libel and defamation aim to prevent the promulgation of false information. The use of computers can lead to physical injury for users, and legislation on health-and-safety aspects of working environments could apply.

6.1 Data protection legislation

Organisations have always retained a certain amount of information about people in their manual filing systems – for example, records relating to employees, customers, students or hospital patients. This information could be misused – for example, being passed to others who have no right to such information, as with the unauthorised passing of a patient's medical history to an insurance company that is considering insuring that individual's life. However, such misuses were historically limited in their scope by the limitations of manual filing technologies; focused legal measures and codes of practice usually sufficed to protect such data.

The arrival of information technologies changed this completely. IT enables much more rapid searching and collating of data, and transmission of such data around the world. Concerns over such issues led to the enacting of data protection legislation – in the UK first in 1984, with later updates. Similar laws now pertain in many jurisdictions; all embody essentially the same principles.

6.2 Data protection law in the UK

Case study 5 quotes the principles of the EU's General Data Protection Regulation (GDPR), which are included in the UK's data protection law of 2018.

Case study 5: The UK Data Protection Act 2018

This Act replaces earlier data protection legislation to make UK law align to the requirements of the EU's General Data Protection Regulation (GDPR). The essence of this act is encapsulated in a set of principles, that are derived from Article 5(1) of the GDPR, quoted below.

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Additionally, as specified in Article 5(2) of the GDPR, there is a seventh principle that requires data controllers to be responsible for, and be able to demonstrate compliance with, the first six principles.

Information Commissioner's Office (2018)

These principles are set out in the Act, together with guidance for interpreting key terms such as what is meant by 'personal data' and 'sensitive processing'. For example, while any data that is linked to an individual in an identifiable way is considered 'personal data', information that may reveal details of an individual that have the potential to affect their fundamental rights or freedoms (e.g., religion, political affiliation, trade union membership) is considered 'sensitive' and need to be processed more carefully. For more details on what is considered 'personal', see the UK Information Commissioner's guidance on ['What is personal data?'](#)

Starting from these principles, GDPR also establishes a number of rights for individuals in relation to the collection and processing of their data:

1. The right to be informed: this relates to the transparency principle and means that individuals need to be told about how their personal data is collected and processed. There is an expectation that this information will be provided in a clear, concise and accessible format.

2. The right of access: which means people can make a request to find out what personal data is being held by an organisation. This is also called a 'Subject Access Request'. Organisations must provide this information in less than a month and should in most cases do this free of charge.
3. The right to rectification: individuals can ask for any errors in information held about them to be corrected on request and organisations are expected to respond promptly, within one calendar month.
4. The right to erasure: sometimes called 'the right to be forgotten', this allows individuals to request that data about them should be deleted by an organisation. However, this is not an absolute right and organisations are not required to comply with requests where there is a legitimate requirement to collect or process data, for example where the data is part of the evidence in a legal claim.
5. The right to restrict processing: this allows individuals to ask organisations to limit the ways in which their personal data is used.
6. The right to data portability: aims to enable individuals to access their data for their own use, or to move it to a different IT system. There needs to be measures for appropriate confidentiality, integrity and availability requirements to be satisfied when data is moved under this right.
7. The right to object: allows individuals to ask organisations to stop processing their data. This gives people the absolute right to stop their data being used for direct marketing and some, more limited grounds for objecting to other uses of their data, such as for research purposes.
8. Rights in relation to automated decision making and profiling: relate to how organisations might use data processing algorithms to make automatic decisions in relation to an individual, for example where a computer system decides whether to grant someone a loan.

GDPR protects EU citizens from abuses of data privacy by companies based in their own country as well as those based in member states. Additionally, any company wishing to process personal data of EU citizens, no matter where they are based in the world, will be obligated to obey GDPR. Under GDPR, each country will have its own Statutory Authority (SA) to oversee data protection, which in the UK will be the Information Commissioner's Office (ICO). GDPR increases the responsibility of companies to ensure personal data is protected at all times. GDPR requires all organisations employing more than 250 people to have at least one Data Protection Officer (DPO) responsible for developing that organisation's data protection policies and ensuring that it is compliant with GDPR. This represents a major change from the 1998 Data Protection Act which did not require organisations to employ DPOs.

