Legal Aspects of Computing & Computer-Related Patent Laws

Dana Switzer
Alex Mangum

First Edition, 2012

ISBN 978-81-323-1285-7

Published by:
College Publishing House
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter 1

Legal Aspects of Computing

Legal aspects of computing are related to various areas of law. **Cyberlaw** is a term that encapsulates the legal issues related to use of communicative, transactional, and distributive aspects of networked information devices and technologies. It is less a distinct field of law than property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include intellectual property, privacy, freedom of expression, and jurisdiction. **Information Technology Law** (or **IT Law**) is a set of recent legal enactments, currently in existence in several countries, which governs the process and dissemination of information digitally. These legal enactments cover a broad gamut of different aspects relating to computer software, protection of computer software, access and control of digital information, privacy, security, internet access and usage, and electronic commerce. These laws have been described as "paper laws" for "paperless environment".

Areas of law

There is intellectual property in general, including copyright, rules on fair use, and special rules on copy protection for digital media, and circumvention of such schemes. The area of software patents is controversial, and still evolving in Europe and elsewhere.

The related topics of software licenses, end user license agreements, free software licenses and open-source licenses can involve discussion of product liability, professional liability of individual developers, warranties, contract law, trade secrets and intellectual property.

In various countries, areas of the computing and communication industries are regulated – often strictly – by government bodies.

There are rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming. There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes. The export of Hardware and Software between certain states is also controlled.

There are laws governing trade on the Internet, taxation, consumer protection, and advertising.

There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies. There are laws on what data must be retained for law enforcement, and what may not be gathered or retained, for privacy reasons.

In certain circumstances and jurisdictions, computer communications may be used in evidence, and to establish contracts. New methods of tapping and surveillance made possible by computers have wildly differing rules on how they may be used by law enforcement bodies and as evidence in court.

Computerized voting technology, from polling machines to internet and mobile-phone voting, raise a host of legal issues.

Some states limit access to the Internet, by law as well as by technical means.

Jurisdiction

Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet.

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extraterritorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of laws, particularly private international law. An example would be where the contents of a web site are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue.

Another major problem of cyberlaw lies in whether to treat the Internet as if it were physical space (and thus subject to a given jurisdiction's laws) or to act as if the Internet is a world unto itself (and therefore free of such restraints). Those who favor the latter view often feel that government should leave the Internet community to self-regulate. John Perry Barlow, for example, has addressed the governments of the world and stated, "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different". A more balanced alternative is the Declaration of Cybersecession: "Human beings possess a mind, which they are absolutely free to inhabit with no legal constraints. Human civilization is developing its own (collective) mind. All we want is to be free to inhabit it with no legal constraints. Since you make sure we cannot harm you, you have no ethical right to intrude our lives. So stop intruding!" Other scholars argue for more of a compromise between the two notions, such as Lawrence Lessig's argument that "The

problem for law is to work out how the norms of the two communities are to apply given that the subject to whom they apply may be in both places at once" (Lessig, Code 190).

With the internationalism of the Internet, jurisdiction is a much more tricky area than before, and courts in different countries have take various views on whether they have jurisdiction over items published on the Internet, or business agreements entered into over the Internet. This can cover areas from contract law, trading standards and tax, through rules on unauthorized access, data privacy and spamming to more political areas such as freedom of speech, censorship, libel or sedition.

Certainly, the frontier idea that the law does not apply in "Cyberspace" is not true. In fact, conflicting laws from different jurisdictions may apply, simultaneously, to the same event. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such, a single transaction may involve the laws of at least three jurisdictions:

1. the laws of the state/nation in which the user resides,
2. the laws of the state/nation that apply where the server hosting the transaction is located, and
3. the laws of the state/nation which apply to the person or business with whom the transaction takes place.

So a user in one of the United States conducting a transaction with another user in Britain through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

In practical terms, a user of the Internet is subject to the laws of the state or nation within which he or she goes online. Thus, in the U.S., Jake Baker faced criminal charges for his e-conduct, and numerous users of peer-to-peer file-sharing software were subject to civil lawsuits for copyright infringement. This system runs into conflicts, however, when these suits are international in nature. Simply put, legal conduct in one nation may be decidedly illegal in another. In fact, even different standards concerning the burden of proof in a civil case can cause jurisdictional problems. For example, an American celebrity, claiming to be insulted by an online American magazine, faces a difficult task of winning a lawsuit against that magazine for libel. But if the celebrity has ties, economic or otherwise, to England, he or she can sue for libel in the British court system, where the standard of "libelous speech" is far lower.

Internet governance is a live issue in international fora such as the International Telecommunication Union (ITU), and the role of the current US-based co-ordinating body, the Internet Corporation for Assigned Names and Numbers (ICANN) was discussed in the UN-sponsored World Summit on the Information Society (WSIS) in December 2003

Regulation of the Internet

The unique structure of the Internet has raised several judicial concerns. While grounded in physical computers and other electronic devices, the Internet is independent of any geographic location. While real individuals connect to the Internet and interact with others, it is possible for them to withhold personal information and make their real identities anonymous. If there are laws that could govern the Internet, then it appears that such laws would be fundamentally different from laws that geographic nations use today.

In their essay "Law and Borders -- The Rise of Law in Cyberspace", David R. Johnson and David G. Post offer a solution to the problem of Internet governance. Given the Internet's unique situation, with respect to geography and identity, Johnson and Post believe that it becomes necessary for the Internet to govern itself. Instead of obeying the laws of a particular country, Internet citizens will obey the laws of electronic entities like service providers. Instead of identifying as a physical person, Internet citizens will be known by their usernames or email addresses. Since the Internet defies geographical boundaries, national laws will no longer apply. Instead, an entirely new set of laws will be created to address concerns like intellectual property and individual rights. In effect, the Internet will exist as its own sovereign nation.

Even if the Internet represents a legal paradigm shift, Johnson and Post do not make clear exactly how or by whom the law of the Internet will be enforced. Instead, the authors see market mechanisms, like those that Medieval merchants used, guiding Internet citizens' actions like Adam Smith's invisible hand. Yet, as more physical locations go online, the greater the potential for physical manifestation of electronic misdeeds. What do we do when someone electronically turns off the hospital lights?

However, there is also substantial literature and commentary that the internet is not only "regulable," but is already subject to substantial regulation, both public and private, by many parties and at many different levels. Leaving aside the most obvious examples of internet filtering in nations like China or Saudi Arabia or Iran (that monitor content), there are four primary modes of regulation of the internet described by Lawrence Lessig in his book, Code and Other Laws of Cyberspace:

1. **Law**: Standard East Coast Code, and the most self-evident of the four modes of regulation. As the numerous statutes, evolving case law and precedents make clear, many actions on the internet are already subject to conventional legislation (both with regard to transactions conducted on the internet and images posted). Areas like gambling, child pornography, and fraud are regulated in very similar ways online as off-line. While one of the most controversial and unclear areas of evolving laws is the determination of what forum has subject matter jurisdiction over activity (economic and other) conducted on the internet, particularly as cross border transactions affect local jurisdictions, it is certainly clear that substantial portions of internet activity are subject to traditional regulation, and that conduct that is unlawful off-line is presumptively unlawful online, and subject to similar

laws and regulations. Scandals with major corporations led to US legislation rethinking corporate governance regulations such as the Sarbanes-Oxley Act.

2. **Architecture**: West Coast Code: these mechanisms concern the parameters of how information can and cannot be transmitted across the internet. Everything from internet filtering software (which searches for keywords or specific URLs and blocks them before they can even appear on the computer requesting them), to encryption programs, to the very basic architecture of TCP/IP protocol, falls within this category of regulation. It is arguable that all other modes of regulation either rely on, or are significantly supported by, regulation via West Coast Code.
3. **Norms**: As in all other modes of social interaction, conduct is regulated by social norms and conventions in significant ways. While certain activities or kinds of conduct online may not be specifically prohibited by the code architecture of the internet, or expressly prohibited by applicable law, nevertheless these activities or conduct will be invisibly regulated by the inherent standards of the community, in this case the internet "users." And just as certain patterns of conduct will cause an individual to be ostracised from our real world society, so too certain actions will be censored or self-regulated by the norms of whatever community one chooses to associate with on the internet.
4. **Markets**: Closely allied with regulation by virtue of social norms, markets also regulate certain patterns of conduct on the internet. While economic markets will have limited influence over non-commercial portions of the internet, the internet also creates a virtual marketplace for information, and such information affects everything from the comparative valuation of services to the traditional valuation of stocks. In addition, the increase in popularity of the internet as a means for transacting all forms of commercial activity, and as a forum for advertisement, has brought the laws of supply and demand in cyberspace.

Net neutrality

Another major area of interest is net neutrality, which affects the regulation of the infrastructure of the Internet. Though not obvious to most Internet users, every packet of data sent and received by every user on the Internet passes through routers and transmission infrastructure owned by a collection of private and public entities, including telecommunications companies, universities, and governments, suggesting that the Internet is not as independent as Barlow and others would like to believe. This is turning into one of the most critical aspects of cyberlaw and has immediate jurisdictional implications, as laws in force in one jurisdiction have the potential to have dramatic effects in other jurisdictions when host servers or telecommunications companies are affected.

Free speech in cyberspace

Article 19 of the Universal Declaration of Human Rights calls for the protection of free expression in all media.

In comparison to traditional print-based media, the accessibility and relative anonymity of cyber space has torn down traditional barriers between an individual and his or her ability to publish. Any person with an internet connection has the potential to reach an audience of millions with little-to-no distribution costs. Yet this new form of highly accessible authorship in cyber space raises questions and perhaps magnifies legal complexities relating to the freedom and regulation of speech in cyberspace.

These complexities have taken many forms, three notable examples being the Jake Baker incident, in which the limits of obscene Internet postings were at issue, the controversial distribution of the DeCSS code, and Gutnick v Dow Jones, in which libel laws were considered in the context of online publishing. The last example was particularly significant because it epitomized the complexities inherent to applying one country's laws (nation-specific by definition) to the internet (international by nature). In 2003, Jonathan Zittrain considered this issue in his paper, "Be Careful What You Ask For: Reconciling a Global Internet and Local Law".

In the UK the case of Keith-Smith v Williams confirmed that existing libel laws applied to internet discussions.

In terms of the tort liability of ISPs and hosts of internet forums, Section 230(c) of the Communications Decency Act may provide immunity in the United States.

Internet censorship

In many countries, speech through cyberspace has proven to be another means of communication which has been regulated by the government. The Open Net Initiative, whose mission statement is "to investigate and challenge state filtration and surveillance practices" to "...generate a credible picture of these practices," has released numerous reports documenting the filtration of internet-speech in various countries. While China has thus far proven to be the most rigorous in its attempts to filter unwanted parts of the internet from its citizens, many other countries - including Singapore, Iran, Saudi Arabia, and Tunisia - have engaged in similar practices of Internet censorship. In one of the most vivid examples of information control, the Chinese government for a short time transparently forwarded requests to the Google search engine to its own, state-controlled search engines.

These examples of filtration bring to light many underlying questions concerning the freedom of speech. For example, does the government have a legitimate role in limiting access to information? And if so, what forms of regulation are acceptable? For example, some argue that the blocking of "blogspot" and other websites in India failed to reconcile the conflicting interests of speech and expression on the one hand and legitimate government concerns on the other hand.

The Creation of Privacy in Cyber-Law

Warren and Brandeis

At the close of the 19th Century, concerns about privacy captivated the general public, and led to the 1890 publication of Samuel Warren and Louis Brandeis: "The Right to Privacy". The vitality of this article can be seen today, when examining the USSC decision of Kyllo v. United States, 533 U.S. 27 (2001) where it is cited by the majority, those in concurrence, and even those in dissent.

The motivation of both authors to write such an article is heavily debated amongst scholoars, however, two developments during this time give some insight to the reasons behind it. First, the sensationalistic press and the concurrent rise and use of "yellow journalism" to promote the sale of newspapers in the time following the Civil War brought privacy to the forefront of the public eye. The other reason that brought privacy to the forefront of public concern was the technological development of "instant photography". This article set the stage for all privacy legislation to follow during the 20 and 21st Centuries.

Reasonable Expectation of Privacy Test and emerging technology

In 1967, the United States Supreme Court decision in Katz v United States, 389 U.S. 347 (1967) established what is known as the Reasonable Expectation of Privacy Test to determine the applicability of the Fourth Amendment in a given situation. It should be noted that the test was not noted by the majority, but instead it was articulated by the concurring opinion of Justice Harlan. Under this test, 1) a person must exhibit an "actual (subjective) expectation of privacy" and 2) "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"

Privacy Act of 1974

Inspired by the Watergate scandal, the United States Congress enacted the Privacy Act of 1974 just four months after the resignation of then President Richard Nixon. In passing this Act, Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies" and that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."

Foreign Intelligence Surveillance Act of 1978

Codified at 50 U.S.C. §§ 1801-1811, this act establishes standards and procedures for use of electronic surveillance to collect "foreign intelligence" within the United States. §1804(a)(7)(B). FISA overrides the Electronic Communications Privacy Act during investigations when foreign intelligence is "a significant purpose" of said investigation.

50 U.S.C. § 1804(a)(7)(B) and §1823(a)(7)(B). Another interesting result of FISA, is the creation of the Foreign Intelligence Surveillance Court (FISC). All FISA orders are reviewed by this special court of federal district judges. The FISC meets in secret, with all proceedings usually also held from both the public eye and those targets of the desired surveillance.

(1986) Electronic Communication Privacy Act

The ECPA represents an effort by the United States Congress to modernize federal wiretap law. The ECPA amended Title III and included two new acts in response to developing computer technology and communication networks. Thus the ECPA in the domestic venue into three parts: 1) Wiretap Act, 2) Stored Communications Act, and 3) The Pen Register Act.

- Types of Communication
    -
    - **Wire Communication:** Any communication containing the human voice that travels at some point across a wired medium such as radio, satellite or cable.
    - **Oral Communication:**
    - **Electronic Communication**

1. **The Wiretap Act**
2. **The Stored Communications Act**
3. **The Pen Register Act**

(1994) Driver's Privacy Protection Act

The DPPA was passed in response to states selling motor vehicle records to private industry. These records contained personal information such as name, address, phone number, SSN, medical information, height, weight, gender, eye color, photograph and date of birth. In 1994, Congress passed the Driver's Privacy Protection (DPPA), 18 U.S.C. §§ 2721-2725, to cease this activity.

(1999) Gramm-Leach-Bliley Act

-This act authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies. The GLBA permits sharing of personal information between companies joined together or affiliated as well as those companies unaffiliated. To protect privacy, the act requires a variety of agencies such as the SEC, FTC, etc. to establish "appropriate standards for the financial institutions subject to their jurisdiction" to "insure security and confidentiality of customer records and information" and "protect against unauthorized access" to this information. 15 U.S.C. § 6801.

(2002) Homeland Security Act

-Passed by Congress in 2002, the Homeland Security Act, 6 U.S.C. § 222, consolidated 22 federal agencies into what is commonly known today as the Department of Homeland Security (DHS). The HSA, also created a Privacy Office under the DoHS. The Secretary of Homeland Security must "appoint a senior official to assume primary responsibility for privacy policy." This privacy official's responsibilities include but are not limited to: ensuring compliance with the Privacy Act of 1974, evaluating "legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the Federal Government", while also preparing an annual report to Congress.

(2004) Intelligence Reform and Terrorism Prevention Act

-This Act mandates that intelligence be "provided in its most shareable form" that the heads of intelligence agencies and federal departments "promote a culture of information sharing." The IRTPA also sought to establish protection of privacy and civil liberties by setting up a five-member Privacy and Civil Liberties Oversight Board. This Board offers advice to both the President of the United States and the entire executive branch of the Federal Government concerning its actions to ensure that the branch's information sharing policies are adequately protecting privacy and civil liberties.

Legal enactments - examples

The Computer Misuse Act 1990 , enacted by Great Britain on 29 June 1990, and which came into force on 29 August 1990, is an example of one of the earliest of such legal enactments. This Act was enacted with an express purpose of making "provision for securing computer material against unauthorised access or modification." Certain major provisions of the Computer Misuse Act 1990 relate to:

- "unauthorised access to computer materials",
- "unauthorised access with intent to commit or facilitate the commission of further offences", and
- "unauthorised modification of computer material."

