

**Contribution to Oxford Encyclopaedia
“Creative Commons, Integrated Circuits, Open Access, Information Technologies”**

Charlotte Waelde

Creative commons

Creative commons (cc) is a non-profit organisation based in the US. Founded in response to the complexities and cost surrounding licensing of works protected by copyright, it provides a simple method for authors to license works and through which users can determine whether a work can be used for specified purposes. cc makes available modularised licences in human and machine readable form: options include attribution, non-commercial, derivative and share-alike. Originally written with US copyright law in mind, there are now over 36 jurisdiction specific licenses: statistics suggest that many millions of works are licensed using cc licences with well over 200000 under the England and Wales, and Scotland cc licences (early 2007). cc now encompasses a number of different projects including science commons (for scholarly works and scientific data) and ccMixer (for music). There have been few court cases in which the enforceability of the licences has been tested. In 2006 a Dutch court confirmed the licences bind users even where there is no express agreement or knowledge of the terms, while a Spanish court held that a bar which played cc music on its premises was not due a royalty to a collecting society. Academic critics of the movement focus attention on the irony of the reliance on property rights and viral contracts to promote free culture, and the absence of an ethical standard of freedom in information in the licence terms. Others, including content industries, re-emphasise the role of copyright law in promoting and sustaining innovation.

Integrated Circuits

An integrated circuit (IC) is an electronic device made from semiconductor material in which the IC is embedded. There are two aspects to ICs: a functional aspect which dictates the operations it performs, and the design or physical aspect that determines the layout of the components. ICs are found in modern electrical devices such as computers, cars and mobile phones. An IC processes information (e.g. tracking the keys used on a computer). To make an IC, a high energy light is shone through a mask onto a piece of silicon. The light only hits those parts not covered by the mask. These are processed so their electrical properties change. Further layers are added. A final mask detailing the layout of the wires connecting the parts of the IC is placed on top. A complex web of protection exists for ICs by way of Community and national registered design and Community unregistered design right. In addition there is a sui generis unregistered design right under s 213(2) Copyright Designs and Patents Act 1988. Protection under this latter measure is given against copying of the pattern fixed on a layer of semiconductor product. To qualify, the design must be original and not commonplace. Private reproduction for non-commercial purposes is permitted as is some reverse engineering. It has been held that the design of even a single layer of a whole chip is a design within the meaning of the 1988 Act.

Open Access

The term open access does not have a legal definition but supports two common elements: first, products of scholarly research should be available on-line free of charge at the point of use; and second, outputs should be re-usable for legitimate scholarly purposes. Three major public definitions of open access are contained in the Budapest (2002), Bethesda (2003), and Berlin (2003) Declarations. While the first open access source of information was made available in 1966, the movement gained momentum early in the 21st century. The spiralling costs on research institutions of subscribing to academic outputs, the promises digital dissemination heralded for accessibility of scholarly writings, and the complexities of working within the boundaries of copyright law combined to galvanise support for the movement. The result has been a plethora of initiatives, both regulatory and Institutional, to facilitate access to, and re-use of scholarly outputs. In 2004 the House of Commons Science and Technology Select Committee advocated that HEIs should establish institutional repositories in which published output could be stored and read free on-line. In 2005 the Research Councils UK indicated it would make future funding grants conditional on a copy of all outputs being deposited in a repository and available free on-line, subject to copyright or licensing arrangements. There has been opposition, most notably from the academic publishing sector. One, as yet unresolved issue is how open access publishing is to be financed. This is linked with the question of whether the model is sustainable over the longer term.

Information Technologies

While there appears to be no legal definition of information technologies, a useful description is 'the systems, equipment, components and software required to ensure the retrieval, processing and storage of information in all centres of human activity (home, office, factories etc) the application of which generally requires the use of electronics or similar technology'. Although not synonymous with computers, lawyers frequently use the term when referring to the relationship between law and computer technologies, and in particular networked computers.

Legal regulation of information technologies encompasses the computer (the hardware), the software, and the information processed using the technology. Also covered are the uses to which information technologies are put. Many of these uses are legitimate, such as communication and e-commerce, but others are not, such as fraudulent activity or to disseminate child pornography.