With the principles of GDPR included in the UK's 2018 Data Protection Act, they will continue to be important requirements for systems that collect and process UK citizen's data. It is also important to note that the Act is not limited to enacting the provisions of the GDPR and that it includes aspects for data collection and processing which fall under UK national jurisdiction – such as those relating to immigration and law enforcement.

Data collected and processed by computer systems should be accurate and appropriate, kept secure, and only used for the purposes for which they were gathered.

6.3 Libel and defamation

In any case where material refers to people and/or organisations, it may be that any material published may give offence and lead to other people holding the people or organisations referred to in low esteem. If what is portrayed is not capable of defence in a court of law, severe damages may result.

When material is thought to be sensitive – as for example in material about disasters, where blame surrounding them is attributed – publishers will necessarily go to great lengths to ensure that they themselves will not be liable for damages. Some publishers, in their agreements with authors, will deflect responsibility onto the author, just as they will deflect onto the author responsibility for copyright clearances.

6.4 Product liability and negligence

When the use of a piece of physical machinery results in harm of some kind, most people would consider it reasonable that anyone suffering that harm should be able to seek redress from the manufacturers and suppliers of that machinery. In particular, in cases where machinery is faulty due to negligence on the part of manufacturers or suppliers, the case would seem clear. However, losses resulting from ‘faulty’ goods may not necessarily result directly from failure of the machinery.

It could be argued that published material – involving no physical machinery – could also lead to damages, with consequences for which the author and publisher of the material could be held responsible. For example, an academic paper about software viruses might include sufficient information about the construction of viruses to enable someone to construct one for themselves. If someone did construct a virus using the information in the academic paper, and damaged someone else’s software as a result, it could be claimed that the author and publisher were liable.

In 1985 the European Community passed a directive (EC, 1985) on the strict liability for defective products regardless of whether or not this arose from negligence – so that anyone in the supply chain could be sued. When this directive was first promulgated the UK software industry protested and petitioned the UK government to make software exempt. When the UK law to embody this directive was enacted, software was not made explicitly exempt, but ‘product’ was defined in such a way that it is not clear whether or not software was included. The difficulty with software is its ‘floodgate risk’: if faulty, it can lead to unlimited liability through its widespread use.

6.5 Limiting liability

Even though there are doubts about the applicability to software of negligence laws, suppliers do often attempt to limit their liability through clauses in their contracts of supply. These clauses may themselves be unlawful and thus void, but it would be unwise to rely on this when accepting such exclusion clauses. Case Study 6 presents an example of how a company might limit its liability through the use of an exclusion clause.

Case study 6: Example of a liability exclusion clause from a website

Terms, conditions, and notices

The information, software, products, and services published on this website may include inaccuracies or typographical errors. In particular, Expedia, Inc. and its affiliates do not guarantee the accuracy of, and disclaim liability for inaccuracies relating to the information and description of the hotel, air, cruise, car and other travel products displayed on this website (including, without limitation, photographs, list of hotel amenities, general product descriptions, etc.), much of which information is provided by the respective suppliers. Any hotel ratings displayed on this website are intended as only general guidelines, and Expedia, Inc. and its affiliates do not guarantee the accuracy of the ratings. Changes are periodically added to the information herein. Expedia, Inc., its affiliates and/or their respective suppliers may make improvements and/or changes on this website at any time.

Expedia, Inc. and/or its respective suppliers make no representations about the suitability of the information, software, products, and services contained on this website for any purpose and the inclusion or offering for sale of any products or services on this website does not constitute any endorsement or recommendation of such products or services by Expedia, Inc. or its affiliates. Expedia, Inc. shall use reasonable care and skill in carrying out the services contained in this website.

Expedia, Inc., its affiliates, and/or its respective suppliers hereby disclaim all warranties, terms and conditions with regard to this information, software, products, and services, including all implied warranties, and conditions, of suitable quality, fitness for a particular purpose, title, and noninfringement.