The impact of the Computer Misuse Act 1990 has been limited and with the adoption of the Council of Europe adopts its Convention on Cyber-Crime, it has been indicated that amending legislation would be introduced in paliamentary session 2004-05 in order to rectify possible gaps in its coverage, which are many.

The CMA 1990 has many weaknesses, the most notable is its' inability to cater for, or provide suitable protection against a host of high tech attacks/crimes which have became more prevalent in the last decade. Certain attacks such as DDOS and BOTNET attacks can not be effectively brought to justice under the CMA. This ACT has been under review for a number of years. Computer crimes such as electronic theft are usually prosecuted in the UK under the legislation that caters for traditional theft (Theft Act 1968), because the CMA is so ineffective.

A recent example of Information Technology Law is India's Information Technology Act 2000, which became effective from 17 October 2000. This Act applies to whole of India, and its provisions also apply to any offence or contravention, committed even outside the territorial jurisdiction of Republic of India, by any person irrespective of his nationality. In order to attract provisions of this Act, such an offence or contravention should involve a computer, computer system, or computer network located in India. The IT Act, 2000 provides an extraterritorial applicability to its provisions by virtue of section 1(2) read with section 75.

India's Information Technology Act 2000 has tried to assimilate legal principles available in several such laws (relating to Information Technology) enacted earlier in several other countries, as also various guidelines pertaining to Information Technology Law. The government of India appointed an Expert Committee to suggest suitable amendments into the existing IT Act, 2000. The amendments suggested by the Committee were severely criticised on various grounds. The chief among them was the dilution of criminal sanctions under the proposed amendments. These amendments, perhaps with some modifications, have been approved by the Cabinet in India on 16 October 2006 and very soon the amendments will be laid down before the Indian Parliament for suitable legislation.

The IT Act, 2000 needs an overall haul keeping in mind the contemporary standards and requirements and the Indian law in this regard is lagging far behind. In the absence of proper law in place, the only recourse is to rely upon the traditional criminal law of India, i.e. Indian Penal Code, 1860 (IPC)that is highly insufficient for cyber crimes in India. Alternatively, a purposive, updating and organic interpretation of the existing provisions of the IT Act, 2000 and IPC by the judiciary must be tried.

The IT Act, 2000 requires a purposive and updating amendment initiative as many contemporary crimes and contraventions are missing from it. Besides, there is an emergent need of introducing the concept of cyber forensics in India.

Many Asian and Middle Eastern nations use any number of combinations of code-based regulation (one of Lessig's four methods of net regulation) to block material that their governments have deemed inappropriate for their citizens to view. PRC, Saudi Arabia and Iran are three excellent examples of nations that have achieved high degrees of success in regulating their citizens access to the Internet.

Electronic Signature Laws

- U.S. - Electronic Signatures in Global and National Commerce Act
- U.S. - Uniform Electronic Transactions Act - adopted by 46 states
- U.S. - Digital Signature And Electronic Authentication Law
- U.S. - Government Paperwork Elimination Act (GPEA)
- U.S. - The Uniform Commercial Code (UCC)
- UK - s.7 Electronic Communications Act 2000
- European Union - Electronic Signature Directive (1999/93/EC)

- Mexico - E-Commerce Act [2000]
- Costa Rica - Digital Signature Law 8454 (2005)
- Australia - *Electronic Transactions Act 1999* (Cth) (also note that there is State and Territory mirror legislation)

Information Technology Law

1. Florida Electronic Security Act
2. Illinois Electronic Commerce Security Act
3. Texas Penal Code - Computer Crimes Statute
4. Maine Criminal Code - Computer Crimes
5. Singapore Electronic Transactions Act
6. Malaysia Computer Crimes Act
7. Malaysia Digital Signature Act
8. UNCITRAL Model Law on Electronic Commerce
9. Information Technology Act 2000 of India

Information Technology Guidelines

1. ABA Digital Signature Guidelines
2. United States Office of Management and Budget

Enforcement agencies

The Information Technology Laws of various countries, and / or their criminal laws generally stipulate enforcement agencies, entrusted with the task of enforcing the legal provisions and requirements.

United States Federal Agencies

Many United States federal agencies oversee the use of information technology. Their regulations are promulgated in the Code of Federal Regulations of the United States.

Over 25 U.S. federal agencies have regulations concerning the use of digital and electronic signatures.

India

A live example of such an enforcement agency is Cyber Crime Police Station, Bangalore, India's first exclusive Cyber Crime enforcement agency.

- Other examples of such enforcement agencies include:
- Cyber Crime Investigation Cell of India's Mumbai Police.
- *Cyber Crime Police Station* of the state Government of Andhra Pradesh, India. This Police station has jurisdiction over the entire state of Andhra Pradesh, and functions from the Hyderabad city.

- In South India, the Crime Branch of Criminal Investigation Department, Tamilnadu police, India, has a Cyber Crime Cell at Chennai.
- In East India, Cyber Crime Cells have been set up by the Kolkata Police as well as the Criminal Investigation Department, West Bengal.

Information Technology Lawyer

An information technology attorney is a professional who handles a variety of legal matters related to IT. The attorney gets involved in drafting, negotiating, and interpreting agreements in the areas of software licensing and maintenance, IT consulting, e-commerce, web site hosting and development, and telecommunications agreements, as well as handling dispute resolution and assisting with the client's Internet domain name portfolio. An information technology attorney works with engineering, IT, and other business units and ensures that customer information gathered by company is collected, stored and used in compliance with privacy policies and applicable laws.

Duties also include providing high quality, specialized and practical advice in business-to-business and business-to-consumer arrangements and advising on issues like IT outsourcing arrangements, software and hardware supply and implementation agreements. An information technology attorney contracts for web site developers and consultants in relation to on-line projects. Provides support and maintains confidentiality/know how agreements. Contracts for Internet service providers and data protection advice. An information technology attorney should have a JD degree or a LLM degree with admission to the local state bar.

Chapter 2

Communications Decency Act and Child Online Protection Act

Communications Decency Act

The **Communications Decency Act of 1996** (**CDA**) was the first notable attempt by the United States Congress to regulate pornographic material on the Internet. In 1997, in the landmark cyberlaw case of *Reno v. ACLU*, the U.S. Supreme Court judge Stewart Dalzell partially overturned the law.

The Act was Title V of the Telecommunications Act of 1996. It was introduced to the Senate Committee of Commerce, Science, and Transportation by Senators James Exon (D-NE) and Slade Gorton (R-WA) in 1995. The amendment that became the CDA was added to the Telecommunications Act in the Senate by an 84–16 vote on June 14, 1995.

As eventually passed by Congress, Title V affected the Internet (and online communications) in two significant ways. First, it attempted to regulate both indecency (when available to children) and obscenity in cyberspace. Second, Section 230 of the Act has been interpreted to say that operators of Internet services are not to be construed as publishers (and thus not legally liable for the words of third parties who use their services).

Anti-indecency and Anti-obscenity provisions

The most controversial portions of the Act were those relating to indecency on the Internet. The relevant sections of the Act were introduced in response to fears that Internet pornography was on the rise. Indecency in TV and radio broadcasting had already been regulated by the Federal Communications Commission—broadcasting of offensive speech was restricted to certain hours of the day, when minors were supposedly least likely to be exposed. Violators could be fined and potentially lose their licenses. The Internet, however, had only recently been opened to commercial interests by the 1992 amendment to the National Science Foundation Act and thus had not been taken into consideration by previous laws. The CDA, which affected the Internet and cable television, marked the first attempt to expand regulation to these new media.

Passed by Congress on February 1, 1996, and signed by President Bill Clinton on February 8, 1996, the CDA imposed criminal sanctions on anyone who

knowingly (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs.

It further criminalized the transmission of materials that were "obscene or indecent" to persons known to be under 18.

Free speech advocates, however, worked diligently and successfully to overturn the portion relating to indecent, but not obscene, speech. They argued that speech protected under the First Amendment, such as printed novels or the use of the *seven dirty words*, would suddenly become unlawful when posted to the Internet. Critics also claimed the bill would have a chilling effect on the availability of medical information. Online civil liberties organizations arranged protests against the bill, for example the Black World Wide Web protest which encouraged webmasters to make their sites' backgrounds black for 48 hours after its passage, and the Electronic Frontier Foundation's Blue Ribbon Online Free Speech Campaign.

Legal challenges

In Philadelphia on June 12, 1996 a panel of federal judges blocked part of the CDA, saying it would infringe upon the free speech rights of adults. The next month, another US federal court in New York struck down the portion of the CDA intended to protect children from indecent speech as too broad. On June 26, 1997, the Supreme Court upheld the Philadelphia court's decision in *Reno v. American Civil Liberties Union,* stating that the indecency provisions were an unconstitutional abridgement of the First Amendment right to free speech because they did not permit parents to decide for themselves what material was acceptable for their children, extended to non-commercial speech, and did not define "patently offensive," a term with no prior legal meaning. (The New York case, *Reno v. Shea*, was affirmed by the Supreme Court the next day, without a published opinion.)

In 2003, Congress amended the CDA to remove the indecency provisions struck down in *Reno v. ACLU*. A separate challenge to the provisions governing obscenity, known as *Nitke v. Gonzales*, was rejected by a federal court in New York in 2005. The Supreme Court summarily affirmed that decision in 2006.

Congress has made two narrower attempts to regulate children's exposure to Internet indecency since the Supreme Court overturned the CDA. Court injunction blocked enforcement of the first, the Child Online Protection Act (COPA), almost immediately after its passage in 1998; the law was later overturned. While legal challenges also

dogged COPA's successor, the Children's Internet Protection Act (CIPA) of 2000, the Supreme Court upheld it as constitutional in 2004.

Section 230 of the Communications Decency Act

Section 230 of the Communications Decency Act of 1996 (a common name for Title V of the Telecommunications Act of 1996) is a landmark piece of Internet legislation in the United States, codified at 47 U.S.C. § 230. Section 230(c)(1) provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by others:

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

In analyzing the availability of the immunity offered by this provision, courts generally apply a three-prong test. A defendant must satisfy each of the three prongs to gain the benefit of the immunity:

1. The defendant must be a "provider or user" of an "interactive computer service."
2. The cause of action asserted by the plaintiff must "treat" the defendant "as the publisher or speaker" of the harmful information at issue.
3. The information must be "provided by another information content provider," i.e., the defendant must not be the "information content provider" of the harmful information at issue.

History

Section 230 of the Communications Decency Act was not part of the original Senate legislation, but was added in conference with the House of Representatives, where it had been separately introduced by Representatives Chris Cox (R-CA) and Ron Wyden (D-OR) as the Internet Freedom and Family Empowerment Act and passed by a near-unanimous vote on the floor. Unlike the more controversial anti-indecency provisions which were later ruled unconstitutional, this portion of the Act remains in force, and enhances free speech by making it unnecessary for ISPs and other service providers to unduly restrict customers' actions for fear of being found legally liable for customers' conduct. The act was passed in part in reaction to the 1995 decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, which suggested that service providers who assumed an editorial role with regard to customer content, thus became publishers, and legally responsible for libel and other torts committed by customers. This act was passed to specifically enhance service providers' ability to delete or otherwise monitor content without themselves becoming publishers. In *Zeran v. America Online, Inc.*, the Court notes that "Congress enacted § 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers

from blocking and screening offensive material, Congress enacted § 230's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." In addition, *Zeran* notes "the amount of information communicated via interactive computer services is...staggering. The specter of tort liability in an area of such prolific speech would have an obviously chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect."

Limits

Section 230's coverage is not complete: it excepts federal criminal liability and intellectual property law. 47 U.S.C. §§ 230(e)(1) (criminal) and (e)(2) (intellectual property); 135 F. Supp. 2d 409 (S.D.N.Y. 2001) (no immunity for contributory liability for trademark infringement). In *Perfect 10, Inc. v. CCBill LLC*, 481 F.3d 751 (9th Cir. Mar. 29, 2007; amended opinion issued May 31, 2007) the Court of Appeals ruled that the exception for intellectual property law applies only to federal intellectual property law, reversing a district court ruling that the exception applies to state right of publicity claims. *Cf. Carfano*, 339 F.3d 1119 (dismissing, inter alia, right of publicity claim under Section 230 without discussion), *but see Doe v. Friendfinder Network, Inc.*, 540 F.Supp.2d 288 (D.N.H. 2008) (230 does not immunize against state IP claims, including right of publicity claims) The *Friendfinder* court specifically discussed and rejected the Ninth Circuit's reading of "intellectual property law" in *CCBill* and held that the immunity does not reach state right of publicity claims.

Controversy

Section 230 is controversial because several courts have interpreted it as providing complete immunity for ISPs with regard to the torts committed by their users over their systems. *See, e.g., Zeran v. AOL*, 129 F.3d 327, 330 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998), which held that Section 230 “creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.” This rule effectively protects online entities, including user-generated content websites, that qualify as a "provider or user" of an "interactive computer service." However some criticize Section 230 for leaving victims with no hope of relief where the true tortfeasors cannot be identified or are judgment proof. For example, the plaintiff in Zeran was clearly defamed by an unidentified user of AOL's bulletin board, but was unable to bring suit against the original poster due to missing records. Since Section 230 barred Zeran from obtaining damages from AOL, he obtained no redress for the harms the messages caused, including death threats that required the involvement of the FBI.

Court Decisions on Section 230

Defamatory information

- *Zeran v. AOL*, 129 F.3d 327 (4th Cir. 1997).

Immunity was ***upheld*** against claims that AOL unreasonably delayed in removing defamatory messages posted by third party, failed to post retractions, and failed to screen for similar postings.

- *Blumenthal v. Drudge*, 992 F. Supp. 44, 49-53 (D.D.C. 1998).

The court ***upheld*** AOL's immunity from liability for defamation. AOL's agreement with the contractor allowing AOL to modify or remove such content did not make AOL the "information content provider" because the content was created by an independent contractor. The Court noted that Congress made a policy choice by "providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others."

- *Carafano v. Metrosplash.com*, 339 F.3d 1119 (9th Cir. 2003).

The court ***upheld*** immunity for an Internet dating service provider from liability stemming from third party's submission of false profile. The plaintiff, Carafano, claimed the false profile defamed her, but because the content was created by a third party, the website was immune, even though it had provided multiple choice selections to aid profile creation.

- *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003).

Immunity was ***upheld*** for a website operator for distributing an email to a listserv where the plaintiff claimed the email was defamatory. Though there was a question as to whether the information provider intended to send the email to the listserv, the Court decided that for determining the liability of the service provider, "the focus should be not on the information provider's intentions or knowledge when transmitting content but, instead, on the service provider's or user's reasonable perception of those intentions or knowledge." The Court found immunity proper "under circumstances in which a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other 'interactive computer service'."

- *Green v. AOL*, 318 F.3d 465 (3rd Cir. 2003).

The court ***upheld*** immunity for AOL against allegations of negligence. Green claimed AOL failed to adequately police its services and allowed third parties to defame him and inflict intentional emotional distress. The court rejected these arguments because holding AOL negligent in promulgating harmful content would be equivalent to holding AOL

"liable for decisions relating to the monitoring, screening, and deletion of content from its network -- actions quintessentially related to a publisher's role."

- *Barrett v. Rosenthal*, 40 Cal. 4th 33 (2006).

Immunity was ***upheld*** for an individual internet user from liability for republication of defamatory statement on a listserv. The court found the defendant to be a "user of interactive computer services" and thus immune from liability for posting information passed to her by the author.

- *MCW, Inc. v. badbusinessbureau.com(RipOff Report/Ed Magedson/XCENTRIC Ventures LLC)* 2004 WL 833595, No. Civ.A.3:02-CV-2727-G, (N.D. Tex. April 19, 2004).

The court ***rejected*** the defendant's motion to dismiss on the grounds of Section 230 immunity, ruling that the plaintiff's allegations that the defendants wrote disparaging report titles and headings, and themselves wrote disparaging editorial messages about the plaintiff, rendered them information content providers.