Legal regulation occurs through a matrix of initiatives designed specifically to regulate information technologies, adaptation of existing measures, the common law, and more informal self regulatory or self help measures.

Hardware

The hardware (the computer, the peripherals) may be protected by patent, registered design or a combination of the two. If the hardware (or part of the hardware) is new, involves an inventive step, and is capable of industrial application a patent may be granted. Registered design protects the appearance of the hardware where it is new and has individual character. Features solely dictated by technical function are unprotectable. Other parts of the hardware, such as integrated circuits, may be protected differently.

Software

Software will be protected by copyright if it meets the test of being the author's own intellectual creation. Protection extends to literal copying of the software, but not to non-textual copying (sometimes referred to as the 'business logic'). Computer software as such cannot be protected by a patent except where it is a software related invention of a technical character and produces a technical effect.

Information

The information processed by information technologies may take many forms including personal information, sound, video, text and data.

Personal information

In response to the worry that the use of information technologies to process personal information could have negative impacts on the privacy of the subject (echoed in the Human Rights Act 1998) regulation was consolidated in the Data Protection Act 1998 (from a European initiative). This Act requires data users to register with a supervisory body (the Information Commissioner) and to process data in accordance with eight principles (e.g. data must be processed fairly and lawfully). Individuals have a right to know what information is held on them, and to have inaccuracies rectified.

Using information technologies

Creative content

Creative works protected by copyright (such as music, computer software, films) can be copied and disseminated using information technologies. This leaves enforcement difficult for the rightholder, a phenomenon exacerbated by the growth of peer-to-peer networks. Two copyright Treaties, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty both 1996, set increased standards of protection which have been translated into domestic law. Key provisions include the introduction of a communication to the public right, and making unlawful the circumvention of technical protection measures used to control dissemination of works (anti-circumvention measures).

Commerce

In the field of e-commerce, initiatives have been directed towards the use of information technologies to facilitate domestic and cross border trade through the creation of orderly markets and provisions to increase consumer confidence. Measures (which originate in Europe) include the Electronic Commerce Directive, the Privacy and Electronic Communications Directive, the Distance Selling Directive and the Digital Signatures Directive. Among others these provide basic rules for the formation of contracts; recognise digital signatures; detail information that must be given by sellers to buyers; provide a system for controlling unsolicited e-mail through the creation of an opt-in framework, and encourage the establishment of alternative forms of dispute resolution.

Crime

Information technologies can be used to circulate information on, and be used for, criminal and other unlawful activity. The term Cybercrime refers to crimes that cannot be carried out except with a computer, for example spamming (often associated with viruses or fraudulent activity). The technology can also be used to commit the crime (such as child pornography, fraud, incitement of religious hatred), or may the target of the crime (such as virus attacks).

Law enforcement agencies could gather information by intercepting communications. In response to fears from civil libertarians over a surveillance society, a framework has been developed (Regulation of Investigatory Powers Act 2000) which permits interception of communications on public and private systems and grants powers for the acquisition and disclosure of data and information. Any permissible interception must take place according to pre-defined conditions and is subject to judicial oversight. Evidence thus gathered can be used in court.

In addition to the common law and existing legislation, criminal measures have been designed specifically for information technologies. The following are examples of criminal activities which can be committed using information technologies: gaining unauthorised access to programs or data held on a computer (hacking) and the modification of information (viruses); publication of obscene material and possession of child pornography; sexual grooming; certain acts of terrorism and incitement to religious or racial hatred.

Challenges

While much legal regulation in the field of information technologies is initiated at International and European level, as information technologies are increasingly deployed on an international scale, the legal processes needed to facilitate and support expansion, penetration and use will need to become still better co-ordinated and sophisticated. For instance, increasing convergence of media including information, broadcasting and telecommunications technologies (convergence of technologies) to provide a platform through which a varying types of interactive communication can take place (convergence of the use of information technologies) suggests legal regulation also needs to converge. Escalating levels of Cybercrime points towards the need to foster ever greater levels of international co-operation (for progress to date see the European Cybercrime Convention and International Convention on Cybercrime).

Developments will inevitably be accompanied by lively debate from all sectors of society made possible by the very information technologies under scrutiny.