The carriers, hotels and other suppliers providing travel or other services for Expedia, Inc. are independent contractors and not agents or employees of Expedia, Inc. or its affiliates. Expedia, Inc. and its affiliates are not liable for the acts, errors, omissions, representations, warranties, breaches or negligence of any such suppliers or for any personal injuries, death, property damage, or other damages or expenses resulting therefrom. Expedia, Inc. and its affiliates have no liability and will make no refund in the event of any delay, cancellation, overbooking, strike, force majeure or other causes beyond their direct control, and they have no responsibility for any additional expense, omissions, delays, re-routing or acts of any government or authority. In no event shall Expedia, Inc., its affiliates and/or their suppliers be liable for any, indirect, incidental, punitive, special, or consequential damages arising out of or in any way connected with the use of this website or with the delay or inability to use this website, or for any information, software, products, and services obtained through this website, or otherwise arising out of the use of this website (including, but not limited to loss of use, data, profits, savings or opportunities), whether based on contract, tort, strict liability or otherwise, even if Expedia, Inc., its affiliates, and/or any of their suppliers have been advised of the possibility of damages. Except in relation to liability for death or personal injury for which no limit applies. Expedia, Inc., its affiliates and/or its respective suppliers shall be liable for direct loss

arising out of the use of this website, whether based on contract, tort, strict liability or otherwise, up to a maximum of the total value of the transaction under which the claim arises for any one event or series of connected events. This does not affect your statutory rights as a consumer.

Important: these terms and conditions and foregoing liability disclaimer do not affect mandatory legal rights that cannot be excluded under applicable law (including your statutory rights under any applicable national or local legislation implementing the EC package travel directive (90/314/eec) as amended from time to time). Should you decide to purchase any travel packages on this website, separate holiday terms and conditions will also apply.

Expedia, Inc. (2014)

These types of statement are periodically revised by organisations.

Software and the digital content it stores can cause harm – harm for which anyone in the supply chain could be held liable.

6.6 Health and safety

The working environment can affect productivity in different ways. For example, the act of observing workers can change performance, as can the effect of legal constraints on the working environment. These constraints will differ considerably between jurisdictions and will relate to office space allocated, temperature and humidity, air quality, and perhaps layout of equipment.

In Western countries during the period of industrialisation, health-and-safety legislation played an important role in helping to stop unscrupulous employers exploiting their workers. Today, with modern office work accommodated within clean and safe working environments, could there be any problem? There are straightforward new health problems, such as Legionnaire's disease lurking in air-conditioning plants – but also, modern office equipment and computers have created their own concerns. Could prolonged attention to a screen or use of a keyboard and mouse lead to problems?

6.7 Best practice in health-and-safety regulations

Physical problems such as RSI (repetitive strain injury) have been attributed to prolonged computer use. Concerned about this, the European Union decided to act to require employers to follow best industrial practice. In May 1990 the EU issued a directive on display screen equipment (European Union, 1990), detailed in Case study 7. This provides an example of how good practice might be brought into regulations. If a worker suffered ill-health and it was found that laws relating to health and safety at work had been flouted, the worker would have a case for compensation.

Case study 7: European directive on display screen equipment

The substance of this directive is the employer's obligations, covered in Articles 3 to 9 and quoted below.

Article 3: Analysis of workstations

1. Employers shall be obliged to perform an analysis of workstations in order to evaluate the safety and health conditions to which they give rise for their workers, particularly as regards possible risks to eyesight, physical problems and problems of mental stress.
2. Employers shall take appropriate measures to remedy the risks found, on the basis of the evaluation referred to in paragraph 1, taking account of the additional and/or combined effects of the risks so found.

Article 4: Workstations put into service for the first time

Employers must take the appropriate steps to ensure that workstations first put into service after 31 December 1992 meet the minimum requirements laid down in the Annex.

Article 5: Workstations already put into service

Employers must take the appropriate steps to ensure that workstations already put into service on or before 31 December 1992 are adapted to comply with the minimum requirements laid down in the Annex not later than four years after that date.

Article 6: Information for, and training of, workers

1. Without prejudice to Article 10 of Directive 89/391/EEC, workers shall receive information on all aspects of safety and health relating to their workstation, in particular information on such measures applicable to workstations as are implemented under Articles 3, 7 and 9.
In all cases, workers or their representatives shall be informed of any health and safety measure taken in compliance with this Directive.
2. Without prejudice to Article 12 of Directive 89/391/EEC, every worker shall also receive training in use of the workstation before commencing this type of work and whenever the organization of the workstation is substantially modified.