False information

- *Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816, 830 (2002).

eBay's immunity was ***upheld*** for claims based on forged autograph sports items purchased on the auction site.

- *Ben Ezra, Weinstein & Co. v. America Online*, 206 F.3d 980, 984-985 (10th Cir. 2000), cert. denied, 531 U.S. 824 (2000).

Immunity for AOL was ***upheld*** against liability for a user's posting of incorrect stock information.

- *Goddard v. Google, Inc.*, C 08-2738 JF (PVT), 2008 WL 5245490, 2008 U.S. Dist. LEXIS 101890 (N.D. Cal. Dec. 17, 2008).

Immunity ***upheld*** against claims of fraud and money laundering. Google was not responsible for misleading advertising created by third parties who bought space on Google's pages. The court found the creative pleading of money laundering did not cause the case to fall into the crime exception to Section 230 immunity.

Sexually explicit content and minors

- *Doe v. America Online*, 783 So. 2d 1010, 1013-1017 (Fl. 2001), cert. denied, 122 S.Ct. 208 (2000)

The court ***upheld*** immunity against state claims of negligence based on "chat room marketing" of obscene photographs of minor by a third party.

- *Kathleen R. v. City of Livermore*, 87 Cal. App. 4th 684, 692 (2001)

The California Court of Appeal ***upheld*** the immunity of a city from claims of waste of public funds, nuisance, premises liability, and denial of substantive due process. The plaintiff's child downloaded pornography from a public library's computers which did not restrict access to minors. The court found the library was not responsible for the content of the internet and explicitly found that section 230(c)(1) immunity covers governmental entities and taxpayer causes of action.

- *Doe v. MySpace*, 528 F.3d 413 (5th Cir. 2008)

The court ***upheld*** immunity for a social networking site from negligence and gross negligence liability for failing to institute safety measures to protect minors and failure to institute policies relating to age verification. The Does' daughter had lied about her age and communicated over MySpace with a man who later sexually assaulted her. In the court's view, the Does' allegations, were "merely another way of claiming that MySpace was liable for publishing the communications."

- *Dart v. Craigslist, Inc.*, 665 F. Supp. 2d 961 (N.D. Ill. Oct. 20, 2009)

The court ***upheld*** immunity for Craigslist against a county sheriff's claims that its "erotic services" section constituted a public nuisance because it caused or induced prostitution.

Discriminatory housing ads

- *Chicago Lawyers' Committee For Civil Rights Under Law, Inc. v. Craigslist, Inc.* 519 F.3d 666 (7th Cir. 2008).

The court ***upheld*** immunity for Craigslist against Fair Housing Act claims based on discriminatory statements in postings on the classifieds website by third party users.

- *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*).

The Ninth Circuit Court of Appeals ***rejected*** immunity for the Roommates.com roommate matching service for claims brought under the federal Fair Housing Act and California housing discrimination laws. The court concluded that the manner in which the service elicited information from users concerning their roommate preferences (by having dropdowns specifying gender, presence of children, and sexual orientation), and the manner in which it utilized that information in generating roommate matches (by eliminating profiles that did not match user specifications), the matching service created or developed the information claimed to violate the FHA, and thus was responsible for it as an "information content provider." The court ***upheld*** immunity for the descriptions

posted by users in the “Additional Comments” section because these were entirely created by users.

Threats

- *Delfino v. Agilent Technologies*, 145 Cal. App. 4th 790 (2006), cert denied, 128 S. Ct. 98 (2007).

A California Appellate Court unanimously ***upheld*** immunity from state tort claims arising from an employee's use of the employer's e-mail system to send threatening messages. The court concluded that an employer that provides Internet access to its employees qualifies as a "provider . . . of an interactive service."

Legislation in other countries

Legislation in other countries may lack the protections afforded by the Act.

European Union

Directive 2000/31/EC establishes a safe haven regime for hosting providers:

- Article 14 establishes that hosting providers are not responsible for the content they host as long as (1) the acts in question are neutral intermediary acts of a mere technical, automatic and passive capacity; (2) they are not informed of its illegal character, and (3) they act promptly to remove or disable access to the material when informed of it.
- Article 15 precludes member states from imposing general obligations to monitor hosted content for potential illegal activities.

Australia

In *Dow Jones & Company Inc v Gutnick*, the High Court of Australia treated defamatory material on a server outside Australia as having been published in Australia when it is downloaded or read by someone in Australia.

Gorton v Australian Broadcasting Commission & Anor (1973) 1 ACTR 6

Under the *Defamation Act 2005* (NSW), s 32, a defence to defamation is that the defendant neither knew, nor ought reasonably to have known of the defamation, and the lack of knowledge was not due to the defendant's negligence.

New Zealand

Failing to investigate the material or to make inquiries of the user concerned may amount to negligence in this context: *Jensen v Clark* [1982] 2 NZLR 268.

France

Directive 2000/31/CE was transposed into the LCEN law. Article 6 of the law establishes safe haven for hosting provider as long as they follow certain rules.

In LICRA vs. Yahoo!, the High Court ordered Yahoo! to take affirmative steps to filter out Nazi memorabilia from its auction site. Yahoo!, Inc. and its then president Timothy Koogle were also criminally charged, but acquitted.

Germany

In 1997, Felix Somm, the former managing director for CompuServe Germany, was charged with violating German child pornography laws because of the material CompuServe's network was carrying into Germany. He was convicted and sentenced to two years probation on May 28, 1998. He was cleared on appeal on November 17, 1999.

The Oberlandesgericht (OLG) Cologne, an appellate court, found that an online auctioneer does not have an active duty to check for counterfiet goods (Az 6 U 12/01).

In one example, the first-instance district court of Hamburg issued a temporary restraining order requiring message board operator Universal Boards to review all comments before they can be posted to prevent the publication of messages inciting others to download a harmful files. The court reasoned that "the publishing house must be held liable for spreading such material in the forum, regardless of whether it was aware of the content."

United Kingdom

The laws of libel and defamation will treat a disseminator of information as having "published" material posted by a user and the onus will then be on a defendant to prove that it did not know the publication was defamatory and was not negligent in failing to know: *Goldsmith v Sperrings Ltd* (1977) 2 All ER 566; *Vizetelly v Mudie's Select Library Ltd* (1900) 2 QB 170; *Emmens v Pottle & Ors* (1885) 16 QBD 354;

Child Online Protection Act

The **Child Online Protection Act** (**COPA**) was a law in the United States of America, passed in 1998 with the declared purpose of restricting access by minors to any material defined as harmful to such minors on the Internet. The United States federal courts have ruled that the law violates the constitutional protection of free speech, and therefore have blocked it from taking effect. As of 2009, the law remains unconstitutional and unenforced.

The law was part of a series of efforts by US lawmakers legislating over Internet pornography. Parts of the earlier and much broader Communications Decency Act had been struck down as unconstitutional by the Supreme Court; COPA was a direct response to that decision, narrowing the range of material covered. COPA only limits commercial speech and only affects providers based within the United States.

COPA required all commercial distributors of "material harmful to minors" to restrict their sites from access by minors. "Material harmful to minors" was defined as material that by "contemporary community standards" was judged to appeal to the "prurient interest" and that showed sexual acts or nudity (including female breasts). This is a much broader standard than obscenity.

Litigation history

The federal government was enjoined from enforcing COPA by a court order in 1998. In 1999, the United States Court of Appeals for the Third Circuit upheld the injunction and struck down the law, ruling that it was too broad in using "community standards" as part of the definition of harmful materials. In May 2002, the Supreme Court reviewed this ruling, found the given reason insufficient and returned the case to the Circuit Court; the law remained blocked. On March 6, 2003, the 3rd Circuit Court again struck down the law as unconstitutional, this time finding that it would hinder protected speech among adults. The government again sought review in the Supreme Court.

On June 29, 2004, in *Ashcroft v. American Civil Liberties Union*, the Supreme Court upheld the injunction on enforcement, ruling that the law was likely to be unconstitutional. Notably, the court mentioned that "filtering's superiority to COPA is confirmed by the explicit findings of the Commission on Child Online Protection, which Congress created to evaluate the relative merits of different means of restricting minors' ability to gain access to harmful materials on the internet." The court also wrote that it was five years since the district court had considered the effectiveness of filtering software and that two less-restrictive laws had been passed since COPA, one prohibiting misleading domain names and another creating a child-safe .kids domain, and that given the rapid pace of internet development those might be sufficient to restrict access by minors to specific material. The court referred the case back to the district court for a trial, which began on October 25, 2006.

In preparation for that trial, the Department of Justice issued subpoenas to various search engines to obtain Web addresses and records of searches as one part of a study undertaken by a witness in support of the law. The search engines turned over the requested information, except for Google, which challenged the subpoenas. The court limited the subpoena to a sample of URLs in Google's database, but declined to enforce the request for searches conducted by users; Google then complied.

On March 22, 2007, U.S. District Judge Lowell A. Reed, Jr. once again struck down the Child Online Protection Act, finding the law facially in violation of the First and Fifth Amendments of the United States Constitution. In addition to the plaintiffs ACLU et al.,

several witnesses testified in defense of first amendment rights on the Internet, including the director of the Erotic Authors Association, Marilyn Jaye Lewis. Reed issued an order permanently enjoining the government from enforcing COPA, commenting that "perhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection." The government again appealed, and the case was heard before the Third Circuit.

On July 22, 2008, the 3rd U.S. Circuit Court of Appeals upheld the 2007 decision.

On January 21, 2009, the United States Supreme Court refused to hear appeals of the lower court decision, effectively killing the bill.

Chapter 3

Computer Fraud and Abuse Act and Computer Misuse Act 1990

Computer Fraud and Abuse Act

The **Computer Fraud and Abuse Act** is a law passed by the United States Congress in 1986, intended to reduce cracking of computer systems and to address federal computer-related offenses. The Act (codified as 18 U.S.C. § 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or where computers are used in interstate and foreign commerce.

It was amended in 1988, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act. Subsection (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Act, but also those who conspire to do so.

Protected computers

The CFAA defines "protected computers" under 18 U.S.C. § 1030(e)(2) to mean a computer:

- exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
- which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

Criminal offenses under the Act

1. Knowingly accessing a computer without authorization in order to obtain national security data

2. Intentionally accessing a computer without authorization to obtain:
    - Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.
    - Information from any department or agency of the United States
    - Information from any protected computer if the conduct involves an interstate or foreign communication
3. Intentionally accessing without authorization a government computer and affecting the use of the government's operation of the computer.
4. Knowingly accessing a protected computer with the intent to defraud and there by obtaining anything of value.
5. Knowingly causing the transmission of a program, information, code, or command that causes damage or intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in:
    - Loss to one or more persons during any one-year period aggregating at least $5,000 in value.
    - The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
    - Physical injury to any person.
    - A threat to public health or safety.
    - Damage affecting a government computer system
6. Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization.

Cases and decisions referring to the Act

- *Theofel v. Farey Jones*, 2003 U.S. App. Lexis 17963, decided August 28, 2003 (U.S. Court of Appeals for the Ninth Circuit). Using a civil subpoena which is "patently unlawful", "bad faith" and "at least gross negligence" to gain access to stored email is a breach of this act and the Stored Communications Act.
- *Robbins v. Lower Merion School District* (U.S. Eastern District of Pennsylvania), where plaintiffs charged two suburban Philadelphia high schools secretly spied on students by surreptitiously and remotely activating webcams embedded in school-issued laptops the students were using at home, violating the Act. The schools admitted to secretly snapping over 66,000 webshots and screenshots, including webcam shots of students in their bedrooms.

Computer Misuse Act 1990

The **Computer Misuse Act 1990** is an Act of the UK Parliament, introduced partly in response the decision in *R v Gold & Schifreen* (1988) 1 AC 1063 (see below). Critics of the bill complained that it was introduced hastily and was poorly thought out. Intention, they said, was often difficult to prove, and that the bill inadequately differentiated "joyriding" crackers like Gold and Schifreen from serious computer criminals. The Act has nonetheless become a model from which several other countries, including Canada and the Republic of Ireland, have drawn inspiration when subsequently drafting their own information security laws.

R v Gold & Schifreen

Robert Schifreen and Stephen Gold, using conventional home computers and modems in late 1984 and early 1985, gained unauthorised access to British Telecom's Prestel interactive viewdata service. While at a trade show, Schifreen by doing what latterly became known as shoulder surfing, had observed the password of a Prestel engineer: the username was 22222222 and the password was 1234. This later gave rise to subsequent accusations that BT had not taken security seriously. Armed with this information, the pair explored the system, even gaining access to the personal message box of Prince Philip.

Unknown to Schifreen and Gold, the Prestel computer network operated on a distributed basis and was intended to act as a hot standby in the event of the UK going to war - in the event that the primary UK military computers were down, the Prestel network could be used to control and launch the UK's nuclear missiles.

Following discussions with GCHQ and MI6, it was decided to investigate Schifreen and Gold's activities, notwithstanding that, as freelancers for Micronet, a joint venture between BT and a major publishing house, the pair had informed their superiors of their discovery.

Following interventions from GCHQ, Prestel installed monitors on both of the pair's modem connections and, acting on the information obtained, decided it was in the best interests of national security to arrest them.

After some months of deliberation, it was decided to charge the pair under section 1 of the Forgery and Counterfeiting Act 1981, with defrauding BT by manufacturing a "false instrument", namely the internal condition of BT's equipment after it had processed Gold's eavesdropped password. Tried at Southwark Crown Court, they were convicted on specimen charges (five against Schifreen, four against Gold) and fined, respectively, £750 and £600.

Although the fines imposed were modest, they elected to appeal to the Criminal Division of the Court of Appeal. Their counsel cited the lack of evidence showing the two had

attempted to obtain material gain from their exploits, and claimed the Forgery and Counterfeiting Act had been misapplied to their conduct.

They were acquitted by the Lord Justice Lane, but the prosecution appealed to the House of Lords. In 1988, the Lords upheld the acquittal. Lord David Brennan said:

We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case. The submissions at the close of the prosecution case should have succeeded. It is a conclusion which we reach without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts.

The Law Lords' ruling led many legal scholars to believe that hacking was not unlawful as the law then stood. The English Law Commission (ELC) and its counterpart in Scotland both considered the matter. The Scottish Law Commission concluded that intrusion was adequately covered in Scotland under the common law related to deception, but the ELC believed a new law was necessary.

Since the case, both defendants have gone to write about IT matters extensively and, in the case of Gold, who detailed the entire case at some length in the Hacker's Handbook, actually presents at conferences alongside the arresting officers in the case.

The Computer Misuse Act

Based on the ELC's recommendations, a Private Member's Bill was introduced by Conservative MP Michael Colvin. The bill, supported by the government, came into effect in 1990. Sections 1-3 of the Act introduced three criminal offences:

1. unauthorised access to computer material, punishable by 6 months' imprisonment or a fine "not exceeding level 5 on the standard scale" (currently £5000);
2. unauthorised access with intent to commit or facilitate commission of further offences, punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment;
3. unauthorised modification of computer material, subject to the same sentences as section 2 offences.

§§2–3 are intended to deter the more serious criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The basic offence is to attempt or achieve access to a computer or the data it stores, by inducing a computer to perform any function with intent to secure access. Hackers that program their computers to search through password permutations are therefore liable, even though all their attempts to log on are rejected by the target

computer. The only precondition to liability is that the hacker should be aware that the access attempted is unauthorized. Thus, using another person's username or identifier (ID) and password without proper authority to access data or a program, or to alter, delete, copy or move a program or data, or simply to output a program or data to a screen or printer, or to impersonate that other person using e-mail, online chat, web or other services, constitute the offence. Even if the initial access is authorized, subsequent exploration, if there is a hierarchy of privileges in the system, may lead to entry to parts of the system for which the requisite privileges are lacking and the offence will be committed. But looking over a user's shoulder or using sophisticated electronic equipment to monitor the electromagnetic radiation emitted by VDUs ("electronic eavesdropping") is outside the scope of this offence.

The §§2–3 offences are aggravated offences, requiring a specific intent to commit another offence (for these purposes, the other offences are to be arrestable, and so include all the major common law and statutory offences of fraud and dishonesty). So a hacker who obtains access to a system intending to transfer money or shares, intends to commit theft, or to obtain confidential information for blackmail or extortion. Thus, the §1 offence is committed as soon as the unauthorized access is attempted, and the §2 offence overtakes liability as soon as specific access is made for the criminal purpose. The §3 offence is specifically aimed at those who write and circulate a computer virus or worm, whether on a LAN or across networks. Similarly, using phishing techniques or a Trojan horse to obtain identity data or to acquire any other data from an unauthorized source, or modifying the operating system files or some aspect of the computer's functions to interfere with its operation or prevent access to any data, including the destruction of files, or deliberately generating code to cause a complete system malfunction, are all criminal "modifications". In 2004 John Thornley pleaded guilty to four offences under §3, having mounted an attack on a rival site, and introduced a Trojan horse to bring it down on several occasions, but it is recognized that the wording of the offence should be clarified to confirm that all forms of denial of service attack are included.

Latest situation

In 2004, the All-Party Internet Group published its review of the law and highlighted areas for development. Their recommendations led to the drafting of the *Computer Misuse Act 1990 (Amendment) Bill* which sought to amend the CMA to comply with the European Convention on Cyber Crime. Under its terms, the maximum sentence of imprisonment for breaching the Act changed from six months to two years. It also sought to explicitly criminalise denial-of-service attacks and other crimes facilitated by denial-of-service. The Bill did not receive Royal Assent because Parliament was prorogued.

Sections 35 to 38 of the Police and Justice Act 2006 contains amendments to the Computer Misuse Act 1990.

Section 37 (*Making, supplying or obtaining articles for use in computer misuse offences*) inserts a new section 3A into the 1990 Act and has drawn considerable criticism from IT

professionals, as many of their tools can be used by the forces of evil in addition to their legitimate purposes, and thus fall under section 3A.

Chapter 4

Convention on Cybercrime and Copyright Aspects of Hyperlinking and Framing

Convention on Cybercrime

The **Convention on Cybercrime** is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg with the active participation of the Council of Europe's observer states Canada, Japan and China.

The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of 2 September 2006, 15 states had signed, ratified and acceded to the convention, while a further 28 states had signed the convention but not ratified it.

On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are requited to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

Objectives

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and Lawful interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention aims principally at:

1. harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime
2. providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form
3. setting up a fast and effective regime of international co-operation.

The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties.

The Convention is the product of four years of work by European and international experts. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. Currently, cyber terrorism is also studied in the framework of the Convention.

Accession by the USA

Its ratification by the United States Senate in August 2006 was both praised and condemned. The U.S. became the 16th nation to ratify the convention. Forty-three nations have signed the treaty. The Convention entered into force in the USA on January 1, 2007.

"While balancing civil liberty and privacy concerns, this treaty encourages the sharing of critical electronic evidence among foreign countries so that law enforcement can more effectively investigate and combat these crimes," said Senate Majority Leader Bill Frist.

"The Convention includes a list of crimes that each signatory state must transpose into their own law. It requires the criminalization of such activities as hacking (including the production, sale, or distribution of hacking tools) and offenses relating to child pornography, and expands criminal liability for intellectual property violations. It also requires each signatory state to implement certain procedural mechanisms within their laws. For example, law enforcement authorities must be granted the power to compel an Internet Service Provider to monitor a person's activities online in real time. Finally, the Convention requires signatory states to provide international cooperation to the widest extent possible for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a

criminal offense. Law enforcement agencies will have to assist police from other participating countries to cooperate with their mutual assistance requests."

Although a common legal framework would eliminate jurisdictional hurdles to facilitate the law enforcement of borderless cyber crimes, a complete realization of a common legal framework may not be possible. Transposing Convention provisions into domestic law is difficult especially if it requires the incorporation of substantive expansions that run counter to constitutional principles. For instance, the U.S. may not be able to criminalize all the offenses relating to child pornography that are stated in the Convention, specifically the ban on virtual child pornography, because of its First Amendment free speech principles. Under Article 9(2)(c) of the Convention, a ban on child pornography includes any “realistic images representing a minor engaged in sexually explicit conduct.” According to the Convention, the U.S. would have to adopt this ban on virtual child pornography as well, however, the U.S. Supreme Court, in Ashcroft v. Free Speech Coalition, struck down as unconstitutional a provision of the CPPA that prohibited "any visual depiction” that "is, or appears to be, of a minor engaging in sexually explicit conduct." In response to the rejection, the U.S. Congress enacted the PROTECT Act to amend the provision, limiting the ban to any visual depiction “that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct.” 18 U.S.C

The United States will not become a Party to the Additional Protocol to the Convention on Cybercrime.

Accession by other non-European states

The Convention has been signed by Canada, Japan, USA and the Republic of South Africa on 23 November 2001 (the signing took place in Budapest, Hungary). Further accessions by other non-European states are planned.

Copyright aspects of hyperlinking and framing

In copyright law, the legal status of **hyperlinking** (also termed “**linking**”) and that of **framing** concern how courts address two different but related web technologies. In large part, the legal issues concern use of these technologies to create or facilitate public access to proprietary media content — such as portions of commercial Web sites. When hyperlinking and framing have the effect of distributing, and creating routes for distribution of, content (information) that does not come from the proprietors of the Web pages affected by these practices, the proprietors often seek the aid of courts to suppress the conduct, particularly when the effect of the conduct is to disrupt or circumvent the proprietors' mechanisms for receiving financial compensation.

The issues about linking and framing have become so intertwined under copyright law that it is impractical to attempt to address them separately. As will appear, some decisions confuse them with one another, while other decisions involve and therefore address both. Framing involves the use of hyperlinking, so that any challenge of framing under copyright law is likely to involve a challenge of hyperlinking as well. (The converse is not true.)

Linking

While hyperlinking occurs in other technologies, US copyright litigation has centered on HTML.

Ordinary link

The HTML code for a simple, ordinary hyperlink is as shown below.

A typical Internet browser will render the foregoing HTML code as:

General Information Concerning Patents

When a user clicks the curser on the underlined words on the monitor screen, the browser jumps from the page on which the link is shown to a page of the Website of the US Patent and Trademark Office (PTO) that has the URL (Web address) shown above**.**

Deep link

Most Web sites are organized hierarchically, with a home page at the top and deeper pages within the site, reached by links on the home page. Businesses often want users to enter their Web sites from the home pages, so that they are exposed to advertising messages. A third party can thwart this expectation by so-called deep linking. The term refers to using a hyperlink that takes a user directly to a page other than the top or home page. The link given above is a deep link. A home-page link would be written this way:

Several lawsuits have involved complaints by proprietors of Web pages against the use of deep links.

Inline link

Related issues arise from use of inline links (also image-source or img-src links, so called because the HTML code begins with "img src=") on Web pages. An inline link places material — usually an image such as a Jpeg or Gif — from a distant Web site onto the Web page being viewed. For example, the image at the right is the seal of the U.S. Patent Office, as shown on some of its pages at the PTO Web site. The former of these becomes an inline or img-src link if *img src=* is inserted before the *http*, angle brackets enclose the whole expression, and the entire code fragment is inserted into the text of a page of HTML code.

When an inline (img-src) link of an image is used on a Web page, it seems to be present as a part of the Web page that you are viewing. The presence of the image is only virtual, however, in the sense that the image file is not physically present at the server for the Web site being viewed. The actual location of the image file, if the image were that of the PTO seal, would be at the PTO server in Virginia. Use of inline linking has led to contentious litigation (discussed below).

Hierarchy of links

Image links can be categorized in a hierarchical series, based on the technological expedient used to effectuate the link. The same series corresponds to successively lower levels of risk of copyright infringement liability. The hierarchy operates as follows, using the PTO seal as an example for discussion purposes (actually, it is not legally protected because it is a government work):

- Copy the image file to your own server. This will create copyright infringement liability unless a defense, such as fair use or license, applies.
- Use an img-src link to the image at the proprietor's Web page, making the image appear on your page in its visual appearance (to the user) the same as above. *But there is no copy of the image file on your server*. (This is also true of all links that follow in this list.)

- Use an ordinary link to the image at the remote server, so that users must click on a link on your page to jump to the image.

- Use a deep link on your page to the specific page on the image proprietor's Web site at which the image is located, thus presenting the image to the user along with the textual material with which the proprietor surrounded it.

- Use a link on your page to the home page of the image proprietor's Web site and explain how to page down through his successive pages and all of his extraneous material in order to find the image. This will not create copyright infringement liability under any theory thus far advanced in US litigation.

Framing

Framing is the juxtaposition of two separate web pages within the same page, usually with a separate frame with navigational elements. Framing is a method of presentation in a Web page that breaks the screen up into multiple non-overlapping windows. Each window contains a display from a separate HTML file, for example, a Web page from a different Web site that is fetched by automatically hyperlinking to it. While the usage of frames as a common web design element has been deprecated for several years (replaced by the usage of elements), some sites, like Google Images and Google Translate, use frames as a way to help navigate non-Google pages from a framed Google interface.

Incorporating copyrighted web content by usage of framing has led to contentious litigation. Frames can be used for web pages belonging to the original site, or to load pages from other sites into a customized arrangement of frames that provide a generalized interface without actually requiring the viewer to browse the linked site from that site's URLs and interfaces.

Proprietors of copyright in framed pages have at times contended that framing their Web pages constituted copyright infringement of their copyrights. The problem with basing the theory of copyright infringement on a reproduction (17 U.S.C. § 106(1)) or distribution (17 U.S.C. § 106(3)) of copies by the accused infringer is that the latter does not directly *reproduce* or *distribute* any copy of the original Web page. Rather, the accused infringer simply establishes a pointer that the user's browser follows to the proprietor's server and Web page.

For a pedagogically exaggerated example of the kind of framing that has incensed proprietors of copyright in Web pages, see Hypothetical Illustration of Irritating Framing, which "frames" a page titled Is Framing Copyright Infringement?. On the theory that a picture is worth 1000 words, the viewer is invited to compare the referenced pages to understand what framing is and why it annoys proprietors of framed pages.

History of copyright litigation in field

In large part, linking and framing are not held to be copyright infringement under US and German copyright law, even though the underlying Web pages are protected under copyright law. Because the copyright-protected content is stored on a server other than that of the linking or framing person (it is stored on the plaintiff's server), there is typically no infringing "copy" made by the defendant linking or framing person (as may be essential), on which to base liability. Some European countries take a more protective view, however, and hold unauthorized framing and so-called deep linking unlawful.

Belgium

Belgian Association of Newspaper Editors v. Google

In September 2006 the Belgian Association of Newspaper Editors sued Google and obtained an injunctive order from the Belgian Court of First Instance that Google must stop deep linking to Belgian newspapers without paying royalties, or else pay a fine of €1 million daily.

But when we really look at the court ruling there is no conviction for using hyperlinks. Google was convicted for copyright issues in Google cache and using reproductions on Google News. The court ruled that Google News was a portal and not a search engine and that it not used snippets but reproductions on that portal. The Court also ruled using hyperlinks was not a problem, a Belgium blogger (deinternetmarketeer.be) cleared this out when getting annoyed with the fact that half of the world published false facts without checking them in the Court rule.

Denmark

Danish Newspaper Publishers Association v. Newsbooster

The Bailiff's Court of Copenhagen ruled in July 2002 against the Danish Website Newsbooster, holding, in a suit brought by the Danish Newspaper Publishers Association (DNPA), that Newsbooster had violated Danish copyright law by deep linking to newspaper articles on Danish newspapers' Internet sites. Newsbooster's service allows users to enter keywords to search for news stories, and then deep links to the stories are provided. The DNPA said that this conduct was "tantamount to theft." The court enjoined Newsbooster's service.

home A/S v. Ofir A-S

The Maritime and Commercial Court in Copenhagen took a somewhat different view in 2005 in a suit that home A/S, a real estate chain, brought against Ofir A-S, an Internet portal (OFiR), which maintains an Internet search engine. home A/S maintains an Internet website that has a searchable database of home's current realty listings. Ofir copied some database information, which the court held unprotected under Danish law,

and also Ofir's search engine provided deep links to the advertisements for individual properties that home A/S listed, thus by-passing the home page and search engine of home A/S. The court held that the deep linking did not create infringement liability. The Court found that search engines are desirable, as well as necessary to the function of the Internet; that it is usual that search engines provide deep links; and that businesses that offer their services on the Internet must expect that deep links will be provided to their websites. Ofir's site did not use banner advertising and its search engine allowed users, if they so chose, to go to a home page rather than directly to the advertisement of an individual property. The opinion does not appear to distinguish or explain away the difference in result from that of the *Newsbooster* case.

DNPA v. Google

In November 2008, the DNPA, citing its success against Newsbooster, demanded that Google stop deep linking to stories in Danish newspapers without paying royalties.

Germany

Holtzbrinck v. Paperboy

In July 2003 a German Federal Superior Court held that the Paperboy search engine could lawfully deep link to news stories. See paidContent:UK, "German Court: Deep Linking Is Legal". An appellate court then overturned the ruling, but the German Federal Supreme Court reversed in favor of Paperboy. MIP Week, "German ruling sanctions deep linking". "A sensible use of the immense wealth of information offered by the world wide web is practically impossible without drawing on the search engines and their hyperlink services (especially deep links)," the German court said.

Scotland

Shetland Times Ltd. v. Wills

The first suit of prominence in the field was *Shetland Times Ltd. v. Wills*, Scot. Ct. of Session (Edinburgh, 24 Oct 1996). The Shetland Times challenged use by Wills of deep linking to pages of the newspaper on which selected articles of interest appeared. The objection was that defendant Wills thus by-passed the front and intervening pages on which advertising and other material appeared in which the plaintiff had an interest but defendant did not. The Times obtained an interim interdict (Scottish for preliminary injunction) and the case then settled.

United States

Washington Post v. Total News

In February 1997 the Washington Post, CNN, the Los Angeles Times, Dow Jones (*Wall Street Journal*), and Reuters sued Total News Inc. for framing their news stories on the Total News Webpage. The complaint was filed in New York federal district court. The case was settled in June 1997, on the basis that linking without framing would be used in the future.

Ticketmaster v. Microsoft

In April 1997 Ticketmaster Corp. sued Microsoft Corp. in Los Angeles federal district court for deep linking. Ticketmaster objected to Microsoft's bypassing the home and intermediate pages on Ticketmaster's site, claiming that Microsoft had "pilfered" its content and diluted its value. Microsoft's ''Answer'' raised a number of defenses explained in detail in its pleadings, including implied license, contributory negligence, and voluntary assumption of the risk. Microsoft also, argued that Ticketmaster had breached an unwritten Internet code, under which any Web site operator has the right to link to anyone else's site. A number of articles in the trade press derided Ticketmaster's suit. The case was settled in February 1999, on confidential terms. But Microsoft stopped the deep linking and instead used a link to Ticketmaster's home page.

Kelly v. Arriba Soft

The first important US decision in this field was that of the Ninth Circuit in *Kelly v. Arriba Soft Corp.* Kelly complained, among other things, that Arriba's search engine used thumbnails to deep link to images on his Web page. The court found that Arriba's use was highly transformative, in that it made available to Internet users a functionality not previously available, and that was not otherwise readily provided — an improved way to search for images (by using visual cues instead of verbal cues). This factor, combined with the relatively slight economic harm to Kelly, tipped the fair use balance decisively in Arriba's favor.

As in other cases, Kelly objected to linking because it caused users to bypass his home page and intervening pages. He was unable, however, to show substantial economic harm. Kelly argued largely that the part of the copyright statute violated was the public display right (17 U.S.C. § 106(5)). He was aware of the difficulties under the reproduction and distribution provisions (17 U.S.C. §§ 106(1) and (3)), which require proof that the accused infringer trafficked in copies of the protected work. The court focused on the fair use defense, however, under which it ruled in Arriba's favor.

Perfect 10 v. Google

In *Perfect 10, Inc. v. Amazon.com, Inc.*, the Ninth Circuit again considered whether an image search engine's use of thumbnail was a fair use. Although the facts were somewhat closer than in the ''Arriba Soft'' case, the court nonetheless found the accused infringer's use fair because it was "highly transformative." The court explained:

We conclude that the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case. … We are also mindful of the Supreme Court's direction that "the more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use."