Article 7: Daily work routine

The employer must plan the worker's activities in such a way that daily work on a display screen is periodically interrupted by breaks or changes of activity reducing the workload at the display screen.

Article 8: Worker consultation and participation

Consultation and participation of workers and/or their representatives shall take place in accordance with Article 11 of Directive 89/391/EEC on the matters covered by this Directive, including its Annex.

Article 9: Protection of workers' eyes and eyesight

1. Workers shall be entitled to an appropriate eye and eyesight test carried out by a person with the necessary capabilities:
 - before commencing display screen work
 - at regular intervals thereafter, and
 - if they experience visual difficulties which may be due to display screen work.
2. Workers shall be entitled to an ophthalmological examination if the results of the test referred to in paragraph 1 show that this is necessary.
3. If the results of the test referred to in paragraph 1 or of the examination referred to in paragraph 2 show that it is necessary and if normal corrective appliances cannot be used, workers must be provided with special corrective appliances appropriate for the work concerned.
4. Measures taken pursuant to this Article may in no circumstances involve workers in additional financial cost.
5. Protection of workers' eyes and eyesight may be provided as part of a national health system.

European Union (1990)

This directive makes good sense, and European national governments have absorbed this directive into their own laws and issued guidance – see, for example, the website of the UK's [Health and Safety Executive](#).

The act of using computers and software in the workplace could also do users harm, and needs regulation.

7 External threats

The law can also be useful to us in protecting us from people outside our own organisation – or indeed from people within our own organisation acting against our interests. Because information and communications technologies (ICTs) are relatively new, laws have only recently been introduced and are still evolving.

You saw how copyright and patent laws could protect us – although it would be up to us to detect infringements and to take any legal action in the civil courts.

ICTs have brought new threats for ourselves and for our organisations. We need the protection of the law, and old laws have had to be reinterpreted for this new technology, with a range of new crimes having to be recognised and legislated against.

Computers can be used for communication among criminals or terrorists, and these messages can be made secret through encryption. This prospect has proved so threatening that some countries – notably, France – prohibit the use of encryption in any communication. Other countries – notably the US – prohibit the export of any foolproof encryption technology. Any encrypted message could, in principle, be decoded by a powerful enough computer given enough time, and in the latter example the intention has been to permit only encryptions that the security forces in the US could break. However, this is all rather futile, since any enemy would in time produce its own secure methods of encryption, and any encryption method that is today breakable by the US Pentagon but not by anyone else will soon be able to be broken by everyone as personal computers become ever more powerful.

This communication issue is one of a class of older crimes simply conducted by newer means. We shall ignore those examples and focus on the newer crimes peculiar to computing – so computer-aided fraud, as when someone siphons money from an employer, will not be addressed further. However, in many cases attempts to reinterpret old laws, such as those for theft, in the new context, have failed. Theft involves the removal of some physical property, and simply accessing information without changing or removing anything may not be interpretable as theft. Examples of such access might include hacking into a person's mailbox and reading what is there, or hacking into a university's file systems and copying an exam paper.

7.1 Legislation on misuse

The problems with the applicability of previously existing legislation led new laws being formulated that focus entirely on computers and communications and information.

What malevolent acts could people commit using computers and communications? The cases that do occur are often encountered in the news media – for example, cases of people breaking into private networks using the facilities of the internet and other networks, or of propagating computer viruses. While these acts may often simply be intended to display the prowess of the perpetrator, they can be used with malevolent and criminal intent – for example, viruses can send personal financial information to external agents. The outcome has been to make unauthorised access to computer-based information or software illegal. This has been enacted in many different countries under the title of 'hacking' or 'computer misuse', as seen in Case study 8.

Case study 8 The Singapore Computer Misuse Act

The Singapore government enacted the Computer Misuse Act in 1993, and amended it in 1998. Part II of the original act listed the following offences:

1. Unauthorised access to computer material.
2. Access with intent to commit or facilitate commission of offence.
3. Unauthorised modification of computer material.
4. Unauthorised use or interception of computer service.
5. Unauthorised obstruction of use of computer.
6. Unauthorised disclosure of access code.
7. Preparation for or furthering of an offence.