In addition, the court specifically addressed the copyright status of linking, in the first US appellate decision to do so:

Google does not…display a copy of full-size infringing photographic images for purposes of the Copyright Act when Google frames in-line linked images that appear on a user's computer screen. Because Google's computers do not store the photographic images, Google does not have a copy of the images for purposes of the Copyright Act. In other words, Google does not have any "material objects…in which a work is fixed…and from which the work can be perceived, reproduced, or otherwise communicated" and thus cannot communicate a copy. Instead of communicating a copy of the image, Google provides HTML instructions that direct a user's browser to a website publisher's computer that stores the full-size photographic image. Providing these HTML instructions is not equivalent to showing a copy. First, the HTML instructions are lines of text, not a photographic image. Second, HTML instructions do not themselves cause infringing images to appear on the user's computer screen. The HTML merely gives the address of the image to the user's browser. The browser then interacts with the computer that stores the infringing image. It is this interaction that causes an infringing image to appear on the user's computer screen. Google may facilitate the user's access to infringing images. However, such assistance raised only contributory liability issues and does not constitute direct infringement of the copyright owner's display rights. …While in-line linking and framing may cause some computer users to believe they are viewing a single Google webpage, the Copyright Act, unlike the Trademark Act, does not protect a copyright holder against acts that cause consumer confusion.

State of US law after *Arriba Soft* and *Perfect 10*

The *Arriba Soft* case stood for the proposition that deep linking and actual reproduction in reduced-size copies (or preparation of reduced-size derivative works) were both excusable as fair use because the defendant's use of the work did not actually or potentially divert trade in the marketplace from the first work; and also it provided the public with a previously unavailable, very useful function of the kind that copyright law exists to promote (finding desired information on the Web). The *Perfect 10* case involved similar considerations, but more of a balancing of interests was involved. The conduct was excused because the value to the public of the otherwise unavailable, useful function outweighed the impact on Perfect 10 of Google's possibly superseding use.

Moreover, in *Perfect 10*, the court laid down a far-reaching precedent in favor of linking and framing, which the court gave a complete pass under copyright. It concluded that "in-line linking and framing may cause some computer users to believe they are viewing a single Google webpage, [but] the Copyright Act" simply does not prohibit such conduct.

Pop-up advertising cases

Pop-up advertising involves some use of linking to copyright-protected Web pages, but the linking is incidental to other issues and has not been singled out as a separate wrong. Moreover, given the breadth of the language of the *Perfect 10* opinion of the Ninth Circuit (quoted above), it appears that such a claim would be unlikely to prevail.

Chapter 5

Copyrighted Content on File Sharing Networks and Cyber defamation law

Copyrighted content on file sharing networks

The legal issues in file sharing involve violation of copyright laws as digital copies of copyrighted materials are transferred between users.

The application of national copyright laws to peer-to-peer and file sharing networks is of global significance. Peer-to-peer ("P2P") technology allows people worldwide to share files and data, and since this includes some that is subject to copyright, it has been targeted by rights holders, although peer-to-peer networks can be used for legitimate purposes.

The architecture of P2P systems vary - some rely upon a centralized server, others are decentralized with no one site operating the system. Newer P2P system architectures often include measures to conceal the identities of senders, recipients and material.

Legal issues relevant to file sharing

The challenges facing copyright holders in the face of file sharing systems are quite novel historically and have highlighted many new challenges in both theory and practice:

- Ambiguities in the interpretation of copyright law
- The new challenges posed by international communications and varying legislations
- Mass litigation and the development of processes for evidence and discovery
- Rapidly developing new technologies and uses
- Low barriers to entry by would-be sharers and the development of a mass usage of the technologies
- File sharing approaches developed in response to litigation against sharers, which obfuscate or hide the fact that sharing is happening, or the identities of those involved. For example: encryption and Darknets.

Copyright law in the United States

Copyright law

A copyright in the United States consists of the rights enumerated under 17 USC 106.

The four largest record companies, working together under the leadership of the RIAA, seek to stop peer-to-peer file sharing by attacking the use of 'shared files folders'. They claim that the making of files available for sharing on a P2P network infringes on their right under 17 USC 106(3) "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending". Critics have argued that the RIAA has failed to show (a) dissemination, (b) of actual phonorecords or copies, (c) "to the public" (as opposed to a limited group), or any (d) sale, transfer of ownership, rental, lease, or lending..... all of which are required components of a 17 USC 106(3) "distribution".

The basic copyright law issues

Case law in this area is in its infancy.

In the United States, the RIAA, on behalf of the four largest worldwide record companies, launched an estimated 30,000 cases over a four year period, against individuals whose Internet access accounts had, according to the plaintiffs, been associated with peer-to-peer file sharing accounts using FastTrack technology, e.g., Kazaa, LimeWire, Gnutella, iMesh, and others. The suits are based upon a report of an Internet investigator who claims to have detected a "shared files folder". At the core of in October, 2007. Although it initially resulted in a verdict against Jammie Thomas of $222,000 for "making available" 24 song files having a total retail value of $23.76, or less, the Judge who presided over the trial overturned the verdict, on the ground that his submission of the case to the jury under the RIAA's "making available" theory was a "manifest error of law". He also criticized the size of the verdict as "wholly disproportionate" to the damages, and urged Congress to amend the Copyright Act to prevent the possibility of a recurrence.

After the *Capitol v. Thomas* trial, and before the decision setting the verdict aside, the Courts in *Atlantic v. Brennan* , *Elektra v. Barker*, above, *Atlantic v. Howell*, and *London-Sire v. Doe 1*, had rejected the RIAA's "making available" theory.. But in *Barker* the judge had suggested to the RIAA another theory which it might plead -- "offering to distribute for purposes of redistribution". The lower courts seem to be forming a consensus that the 'making available' theory is incorrect. But the question of whether merely 'making files available' over a peer-to-peer network is actionable has yet to be decided on an appellate level. In *Thomas* Judge Michael J. Davis agreed most closely with the *Howell*, *Brennan*, and *London-Sire* analyses, and rejected the "offer to distribute" theory proffered by the judge in *Barker*.

Primary infringement liability

The fundamental question, "what use can a P2P file-sharing network's customers make of the software and of copyrighted materials without violating copyright law", has no answer at this time, as there has been almost no dispositive decision-making on the subject.

This issue has received virtually no appellate attention, the sole exception being *BMG Music v. Gonzalez*, a decision of the U.S. Court of Appeals for the Seventh Circuit, which held that where a defendant has admitted downloading and copying song files from other users in the P2P network without permission of the copyright holders, she cannot claim that such copying is a "fair use". Since *Gonzalez* involves a defendant who had admitted to actual copying and downloading of songs from other unauthorized users, it is of limited applicability in contested cases, in that it relates solely to the reproduction right in 17 USC 106(1), and has no bearing on the 17 USC 106(3) distribution right.

A series of cases dealing with the RIAA's "making available" theory has broad implications, not only for the subject of P2P file sharing but for the Internet at large. The first to receive a great deal of attention was *Elektra v. Barker*, an RIAA case against Tenise Barker, a Bronx nursing student. Ms. Barker moved to dismiss the complaint, contending, among other things, that the RIAA's allegation of "making available" did not state any known claim under the Copyright Act.. The RIAA countered with the argument that even without any copying, and without any other violation of the record companies' distribution rights, the mere act of "making available" is a copyright infringement, even though the language does not appear in the Copyright Act, as a violation of the "distribution" right described in 17 USC 106(3). Thereafter, several *amicus curiae* were permitted to file briefs in the case, including the MPAA, which agreed with the RIAA's argument, and the Electronic Frontier Foundation (EFF), the U.S. Internet Industry Association (USIIA), and the Computer & Communications Industry Association (CCIA), which agreed with Ms. Barker. The US Department of Justice submitted a brief refuting one of the arguments made by EFF, but did not take any position on the RIAA's "making available" argument, noting that it had never prosecuted anyone for "making available".. The *Elektra v. Barker* case was argued before Judge Kenneth M. Karas in Manhattan federal court on January 26, 2007, and decided on March 31, 2008.

The decision rejected the RIAA's "making available" theory but sustained the legal sufficiency of the RIAA's pleading of actual distribution and actual downloading. Additionally, the Court suggested to the RIAA that it might want to amend its complaint to include a claim for "offering to distribute for purposes of distribution", but gave no guidance on what type of evidence would be required for an "offer". The Court's suggestion that merely "offering" to distribute could constitute a violation of the Act has come under attack from William Patry, the author of the treatise Patry on Copyright.

Three other decisions, also rejecting the RIAA's "making available" theory, came from more unexpected sources.

The *Barker* decision was perhaps rendered anticlimactic by the decision of Judge Janet Bond Arterton, from the District of Connecticut, handed down six weeks earlier, in *Atlantic v. Brennan* , rejecting the RIAA's application for a default judgment. *Brennan*, like *Barker*, rejected the RIAA's "making available" theory, but unlike *Barker* it found the RIAA's specificity on the other issues to be insufficient, and it rejected the conceptual underpinnings upon which Judge Karas based his "offer to distribute" idea.

And *Barker* was perhaps overshadowed by the decision of Judge Gertner, rendered the same day as the *Barker* decision, in quashing a subpoena served on Boston University to learn the identity of BU students, in *London-Sire v. Doe 1* . Here too the Court rejected the RIAA's "making available" theory, but here too—like *Atlantic* but unlike *Elektra* -- also rejected any possible underpinning for an "offer to distribute" theory.

And then came the decision of the District Judge Neil V. Wake, in the District of Arizona, in *Atlantic v. Howell*.. This 17-page decision -- rendered in a case in which the defendant appeared *pro se* (i.e., without a lawyer) but eventually received the assistance of an *amicus curiae* brief and oral argument by the Electronic Frontier Foundation-- was devoted almost exclusively to the RIAA's "making available" theory and to the "offer to distribute" theory suggested by Judge Karas in *Barker*. *Atlantic v. Howell* strongly rejected both theories as being contrary to the plain wording of the Copyright Act. The Court held that "Merely making a copy available does not constitute distribution....The statute provides copyright holders with the exclusive right to distribute "copies" of their works to the public "by sale or other transfer of ownership, or by rental, lease, or lending." 17 U.S.C. ...106(3). Unless a copy of the work changes hands in one of the designated ways, a "distribution" under ...106(3) has not taken place." The Court also expressly rejected the 'offer to distribute' theory suggested in *Barker*, holding that "An offer to distribute does not constitute distribution".

The next critical decision was that in *Capitol v. Thomas*, which had received a great deal of media attention because it was the RIAA's first case to go to trial, and probably additional attention due to its outsized initial jury verdict. The RIAA had prevailed upon the trial judge to give the jurors an instruction which adopted its "making available" theory, over the protestations of the defendant's lawyer. Operating under that instruction, the jury returned a $222,000 verdict over $23.76 worth of song files. Almost a year after the jury returned that verdict, however, District Judge Michael J. Davis set the verdict aside, and ordered a new trial, on the ground that his instruction to the jurors—that they did not need to find that any files were actually distributed in order to find a violation of plaintiffs' distribution right—was a "manifest error of law". The Judge's 44-page decision agreed with *Howell* and *London-Sire* and rejected so much of *Barker* as intimated the existence of a viable "offer to distribute" theory.

There may be indications that the RIAA has been jettisoning its "making available" theory. In a San Diego, California, case, *Interscope v. Rodriguez*, where the Judge dismissed the RIAA's complaint as "conclusory", "boilerplate", "speculation", the RIAA filed an amended complaint which contained no reference at all to "making available". In

subsequent cases, the RIAA's complaint abandoned altogether the "making available" theory, following the model of the *Interscope v. Rodriguez* amended complaint.

In its place, it is apparently adopting the "offer to distribute" theory suggested by Judge Karas. In the amended complaint the RIAA filed in *Barker*, it deleted the "making available" argument—as required by the judge—but added an "offer to distribute" claim, as the judge had suggested. It remains to be seen if it will follow that pattern in other cases.

Secondary infringement liability

Secondary liability, the possible liability of a defendant who is not a copyright infringer but who may have encouraged or induced copyright infringement by another, has been discussed generally by the United States Supreme Court in *MGM v. Grokster*, which held in essence that secondary liability could only be found where there has been affirmative encouragement or inducing behavior. On remand, the lower court found Streamcast, the maker of Morpheus software, to be liable for its customers' copyright infringements, based upon the specific facts of that case.

Under US law "the Betamax decision" (Sony Corp. of America v. Universal City Studios, Inc.), holds that copying "technologies" are not *inherently* illegal, if substantial non-infringing use can be made of them. Although this decision predated the widespread use of the Internet, in *MGM v. Grokster*, the U.S. Supreme Court acknowledged the applicability of the Betamax case to peer-to-peer file sharing, and held that the networks could not be liable for merely providing the technology, absent proof that they had engaged in "inducement."

A little over a year later, the RIAA initiated the first major post-Grokster, secondary liability case, *Arista v. Limewire*, in Manhattan federal court. LimeWire denied the allegations, and counterclaimed, charging the major record companies with antitrust violations and other misconduct."Lime Wire Sues RIAA for Antitrust Violations" The antitrust claims have, however, been dismissed, so the case is moving ahead solely on the copyright issues.

Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF) seeks to protect and expand digital rights through litigation, political lobbying, and public awareness campaigns. The EFF has vocally opposed the RIAA in its pursuit of lawsuits against users of file sharing applications and supported defendants in these cases. The foundation promotes the legalization of peer-to-peer sharing of copyrighted materials and alternative methods to provide compensation to copyright holders.

In September, 2008, the organization marked the 5th 'anniversary' of the RIAA's litigation campaign by publishing a highly critical, detailed report, entitled "RIAA v. The People : Five Years Later", concluding that the campaign was a failure.

End of litigation campaign?

Several months later, it was reported that the RIAA was suspending its litigation campaign. This was followed by a report that it had fired its investigative firm, SafeNet (formerly MediaSentry). Some of the details of the reports, including claims that the RIAA had actually stopped commencing new lawsuits months earlier, and that its reason for doing so was that it had entered into tentative agreements with Internet service providers to police their customers, proved to be either inaccurate or impossible to verify. (See, e.g. "Questions about New York State Attorney General agreement with record labels", Recording Industry vs. People, January 1, 2009 and "RIAA claim not to have filed new cases "for months" is false", Recording Industry vs. The People, December 19, 2008)

Copyright law in European Union

Graduated response

Demonstration in Sweden in support of file sharing, 2006

In response to copyright violations using peer-to-peer file sharing the content industry has proposed legislation instituting a *graduated response*, or *three strikes system*. Consumers who do not adhere to repeated complaints on copyright infringement, risk losing access to the Internet. The content industry has sought to gain the co-operation of Internet service providers (ISPs), asking them to provide subscriber information for ISP addresses

accused by the content industry of engaging in copyright violations. Consumer rights groups have argued that this approach denies consumers the right to due process and the right to privacy. The European Parliament passed a non-binding resolution in April 2008 admonishing laws that would require ISPs to disconnect their users and would prevent individuals from acquiring access to broadband.

In a number of European countries attempts to implement a graduated response have led to court cases to establish under which circumstances an ISP may provide subscriber data to the content industry. In order to pursue those that download copyrighted material the individual committing the infringing must be identified. Internet users are often only identifiable by their Internet Protocol address (IP address), which distinguishes the virtual location of a particular computer, unless that IP address is behind a NAT. Most ISPs allocate a pool of IP addresses as needed, rather than assigning each computer a static IP address. Using ISP subscriber information the content industry has thought to remedy copyright infringement, presuming and accusing that that the ISPs are legally responsible for end user activity, (in the US, under the DMCA, they are not) and that the end user is responsible for all illegal activity connected to his or her IP address.

In 2005 a Dutch court ordered ISPs in the Netherlands to not divulge subscriber information because of the way the Dutch content industry group had collected the IP addresses (Foundation v. UPC Nederland). According to Dutch law ISPs can only be ordered to provide personal subscriber data if it is plausible that an unlawful act occurred, and if it is shown beyond a reasonable doubt that the subscriber information will identify the person who committed the infringing act. In Germany court specifically considered the right to privacy and in March 2008 the German Federal Constitutional Court ruled that ISPs could only give out IP address subscription information in case of a "serious criminal investigation". The court furthermore ruled that copyright infringement did not qualify as a serious enough offense. Subsequently, in April 2008, the Bundestag (German parliament) approved a new law requiring ISPs to divulge the identity of suspected infringers who infringe on a commercial scale. Similarly, in Sweden, a controversial file sharing bill is awaiting the Riksdag's approval. The law, which would enter into effect on April 1, 2009, would allow copyright holders to request the IP addresses and names of copyright infringement suspects in order to take legal action against them. The copyright holders, though, should present sufficient evidence of harm to justify the release of information regarding the Internet subscribers. In Italy courts established that criminally liability does not extend to file sharing copyrighted material, as long as it is not done for commercial gain. Ruling on a case involving a copyright holder employed a third party to collect IP addresses of suspected copyright infringers, the Italian Data Protection Authority ruled in February 2008 that the systematic monitoring peer-to-peer activities for the purpose of detecting copyright infringers and suing them.

At the same time a number of other European countries are considering to implement a graduated response to copyright infringement via the Internet, including France and Britain. In France President Nicolas Sarkozy is backing a proposal to implement a graduated response law, while in Britain voluntary arrangement between ISPs and the content industry is considered towards this end.

Spain

In a series of cases, Spanish courts have ruled that file sharing for private use is legal. In 2006, the record industry's attempt to criminalize file sharing were disappointed when Judge Paz Aldecoa declared it legal to download indiscriminately in Spain, if done for private use and without any profit purpose,, and the head of the police's technology squad has publicly said "No pasa nada. Podéis bajar lo que queráis del eMule. Pero no lo vendáis." ("It's ok. You can download whatever you want with eMule. But don't sell it."). There have been demonstrations where the authorities has been informed that copyrighted material was going to be downloaded in a public place, the last of which took place on the 20th December 2008. No legal action was taken against it. In another decision, in May 2009, a judge ruled in favor of a person engaged in the private, non-commercial file-sharing of thousands of movies, even though the copying was done without the consent of the copyright owners.

The Spanish Supreme Court has ruled that personal data associated with an IP address could only be disclosed in the course of a criminal investigation or for public safety reasons. (Productores de Música de España v. Telefónica de España SAU).

Copyright law in Canada

Interestingly, Canada stands out by authorizing, at least until the projected copyright reform proposed by Bill C-61, downloads on peer-to-peer networks under the "private copying" exception. However, bill C-61 never became law because of an election in late 2008. The Conservative Party that tabled Bill C-61 have promised to do another similar bill in the future.

It is to be noted that Canada does not explicitly condone piracy. However, the federal police do not actively search for copiers that do not make profits from their illicit activities.

Copyright law in Australia

A secondary liability case in Australia, under Australian law, was *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2005] FCA 1242 5 September 2005, which was settled out of court.

In the case of AFACT v iiNet; which was fought out in Sydney Federal Court, determined that iiNet was not liable, for the copyright infringement of their users, and thus created a precedent that other Australian ISP's were not liable for the copyright infringement of their users. AFACT and other Major Australian copyright holders, hope to appeal the case, or pursue the matter by lobbying the government to change the Australian law.

Important cases

USA

- Sony Corp. v. Universal City Studios (The Betamax decision)
- MGM v. Grokster
- The AACS encryption key controversy of 2007

Sweden

- The Pirate Bay trial

Singapore

- Odex's actions against file-sharing

Cyber defamation law

Cyber Defamation is a crime conducted in cyberspace, usually through the Internet, with the intention of defaming others. The cyber defamation law that the Korean government tries to make is intended to capture such criminal activities by allowing police to crack down on hateful comments without any reports from the victims. The only country where such cyber defamation law is being implemented is China, and South Korea is the first democratic country in the process of introducing the law.

South Korea

The Korea Communications Commission (KCC), South Korea's telecommunications and broadcasting regulator, has been considering revising the current Telecommunications Law and put more regulations and deeper scrutiny on major Internet portals.

Controversies

There have been talks about introducing the stricter laws in cyberspace. A famous celebrity's suicide in South Korea, triggered the controversies once again as to whether such law is necessary. The law supported by the governing Grand National Party (GNP), if implemented, will allow police to investigate the cyber defamation cases without any complaints of the victims. The opposition Democratic Party (DP) has been against the introduction of such law.

Advocate views

- The current laws have failed to prevent the number of the victims from increasing at an escalating rate.
- Freedom of speech comes with responsibility.
- Due to the fact that information and rumors can travel in a matter of seconds in the Internet, cyber-bullying and cyber defamation could take a significant toll on each victim without such strict regulations by authorities.

Opposing views

- There are already ways to regulate the cyberspace with the current laws.
- It is potentially possible for the law to be exploited by authorities in an attempt to crack down on people who express opposite views.
- Such law might cause a harmful effect on freedom of speech.
- "Defamation" is too ambiguous to be defined by a third party, other than the victims.

Survey

A Research & Research survey of 800 Korean people conducted on Jan. 14, 2009 showed that 60% supported the GNP-led bill dealing with cyber defamation, and 32.1% opposed it.

Celebrities' suicide

Some Korean celebrities have suffered from severe depression, caused in part by malicious online comments, before committing suicide.

- Lee Eun-ju
- Jung Da Bin
- U;Nee
- Choi Jin-sil

Chapter 6

Deleting Online Predators Act of 2006

The **Deleting Online Predators Act of 2006** (**DOPA**) is a bill (**H.R. 5319**) brought before the United States House of Representatives on May 9, 2006 by Republican Pennsylvania Representative (R-PA) Mike Fitzpatrick. The bill, if enacted, would amend the Communications Act of 1934, requiring schools and libraries that receive E-rate funding to protect minors from online predators in the absence of parental supervision when using "Commercial Social Networking Websites" and "Chat Rooms". The bill would prohibit schools and libraries from providing access to these types of websites to minors or create restrictions to use of these type of sites. The bill also would require the institutions to be capable of disabling the restrictions for "use by an adult or by minors with adult supervision to enable access for educational purposes."

The bill is considered controversial because according to its critics the bill could limit access to a wide range of websites, including many with harmless and educational material. Arguments for the bill focus on the fear of adults contacting children on MySpace and similar websites. Many Internet websites, however (ranging from Yahoo to Slashdot to Amazon.com), allow user accounts, public profiles, and user forums, in accord with the bill's definition of "social networking". The bill places the onus upon the Federal Communications Commission to provide clarification.

History of the Deleting Online Predators Act

The bill was introduced on May 9, 2006 by Rep. Michael Fitzpatrick (R-PA) as part of the Suburban Caucus agenda. Along with co-sponsors, he spoke in favor of it. The Caucus' "Suburban Agenda" was shaped around the results of a January 2007 survey conducted by John McLaughlin . McLaughlin focused on issues that could weaken the expected impact of midterm elections on the Republican hold of Congress in Suburban constituencies like Bucks County, Pennsylvania and Orange County, California.

On July 26, 2006, DOPA was brought up for debate and an immediate vote in the House. It was criticized by Rep. Edward Markey (D-MA) and Rep. Bart Stupak (D-MI) for being hastily rewritten before its vote and did not get markup of a full House Committee. The House of Representatives voted 410-15 (7 Not Voting), on a Roll Call vote, to pass the bill as amended. The following day, the bill was received in the U.S. Senate and referred to the Commerce, Science, and Transportation Committee.

As a House bill, it was passed to the Senate for approval. The bill was not voted on by the Senate.

On January 4, 2007, Senator Ted Stevens (R-AK) reintroduced DOPA in the U.S. Senate as part of S.49, "Protecting Children in the 21st Century Act". The bill was immediately referred to the Commerce, Science, and Transportation Committee. On February 16, 2007, Rep. Mark Kirk (R-IL) reintroduced The Deleting Online Predators Act of 2007. The bill was referred to the House Committee on Energy and Commerce.

State Legislation Restricting Access to Social Networking Sites

Similar bills to ban or restrict access to social networking sites have been introduced in Georgia, North Carolina, Oklahoma and Illinois in 2007.

The untitled Georgia bill and the North Carolina Protect Children From Sexual Predators Act impose criminal penalties on any owner or operator of a social networking website that permits a minor to create a profile or join the site without parental consent; if the parent consents, the site must allow parents full access to the minor's profile and webpage. Oklahoma's HB 1715 would require public libraries to block access to email and social networking sites or deny minors access to the Internet in its entirety.

The Illinois Social Networking Prohibition Act would require all public libraries and schools to block access to any social networking site for users of all ages.

Specifics of the proposed Act

Definitions

"Commercial Social Networking Websites" were originally defined within the bill as:

Sec.2(c)(J) a commercially operated Internet website that-
(i) allows users to create web pages or profiles that provide information about themselves and are available to other users; and
(ii) offers a mechanism for communication with other users, such as a forum, chat room, email, or instant messenger.

The term "chat rooms" were defined as:

Sec.2(c)(K) Internet websites through which a number of users can communicate in real time via text and that allow messages to be almost immediately visible to all other users or to a designated segment of all other users.

Popular websites fitting this definition include MySpace, Facebook, Friendster, and LiveJournal. This definition could, however, potentially cover a much broader range of websites. Many news websites such as Slashdot and blogs like RedState permit both public profiles and personal journals. Amazon.com allows personal profiles including

photos, interests, and contact information. In addition, many media companies, such as News.com publisher CNET Networks, permit users to create profiles displaying photos and other personal information, as well as sending email to other members. Some popular chat services include ICQ, AOL Instant Messenger, and Yahoo! Chat.

Before the floor vote in the House, the bill was amended to read:

(J) COMMERCIAL SOCIAL NETWORKING WEBSITES; CHAT ROOMS—Within 120 days after the date of enactment of the Deleting Online Predators Act of 2006, the Commission shall by rule define the terms 'social networking website' and 'chat room' for purposes of this subsection. In determining the definition of a social networking website, the Commission shall take into consideration the extent to which a website—
(i) is offered by a commercial entity;
(ii) permits registered users to create an on-line profile that includes detailed personal information;
(iii) permits registered users to create an on-line journal and share such a journal with other users;
(iv) elicits highly-personalized information from users; and
(v) enables communication among users.

Under the new language, the Federal Communications Commission, not Congress, will define these terms, using the five criteria as guidelines. Whether the new definition would ultimately be broader or narrower than the original one is unclear. Commercial operation, however, no longer appears to be an absolute requirement, and it could potentially encompass other websites. Like all other provisions of the bill, it is subject to change in a conference committee before it becomes law.

FTC Requirements

The bill would also require the Federal Trade Commission to issue a consumer alert about the online predation dangers of commercial social networking websites and chat rooms and to create a website for parents, teachers, school administrators, and others about the dangers of these types of websites, including a list of such websites.

Controversy

Both sides spoke out in favor of blocking online predators. The controversy was over the effectiveness and drawbacks of the specific measures to be taken.

Arguments in Favor

The bill's proponents, including members of the Suburban Caucus, argue that restrictions on access to social networking websites are necessary to protect children from online predators, whether the predators be sexually oriented offenders or even simple online bullies. In introducing his part of the Suburban Caucus agenda, Rep. Michael Fitzpatrick (R-PA) said that as a father he was concerned that, since the "world moves and changes

at a dizzying pace," he felt he could no longer keep up in protecting his children, especially when they had Internet access in places other than their own home. He believed legislation was therefore necessary. In his speech, he noted that one in five children had received an unwanted online solicitation of a sexual nature and that child pornography had increased by 2,000 percent in the past decade. The former is most likely a reference to the Youth Internet Safety Survey from University of New Hampshire, while the latter is a reference to the increase in arrests from the FBI's "Innocent Images National Initiative".

Rep. Judy Biggert (R-IL) added that children have often been taught never to talk to strangers, and that the Internet makes the temptation to talk to strangers stronger. In fact, she noted, a minor in Michigan had traveled halfway across the world to Jericho to meet in person someone she met on MySpace.

Rep. Ginny Brown-Waite (R-FL) spoke and referred to the murder of Jessica Lunsford by John Couey, and said that stalking could now occur online as well as in person.

There are many online safety concerns for children using MySpace, including the amount of specific personal information to use certain website tools, lack of validation for other members' information, and lack of sufficient moderation by the website for review of user violations.

Arguments in Opposition

The arguments against the bill have focused on efforts to revise it to directly address the problem of online predators, and to prevent the blocking of harmless and/or educational websites. Rep. Bart Stupak (D-MI) summarized: "Unfortunately, child predators are not the target of today's bill. This bill will not delete online predators. Rather, it will delete legitimate Web content from schools and libraries."

Overly Broad Definition

As noted in the Definition section, many websites allow public user profiles and provide forums. Examples include Yahoo, Amazon.com, Slashdot, RedState, CNET Networks, and thousands of others. This potentially qualifies them as social networking websites regardless of the content within the websites.

Educational Use

Most school libraries already have filters on incoming Internet access due to the Children’s Internet Protection Act (CIPA). Opponents of the bill point out that the language of the bill would extend such filtering to include websites based on specific technologies rather than specific content, including websites based on those technologies that are used for educational purposes. Some educators have incorporated blogs into classroom lessons for students due to their usefulness as a critiquing and editing tool for students' work and as a forum for comments and suggestions by teachers and other

students. These educators also favor such technologies because they enable discussion outside of the classroom that can involve students and teachers as well as parents.

Some examples of educational use of these technologies:

- Will Richardson, a teacher in New Jersey, set up a blog for student discussion of *The Secret Life of Bees* and invited author Sue Monk Kidd to join the chat. She was able to answer the students' questions about the book and give more insight than the teacher alone would have been capable. A separate blog was set up to allow parents to discuss the book in parallel with the students.

- Some school administrators are using blogs to communicate news and information about events to parents and students. The homepage for the Meriweather Lewis Elementary School in Oregon is updated with notes from the PTA. The principal and teachers are using blogging software and RSS to allow parents and students to view up-to-date information from the school.

- The Pawtucket Public Library in Pawtucket, Rhode Island is one of a number of public libraries that have created their own MySpace profile webpage. These libraries are attempting to communicate with young adult patrons more effectively through the use of online methods to which young adults are becoming accustomed.

The bill would allow minors strictly limited access to those sites. For schools, access would be allowed only with adult supervision *and* if the site is being used for an educational purpose. For libraries, access would be allowed only if parental authorization is given and the parents are informed that "sexual predators can use these websites and chat rooms to prey on children."

The American Library Association

The American Library Association is asking its members to oppose DOPA. Former ALA president Michael Gorman said, "We know that the best way to protect children is to teach them to guard their privacy and make wise choices. To this end, libraries across the country offer instruction on safe Internet use". On July 11, 2006, the Executive Director of the Young Adult Library Services Association (YALSA), Beth Yoke, testified before the Subcommittee on Telecommunications and the Internet under the Committee on Energy and Commerce. She defined the ALA and YALSA combined stance on the issue by saying:

Youth librarians believe, and more importantly know from experience, that education about safe Internet practices—for both youth *and* parents—is the best way to protect young people. We believe that the overly broad technological controls that would be required under DOPA are often ineffective given the fast-moving nature of modern technology. Further, such technological controls often inadvertently obstruct access to beneficial sites. In essence, we believe that this legislation will lead to the blocking of

essential and beneficial Interactive Web applications and will further widen the digital divide.

The ALA and other opponents of the bill also believe that this issue is one that should be determined by local authorities, such as local library trustees, community members, and school boards. Opponents argue that this federal action could degrade the authority of those responsible for safe use of the libraries, whereas up to 80% of the funding for the library or school is locally derived.

Effectiveness in Protecting Minors

Rep. Diane Watson (D-CA) and Rep. John Dingell (D-MI) argued that the bill would fail to combat the threats to minors and that it would place a burden on schools and libraries to block millions of sites with largely innocent information. Rep. Jay Inslee (D-WA) suggested that the law should focus upon directly blocking and prosecuting predators as well as providing tools to educate children on how to avoid dangers -- noting that most Internet access, especially to social networking sites, occurs in the home. Education and prevention programs regarding predators and social networking could help reduce the rate of sexual assaults overall -- whether over the Internet from home or offline. The Youth Internet Safety Survey from the University of New Hampshire, which was implicitly cited by Rep. Michael Fitzpatrick, found two cases of rape/sexual assault through Internet solicitation in its two surveys covering 3,001 children ages 10 to 17. According to the FBI's criminal victimization tables' national rate for sexual assault, one would expect seven rapes or sexual assaults among such a group every year.