Singapore Government (2007)

Computer misuse acts have been strongly criticised for being technically inept – making them over-restrictive, given current security technologies – and for threatening to infringe human rights.

Harm may be caused deliberately, and acts which cause deliberate harm should be criminal offences.

7.2 Virus propagation as misuse

Complete Activity 6.

Activity 6: Computer viruses and spyware

A recurrent fear with computer installations connected to the internet is that of computers sending private information to outsiders using computer viruses or internet 'cookies'. If a computer virus infected your computer, and then broadcast personal information about other people which you happened to store on your computer for perfectly legitimate reasons, what areas of law would apply?

Discussion

There's clearly a data protection issue here, and while you did not misuse the data, you could be deemed not to have kept the data secure enough. The person who sent the virus is also guilty of computer misuse, and could be charged if he or she were caught.

Conclusion

In this course you saw how the state regulates the use of software in the interests of the wider community. However, this legal regulation does not always have wide support, and in discussion of these laws you encountered a number of issues. This area of law will continue to evolve in the years ahead.

We made the following points:

1. Intellectual property in the form of software and digital content needs the protection of the law because copying such material is easy and cheap.
2. Protection of property rights by law may not always be in the wider social interest, and some development is necessary here, particularly with a view to helping developing nations.
3. Copyright law protects the expression of an idea but not the idea itself; the rights protected by copyright law include the moral right to be known as the author, and the right to economic benefit.
4. Patents protect ideas themselves and are now applicable to software, although this is controversial.
5. Software, as public goods, can be protected using intellectual property law.
6. Contracts need to be carefully drawn up to protect the interests of all parties against a range of contingencies.
7. Data stored in computer systems should be accurate and appropriate and used only for the purposes for which it was gathered.
8. Software and the digital content it stores can cause harm for which anyone in the supply chain could be held liable.
9. The workplace in which computers and software are used needs regulation to protect those who use the computers.
10. Harm may be caused deliberately, and acts which cause deliberate harm should be treated as criminal offences.

When acquiring, developing and deploying software and computer systems, all these legal matters must be taken into account and expert legal advice should be sought.

Glossary

cloud computing

Storage of and access to data residing on a site which is part of the internet.

copyright

The legal protection of the expression of ideas in written works, drawings, music and similar, but not protection of the ideas themselves.

cyberspace

The online world of networked computer systems – especially the internet.

entire agreement

A legal phrase denoting the restriction of a contractual agreement solely to what is in the contractual document concerned.

escrow agreement

An arrangement for a copy of source code to be held by some third party – perhaps a bank – to be released should certain conditions arise, such as the supplier going bankrupt.

excludability

Usage of a good by one person such that it immediately denies use of the same good to another person.

force majeure

Used to describe the circumstances under which a contract fails but for reasons for which the parties to the contract cannot be held responsible.

jurisdiction

The legal system and set of laws that apply to a particular contract.

letter of intent

A letter stating that a contract is to be drawn up, thus enabling work to start in anticipation of the contract.

letting of a contract

The act of awarding a contract.

milestone

A key event within a project plan, typically entailing the completion of a specific deliverable by a specific date.

patent

A legal mechanism to protect an invention and its subsequent economic exploitation in manufacture, protecting the idea itself and not just its expression.

restraint on trade

A clause in a contract that is intended to restrict what one of the signatories can do either during or after the period of the contract in order to protect the interests of the other parties.

subject to contract

The specification, set out by a clause in a letter of intent, that commitments in that letter will be legally enforceable only if the contract is duly prepared and agreed, and signed.

References

Alsegård, E. (2004) 'Global pharmaceutical patents after the Doha Declaration: what lies in the future?', *1:1 SCRIPTed*, 12 [online], available at www.law.ed.ac.uk/ahrc/script-ed/docs/doha.asp (accessed 11 February 2014).

Bainbridge, D. (2004) *Software Copyright Law*, 4th edn, London, Butterworth.

Cooper, A. (1995) *About Face: the Essentials of User Interface Design*, Foster City, CA, IDG Books.

Edwards, C., Savage, N. and Walden, I. (eds) (2000) *Information Technology and the Law*, 2nd edn, London, Macmillan.