Overall, the Youth Internet Safety Survey suggested that fewer children are actually being sexually solicited online in 2005 than in 1999, hypothesizing that those who encountered solicitations knew better now to rebuff or ignore these solicitations. However, children ages 10 to 17 report more harassment and bullying online -- largely from their peers, not the strangers from which Michael Fitzpatrick believes children should be protected.

Chapter 7

Software Patent

Software patent does not have a universally accepted definition. One definition suggested by the Foundation for a Free Information Infrastructure is that a software patent is a "patent on any performance of a computer realised by means of a computer program".

There is intense debate over the extent to which software patents should be granted, if at all. Important issues concerning software patents include:

- Where the boundary between patentable and non-patentable software should lie;
- Whether the inventive step and non-obviousness requirement is applied too loosely to software; and
- Whether patents covering software discourage, rather than encourage, innovation.

Background

A patent is a set of exclusionary rights granted by a state to a patent holder for a limited period of time, usually 20 years. These rights are granted to patent applicants in exchange for their disclosure of the inventions. Once a patent is granted in a given country, no person may make, use, sell or import/export the claimed invention in that country without the permission of the patent holder. Permission, where granted, is typically in the form of a license which conditions are set by the patent owner: it may be gratis or in return for a royalty payment or lump sum fee.

Patents are territorial in nature. To obtain a patent, inventors must file patent applications in each and every country in which they want a patent. For example, separate applications must be filed in Japan, China, the United States and India if the applicant wishes to obtain patents in those countries. However, some regional offices exist, such as the European Patent Office (EPO), which act as supranational bodies with the power to grant patents which can then be brought into effect in the member states, and an international procedure also exists for filing a single international application under the Patent Cooperation Treaty (PCT), which can then give rise to patent protection in most countries.

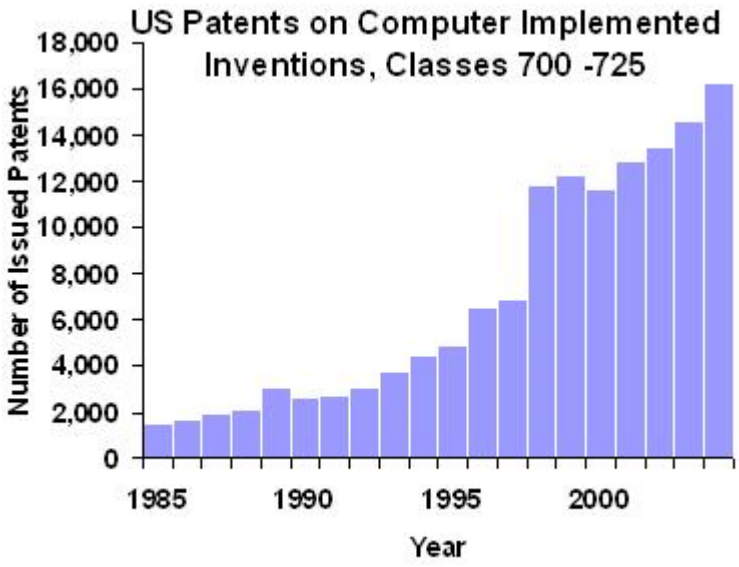
These different countries and regional offices have different standards for granting patents. This is particularly true of software or computer-implemented inventions, especially where the software is implementing a business method.

History and current trends

Early example of a software patent

On 21 May 1962, a British patent application entitled "*A Computer Arranged for the Automatic Solution of Linear Programming Problems*" was filed. The invention was concerned with efficient memory management for the simplex algorithm, and could be implemented by purely software means. The patent was granted on August 17, 1966 and seems to be one of the first software patents.

United States



Growth of software patents in US

The United States Patent and Trademark Office has granted patents that may be referred to as software patents since at least the early 1970s. In Gottschalk v. Benson (1972), the United States Supreme Court ruled that a patent for a process should not be allowed if it would "wholly pre-empt the mathematical formula and in practical effect would be a patent on the algorithm itself", adding that "it is said that the decision precludes a patent for any program servicing a computer. We do not so hold." In 1981, the Supreme Court stated that "a claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula, computer program, or digital computer" and a claim is patentable if it contains "a mathematical formula [and] implements or applies the formula in a structure or process which, when considered as a whole, is performing a function which the patent laws were designed to protect".

Due to different treatment of federal patent rights in different parts of the country, in 1982 the U.S. Congress created a new court (the Federal Circuit) to hear patent cases. Following several landmark decisions by this court, by the early 1990s the patentability of software was well established, and in 1996 the USPTO issued Final Computer Related Examination Guidelines stating that "A *practical application* of a computer-related invention is statutory subject matter. This requirement can be discerned from the variously phrased prohibitions against the patenting of abstract ideas, laws of nature or natural phenomena" (emphasis added).

The recent expansion of the Internet and e-commerce has led to many patents being applied for and being granted for business methods implemented in software and the question of whether business methods are statutory subject matter is a separate issue from the question of whether software is. There have been several successful enforcement trials in the USA, some of which are listed in the list of software patents article.

Europe

Within European Union member states, the EPO and other national patent offices have issued many patents for inventions involving software since the European Patent Convention (EPC) came into force in the late 1970s. Article 52 EPC excludes "programs for computers" from patentability (Art. 52(2)) to the extent that a patent application relates to a computer program "as such" (Art. 52(3)). This has been interpreted to mean that any invention which makes a non-obvious "technical contribution" or solves a "technical problem" in a non-obvious way is patentable even if that technical problem is solved by running a computer program.

Computer-implemented inventions which *only* solve a business problem using a computer, rather than a technical problem, are considered unpatentable as lacking an inventive step. Nevertheless, the fact that an invention is useful in business does not mean it is not patentable if it also solves a technical problem.

United Kingdom

United Kingdom patent law is interpreted to have the same effect as the European Patent Convention such that "programs for computers" are excluded from patentability to the extent that a patent application relates to a computer program "as such". Current case law in the UK states that an (alleged) invention will only be actually regarded as an invention if it provides a contribution that is not excluded and which is also technical. A computer program implementing a business process is therefore not an invention, but a computer program implementing an industrial process may well be.

Japan

Software-related inventions are patentable. To qualify as an invention, however, there must be "a creation of technical ideas utilizing a law of nature" although this requirement is typically met by "concretely realising the information processing performed by the

software by using hardware resources". Software-related inventions may be considered obvious if they involve: the application of an operation known in other fields; the addition of a commonly known means or replacement by equivalent; the implementation in software of functions which were previously performed by hardware; or the systematisation of known human transactions.

Other countries

In India, a clause to include software patents was quashed by the Indian Parliament in April 2005.

In Australia, pure or abstract methods of doing business are not considered to be patentable, but if the method is implemented using a computer, it avoids the exclusion for business methods.

In New Zealand computer programs are to be excluded from patentability under a 2010 Patents Bill, but guidelines permitting embedded software are to be drafted once the bill has passed.

In the Philippines, "schemes, rules and methods of performing mental acts, playing games or doing business, and programs for computers" are non-patentable inventions under Sec. 22.2 of Republic Act No. 8293, otherwise known as the "Intellectual Property Code of the Philippines."

In South Korea, software is considered patentable and many patents directed towards "computer programs" have been issued. In 2006, Microsoft was ordered to halt sales of its "Office" suite due to a patent infringement ruling by the Supreme Court of Korea. The company was found to have infringed upon patents directed towards automatic language translation within software programs.

Patentable subject matter

Patents are intended to promote innovation by encouraging the timely disclosure of how to make and use inventions and by protecting investments made to commercialize inventions. They attempt to accomplish this by requiring that a prompt and full disclosure is made by an inventor of how to make and use the invention and by granting a monopoly right for a limited period of time to a patent owner to prevent others from making, using or selling the invention in exchange for said prompt and full disclosure.

There is debate as to whether or not these aims are achieved with software patents.

Proposals

In seeking to find a balance, different countries have different policies as to where the boundary between patentable and non-patentable software should lie. In Europe, a number of different proposals for setting a boundary line were put forward during the

debate concerning the proposed Directive on the patentability of computer-implemented inventions, none of which were found acceptable by the various parties to the debate. Two particular suggestions for a hurdle that software must pass to be patentable include:

- A computer program that utilises "controllable forces of nature to achieve predictable results".
- A computer program which provides a "technical effect".

In the US, Ben Klemens, a Guest Scholar at the Brookings Institution, proposed that patents should be granted only to inventions that include a physical component that is by itself nonobvious. This is based on Justice William Rehnquist's ruling in the U.S. Supreme Court case of Diamond v. Diehr that stated that "... insignificant postsolution activity will not transform an unpatentable principle into a patentable process." By this rule, one would consider software loaded onto a stock PC to be an abstract algorithm with obvious postsolution activity, while a new circuit design implementing the logic would likely be a nonobvious physical device. Upholding an "insignificant postsolution activity" rule as per Justice Rehnquist's ruling would also eliminate most business method patents.

Obviousness

A common objection to software patents is that they relate to trivial inventions. A patent on an invention that many people would easily develop independently of one another should not, it is argued, be granted since this impedes development. Different countries have different ways of dealing with the question of inventive step and non-obviousness in relation to software patents.

Inventive step test in Europe

Perceived negative effects

Compatibility

There are a number of high profile examples where the patenting of a data exchange standards forced another programming group to introduce an alternative format. For instance, the PNG format was largely introduced to avoid the GIF patent problems, and Ogg Vorbis to avoid MP3. If it is discovered that these new suggested formats are themselves covered by existing patents, the final result may be a large number of incompatible formats. Creating such formats and supporting them costs money, creates inconvenience to users and even threatens to split the Internet into several partially incompatible sub-networks (ASF and non-ASF, for example).

Conflicts

Computer-implemented invention (CII)

A microsite of the EPO website states that a generally accepted and widely used definition of a CII is "an invention whose implementation involves the use of a computer, computer network or other programmable apparatus, the invention having one or more features which are realised wholly or partly by means of a computer program." A similar definition is provided by The Guidelines for Examination at the EPO.

The EPO, in contrast, deny that they grant software patents. They further argue that the term *software patent* is itself a misleading concept since it could imply that an invention must be in the form of software to count as a CII. The case law of the EPO and various national courts in Europe states that a computer program cannot be patented in the guise of an object or as hardware if the underlying invention is still a computer program as such. *Computer-implemented invention* also covers inventions relating to computer control of processes external to a computer, such as anti-lock braking systems (ABS). Such inventions are not caught by many definitions of *software patent*, such as the one proposed by the FFII.

Additionally, the EPO do not grant patents to all computer-implemented inventions since they must still provide a technical solution to a technical problem to be viewed as being inventive, whereas the term software patent implies a granted patent. Nevertheless, the fact that the EPO deem that many software-related patent applications describe inventions is a point of contention.

Overlap with copyright

Protection by patent protection and copyright constitute two different means of legal protection which may cover the same subject-matter, such as computer programs, since each of these two means of protection serves its own purpose. Software is protected as works of literature under the Berne Convention. This allows the creator to prevent another entity from copying the program and there is generally no need to register code in order for it to be copyrighted.

Patents, on the other hand, give their owners the right to prevent others from using a claimed invention, even if it was independently developed and there was no copying involved. In fact, one of the most recent EPO decisions T 424/03 clarifies the distinction, stating that software is patentable, because it is basically only a technical method executed on a computer, which is to be distinguished from the program itself for executing the method, the program being merely an expression of the method, and thus being copyrighted.

Patents cover the underlying methodologies embodied in a given piece of software, or the function that the software is intended to serve, independent of the particular language or code that the software is written in. Copyright prevents the direct copying of some or all

of a particular version of a given piece of software, but do not prevent other authors from writing their own embodiments of the underlying methodologies. Copyright can also be used to prevent a given set of data from being copied while still allowing the author to keep the contents of said set of data a trade secret.

Whether and how the numerus clausus principle shall apply to the legal hybrid software to provide a judicious balance between property rights of the title holders and freedom rights of computing professionals and the society as a whole, is in dispute.

Free and open source software

There is tremendous animosity and disgust in the free software community towards software patents. Much of this has been caused by free software or open source projects shutting down when the holders of patents covering aspects of a project demanded license fees that the project could not or was not willing to pay or offered licenses under terms which the project was unwilling to accept, or could not accept because it conflicted with the free software licence in use.

Several patent holders have offered royalty-free patent licenses. Companies that have done this include Apple Inc, IBM, Microsoft, Nokia, Novell, Red Hat, Sun Microsystems and Unisys. Such actions have rarely appeased the free and open source software communities for reasons such as fear of the patent holder changing their mind or problems with some of the license terms.

In 2005 Sun Microsystems announced that they were making a portfolio of 1,600 patents available through a patent license called Common Development and Distribution License.

In 2006, Microsoft's patent pledge not to sue Novell Linux customers, openSUSE contributors, and free/open source software developers and the associated collaboration agreement with Novell was met with disdain from the Software Freedom Law Center while commentators from the Free Software Foundation stated that the agreement would not comply with GPLv3.

Draft versions of the GNU GPL version 3 may also conflict with patents on software by preventing any patent holder from enforcing their patents against a user if said patent holder also distributes software covered by those patents under the GPL.

Unisys case

In the late 1990s, Unisys claimed to have granted royalty free licenses to hundreds of not-for-profit organizations that used the patented LZW compression method and, by extension, the GIF image format. However, this did not include most software developers and Unisys were "barraged" by negative and "sometimes obscene" emails from software developers.

Jurisdictions

Substantive law regarding the patentability of software and computer-implemented inventions, and case law interpreting the legal provisions, are different under different jurisdictions.

Software patents under multilateral treaties:

- Software patents under TRIPs Agreement
- Software patents under the European Patent Convention
- Computer programs and the Patent Cooperation Treaty

Software patents under national laws:

- Software patents under United States patent law
- Software patents under United Kingdom patent law

Litigation

Several successful litigations show that software patents are enforceable in the US.

Similarly in Japan, software patents have been successfully enforced. In 2005, for example, Matsushita won a court order barring Justsystem from infringing Matsushita's Japanese patent 2,803,236 covering word processing software. A Tokyo court ordered Justsystem to pull their product from the market. On September 30, 2005, Intellectual Property High Court of Japan, which was established in April 2005, granted Justsystems' appeal and overturned the Tokyo District Court decision in October 2005.

Licensing

US Class	Description	Total Patents Issued
700	Data Processing: Generic Control Systems or Specific Applications	10716
701	Data Processing: Vehicles, Navigation, and Relative Location	11453
702	Data Processing: Measuring, Calibrating, or Testing	9662
703	Data Processing: Structural Design, Modeling, Simulation, and Emulation	2759
704	Data Processing: Speech Signal Processing, Linguistics, Language Translation, and Audio Compression/Decompression	6399
705	Data Processing: Financial, Business Practice, Management, or Cost/Price Determination	5350
706	Data Processing: Artificial Intelligence	2505
707	Data Processing: Database and File Management or Data Structures	9966
708	Electrical Computers: Arithmetic Processing and Calculating	6383
709	Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring or Plural Processor Synchronization	9665
710	Electrical Computers and Digital Data Processing Systems: Input/Output	11092
711	Electrical Computers and Digital Processing Systems: Memory	11251
712	Electrical Computers and Digital Processing Systems: Processing Architectures and Instruction Processing (e.g., Processors)	5956
713	Electrical Computers and Digital Processing Systems: Support	7636
714	Error Detection/Correction and Fault Detection/Recovery	13896
715	Data Processing: Presentation Processing of Document, Operator Interface Processing, and Screen Saver Display Processing	6705
716	Data Processing: Design and Analysis of Circuit or Semiconductor Mask	4083
717	Data Processing: Software Development, Installation, and Management	3340
718	Electrical Computers and Digital Processing Systems: Virtual Machine Task or Process Management or Task Management/Control	1402
719	Electrical Computers and Digital Processing Systems: Interprogram Communication or Interprocess Communication (Ipc)	1209
720	Dynamic Optical Information Storage or Retrieval	1851
725	Interactive Video Distribution Systems	2345

Total US software patents by class of invention as of 2004

Patenting software is widespread in the US. As of 2004, approximately 145,000 patents had issued in the 22 classes of patents covering "computer implemented inventions". (see table above).