European Community (1985) 'Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' [online], *Official Journal of the European Union*, vol. L210, pp. 29–33. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0374:EN:HTML> (accessed 6 May 2014).

European Community (2000) *Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the Implementation and Effects of Directive 91/250/EEC on the Legal Protection of Computer Programs* [online]. Available at <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52000DC0199> (accessed 6 May 2014).

European Union (1990) 'Council Directive 90/270/EEC of 29 May 1990 on the minimum safety and health requirements for work with display screen equipment', *Official Journal of the European Communities*, vol. 156, no. 14, pp. 14–18. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1990L0270:20070627:EN:HTML> (accessed 7 February 2014).

European Union (1991) 'Legal protection of computer programs: Council Directive 91/250/EEC of 14 May 1991', *Official Journal of the European Communities*, vol. 122, pp. 42–6. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML> (accessed 7 February 2014).

Expedia, Inc. (2014) 'Terms, conditions, and notices', *Expedia.co.uk* [online], www.expedia.co.uk/daily/service/legal.asp (accessed 7 February 2014).

Gilbert, A. (2004) 'PeopleSoft charged with contract breach', *CNET News* [online], 30 March. Available at http://news.cnet.com/2100-2513_3-5182213.html (accessed 7 February 2014).

Gordon, T. and Cookfair, A. (2000) *Patent Fundamentals for Scientists and Engineers*, Boca Raton, FL, CRC Press.

Holt, J. and Newton, J. (eds) (2004) *A Manager's Guide to IT Law*, Swindon, British Computer Society.

Information Commissioner's Office (2018), 'The Guide to the General Data Protection Regulation' *The Guide to the General Data Protection Regulation* [online]. Available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/> (accessed 11 June 2018).

Saffer, J. (1997) *Copyright and Performing Rights Societies in the United States of America*, New York, Broadcast Music Inc.

Singapore Government (2007) *Computer Misuse and Cybersecurity Act* [online]. Available at <http://statutes.agc.gov.sg/aol/search/display/view.w3p?page=0;query=DocId%3A8a3534de-991c-4e0e-88c5-4ffa712e72af%20Depth%3A0%20ValidTime%3A09%2F04%2F2013%20TransactionTime%3A09%2F04%2F2013%20Status%3Ainforce;rec=0/> (accessed 6 May 2014).

Stallman, R. (2002) *Free Software, Free Society: Selected Essays of Richard M. Stallman*, New York, GNU Press/Free Software Foundation.

Thompson, D. (1995) *Concise Oxford Dictionary*, 9th edn, Oxford, Clarendon Press.

USPTO (2013) *The United States Patent and Trademark Office* [online]. Available at www.uspto.gov/main/trademarks.htm (accessed 7 February 2014).

USPTO (2014) *Appendix L: Patent Laws. United States Code Title 35: Patents* [online]. Available at www.uspto.gov/web/offices/pac/mpep/mpep-9015-appx-l.html (accessed 6 May 2014).

Zavin, J. and Martin, S. (1997) 'The value of intellectual property rights enforcement in developing countries', *Economic Perspective: An Electronic Journal of the US Information Agency*, vol. 2, no. 3, p. 13.

Acknowledgements

This free course was written by Arosha Bandara.

Except for third party materials and otherwise stated (see [terms and conditions](#)), this content is made available under a

[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence](#).

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this free course:

Images

Course image: ollo / E+ / Getty Images.

Text

Case study 3: extract adapted from: David Bainbridge (2004) *Software Copyright Law*, pp. 50, 58–9, 92–3, 96–7.

Case study 4: extract from: Alorie Gilbert, staff writer, CNET News.com

Case study 5: extract from The Guide to the General Data Protection Regulation, Information Commissioner's Office (2018)

<https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>

Case study 6: extract from terms, conditions, notices Expedia Inc. (2014)

Case study 7: extract from European Directive on Display Screen Equipment, European Union (1990)

Case study 8: extract from Singapore Government, *Computer Misuse and Cybersecurity Act* (2007)

AV

Videos 1, 2 and 3: © The Open University

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Don't miss out

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – www.open.edu/openlearn/free-courses.