Many software companies cross license their patents to each other. These agreements allow each party to practice the other party's patented inventions without the threat of being sued for patent infringement. Microsoft, for example, has agreements with IBM, Sun Microsystems, SAP, Hewlett-Packard, Siemens AG, Cisco, Autodesk and recently

Novell. Microsoft cross-licensed its patents with Sun, despite being direct competitors, and with Autodesk even though Autodesk has far fewer patents than Microsoft.

The ability to negotiate cross licensing agreements is a major reason that many software companies, including those providing open source software, file patents. As of June 2006, for example, Red Hat has developed a portfolio of 10 issued US patents, 1 issued European patent, 163 pending US patent applications, and 33 pending international PCT (Patent Cooperation Treaty) patent applications. Red Hat uses this portfolio to cross license with proprietary software companies so that they can preserve their freedom to operate.

Many software patent holders license their patents in exchange for monetary royalties. Some patent owners, such as IBM, are in the business of selling the products they patent and view licensing as a way to increase the return on their investment in innovation. IBM generates an additional $US 2 billion per year by licensing.

Other patent holders are in the business of inventing new "computer implemented inventions" and then commercializing the inventions by licensing the patents to other companies that manufacture the inventions. Walker Digital, for example, has generated a large patent portfolio from its research efforts, including the basic patent on the Priceline.com reverse auction technology. US universities also fall into this class of patent owners. They collectively generate about $1.4 billion per year through licensing the inventions they develop to both established and start up companies in all fields of technology, including software.

Still other patent holders focus on obtaining patents from original inventors and licensing them to companies that have introduced commercial products into the marketplace after the patents were filed. Some of these patent holders, such as Intellectual Ventures, are privately held companies financed by large corporations such as Microsoft, Intel, Google, etc. Others, such as Acacia Technologies, are publicly traded companies with institutional investors being the primary shareholders.

The practice of acquiring patents merely to license them is controversial in the software industry. Companies that have this business model are pejoratively referred to as patent trolls. It is an integral part of the business model that patent licensing companies sue infringers that do not take a license. Furthermore, they may take advantage of the fact that many companies will pay a modest license fee (e.g.$100,000 to $1,000,000) for rights to a patent of questionable validity, rather than pay the high legal fees ($2,000,000 on up) to demonstrate in court that the patent is invalid.

Chapter 8

Software Patents under United States Patent Law

Software or computer programs are not explicitly mentioned in United States patent law. In the face of new technologies, decisions of the United States Supreme Court and United States Court of Appeals for the Federal Circuit (CAFC) in the latter part of the 20th century sought to redefine the boundary between patent-eligible and patent-ineligible subject matter, in a way that seemed to deviate from Supreme Court precedent. These CAFC decisions for at least a time resulted in a regime in the United States more open to the patenting of software than that of other countries. More recent decisions of the CAFC, however, such as In re Bilski, seem to indicate a return to the patent-eligibility law of the 1970s and early 1980s, which were dominated by the Supreme Court's patent-eligibility trilogy, taking a more limited view of what kind of technological advance could be patented, based on pre-computer precedents going back to the mid-19th century.

Law

Section 101 of title 35, United States Code, provides:

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

History

In the late 1960s and early 1970s, the USPTO and the United States Court of Customs and Patent Appeals (CCPA) were at odds over the patent-eligibility of technical advances whose departure from the prior art was only in the use of a software algorithm. The USPTO rejected such claims and declined to patent them, but the CCPA repeatedly reversed the USPTO's rulings and ordered the issuance of patents. The USPTO's position was hampered during the 1960s by the uncertainty over whether the Supreme Court could review decisions of the CCPA, because it was unclear whether it was an Article III court. That question was resolved, however, in *Brenner v. Manson*, in which the Court held that it had *certiorari* jurisdiction to review CCPA decisions. That decision also began a string of decisions in which the Supreme Court reversed decisions of the CCPA, and then its

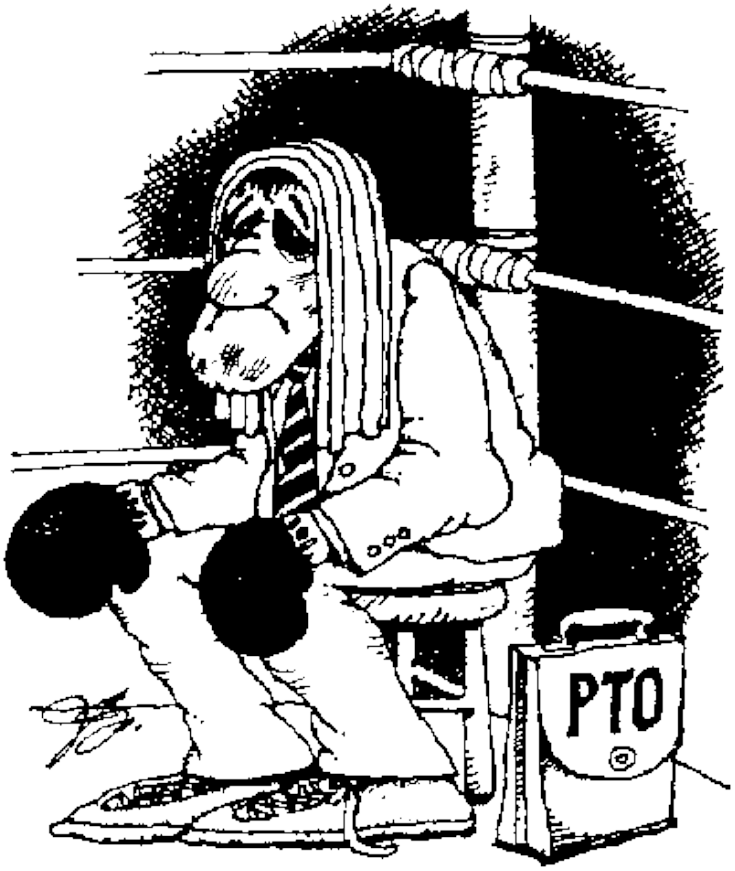
successor court the United States Court of Appeals for the Federal Circuit (CAFC), which had reversed decisions of the USPTO denying a patent to an applicant.

In the first of the Supreme Court's computer software decisions (the "patent-eligibility trilogy"), *Gottschalk v. Benson*, the Court reversed the CCPA's reversal of a USPTO decision denying a patent on an algorithm for converting binary-coded decimal numbers into pure binary numbers. In so ruling, the Court looked back to 19th century decisions such as *O'Reilly v. Morse*, which held that abstract ideas could not be made the subject of patents. The Court's 1978 ruling in *Parker v. Flook*, was similar in principle. These cases also established that the "clue" to whether a patent might be granted on a process was whether the process was carried out with a particular apparatus or else effectuated a transformation of an article from one state or thing to another state or thing. In *Flook*, where the sole departure from the prior art was concededly the formula or algorithm, no transformation was alleged, and it was conceded that the implementing apparatus was old or conventional, the process was simply not the kind of process that could be patented.

In the 1981 case of *Diamond v. Diehr*, the United States Supreme Court upheld the CCPA's reversal of the USPTO, and ordered the grant of a patent on an invention, a substantial part of which involved use of a computer program which used a well-known formula (the Arrhenius Equation) for calculating the time when rubber was cured and the mold could therefore be opened. The Supreme Court stated that in this case, the invention was not merely a mathematical algorithm, but a process for molding rubber, which was therefore patentable. In the *Diehr* case, there was no concession that the implementation was conventional, and the process did effectuate a transformation of substances (from uncured rubber to cured rubber).

After this point, more patents on software began to be granted, albeit with conflicting and confusing results. After its creation in 1982, the CAFC charted a course that tried to follow the *Diehr* precedent. Patents were allowed only if the claim included some sort of apparatus, even rather nominal apparatus at times, such as an analog-to-digital converter front end, or in one case a scratch-pad memory for storing intermediate data. A representative decision from this period is *In re Schrader*, in which the CAFC set forth probably its best and most detailed formulation of the rule it was attempting to follow.

Dissatisfaction with the perceived artificiality of this rule erupted, however, in rulings beginning with the en banc 1994 decision in *In re Alappat*, in which the CAFC majority held that a novel algorithm combined with a trivial physical step constitutes a novel physical device. Therefore, a computing device on which is loaded a mathematical algorithm is a "new machine", which is patentable. This ruling was followed up in *In re Lowry*, which held that a data structure representing information on a computer's hard drive or memory is similarly to be treated as a patent-eligible physical device. Finally, in *State Street Bank v. Signature Financial Group*, the CAFC ruled that a numerical calculation that produces a "useful, concrete and tangible result", such as a price, is patent-eligible.



"The USPTO gets ready to throw in the towel", cartoon published in IEEE Micro in 1994-1995(?)

The USPTO's reaction to this change was, for the time being at least, to "throw in the sponge." The Clinton administration appointed Bruce Lehman as Commissioner of the USPTO in 1994. Unlike his predecessors, Lehman was not a patent lawyer but the chief lobbyist for the Software Publishing Industry. In 1995, the USPTO established some broad guidelines for examining and issuing software patents. The USPTO interpreted the courts as requiring the USPTO to grant software patents in a broad variety of circumstances. Although the U.S. Congress has never legislated specifically that software is patentable, the broad description of patentable subject in the Patent Act of 1952 and the failure of Congress to change the law after the CAFC decisions allowing software patents, was interpreted as an indication of Congressional intent. The reaction of the defeated-feeling USPTO was characterized in the cartoon shown at right, which appeared in IEEE Micro at this time.

The United States Supreme Court remained silent on these decisions and developments for years. The first response appeared in a dissenting opinion in *LabCorp v. Metabolite, Inc* (2006). Although *certiorari* had been granted, the Court dismissed it as improvidently granted; the minority argued that the question of statutory subject matter in patent law should be addressed. Justice Breyer's dissent stated:

"[State Street] does say that a process is patentable if it produces a 'useful, concrete, and tangible result.' But this Court has never made such a statement and, if taken literally, the statement would cover instances where this Court has held the contrary."

He continues to directly address the claim that software loaded onto a computer is a physical device:

"...And the Court has invalidated a patent setting forth a process that transforms, for computer-programming purposes, decimal figures into binary figures-even though the result would seem useful, concrete, and at least arguably (within the computer's wiring system) tangible."

At about the same time, in a concurring opinion in *eBay Inc. v. MercExchange, L.L.C.*, Justice Kennedy (joined by Justices Stevens, Souter, and Breyer)questioned the wisdom of permitting injunctions in support of "the burgeoning number of patents over business methods," because of their "potential vagueness and suspect validity" in some cases.

This was followed by the decision of the CAFC in *In re Bilski*, which has opened a new chapter in this history. In *Bilski*, as the article on that case explains, the CAFC superseded *State Street* and related decisions with a return to the tests of the patent-eligibility trilogy, although while those decisions had merely treated the machine-or-transformation test as the clue to past decisions the CAFC now made that test dispositive.

Landmark decisions

Diamond v. Diehr

Diamond v. Diehr, 450 U.S. 175 (1981), was a 1981 U.S. Supreme Court decision which held that the execution of a physical process, controlled by running a computer program was patentable. The high court reiterated its earlier holdings that mathematical formulas in the abstract could not be patented, but it held that the mere presence of a software element did not make an otherwise patent-eligible machine or process un-patentable. *Diehr* was the third member of a trilogy of Supreme Court decisions on the patent-eligibility of computer software related inventions.

Background

The problem and its solution

The inventors, respondents, filed a patent application for a "[process] for molding raw, uncured synthetic rubber into cured precision products." The process of curing synthetic rubber depends on a number of factors including time, temperature and thickness of the mold. Using the Arrhenius equation --

$k = Ae^{-E_a/RT}$, which may be restated as $ln(v)=CZ+x$ --

it is possible to calculate when to open the press and to remove the cured, molded rubber. The problem was that there was, at the time the invention was made, no disclosed way to obtain an accurate measure of the temperature without opening the press.

The invention solved this problem by using embedded thermocouples to constantly check the temperature, and then feeding the measured values into a computer. The computer then used the Arrhenius equation to calculate when sufficient energy had been absorbed so that the molding machine should open the press.

The claims

Independent claim 1 of the allowed patent is representative. It provides:

1. A method of operating a rubber-molding press for precision molded compounds with the aid of a digital computer, comprising:

- providing said computer with a data base for said press including at least, natural logarithm conversion data (ln), the activation energy constant (C) unique to each batch of said compound being molded, and a constant (x) dependent upon the geometry of the particular mold of the press,
- initiating an interval timer in said computer upon the closure of the press for monitoring the elapsed time of said closure,

- constantly determining the temperature (Z) of the mold at a location closely adjacent to the mold cavity in the press during molding,
- constantly providing the computer with the temperature (Z),
- repetitively performing in the computer, at frequent intervals during each cure, integrations to calculate from the series of temperature determinations the Arrhenius equation for reaction time during the cure, which is

  $\ln(v)=CZ+x$
  where v is the total required cure time,

- repetitively comparing in the computer at frequent intervals during the cure each said calculation of the total required cure time calculated with the Arrhenius equation and said elapsed time, and
- opening the press automatically when a said comparison indicates completion of curing.

Proceedings before Office and CCPA

The patent examiner rejected this invention as unpatentable subject matter under 35 U.S.C. 101. He argued that the steps performed by the computer were unpatentable as a computer program under *Gottschalk v. Benson*, 409 U.S. 63 (1972). The Board of Patent Appeals and Interferences of the USPTO affirmed the rejection. The Court of Customs and Patent Appeals (CCPA), the predecessor to the current Court of Appeals for the Federal Circuit, reversed, noting that an otherwise patentable invention did not become unpatentable simply because a computer was involved.

The U.S. Supreme Court granted the petition for certiorari by the Commissioner of Patents and Trademarks to resolve this question.

The Supreme Court's opinion

The court repeated its earlier holding that mathematical formulas in the abstract are not eligible for patent protection. But it also held that a physical machine or process which makes use of a mathematical algorithm is different from an invention which claims the algorithm, as such, in the abstract. Thus, if the invention as a whole meets the requirements of patentability—that is, it involves "transforming or reducing an article to a different state or thing"—it is patent-eligible, even if it includes a software component.

The reversal of the patent rejection was affirmed. But the Court carefully avoided overruling *Benson* or *Flook*. It did criticize the analytic methodology of *Flook*, however, by challenging its use of analytic dissection, based on *Neilson v. Harford*. The *Diehr* Court said, without citation of any supporting authority, that under section 101 the invention had to be considered as a whole.

The patent

The patent that issued after the decision was US 4344142, "Direct digital control of rubber molding presses." The patent includes 11 method claims, three of which are independent. All method claims relate to molding of physical articles.

Chapter 9

Software Patents under the European Patent Convention

The **patentability of software**, computer programs and computer-implemented inventions **under the European Patent Convention (EPC)** is the extent to which subject matter in these fields is patentable under the Convention on the Grant of European Patents of October 5, 1973. The subject also includes the question of whether European patents granted by the European Patent Office (EPO) in these fields (sometimes called "software patents") are regarded as valid by national courts.

Under the EPC, and in particular its Article 52, "programs for computers" are not regarded as inventions for the purpose of granting European patents, but this exclusion from patentability only applies to the extent to which a European patent application or European patent relates to a computer program as such. As a result of this partial exclusion, and despite the fact that the EPO subjects patent applications in this field to a much stricter scrutiny when compared to their American counterpart, that does not mean that all inventions including some software are *de jure* not patentable.

Article 52 of the European Patent Convention

The European Patent Convention (EPC), Article 52, paragraph 2, excludes from patentability, "in particular

1. discoveries, scientific theories and mathematical methods;
2. aesthetic creations;
3. schemes, rules and methods for performing mental acts, playing games or doing business, and **programs for computers**; [emphasis added]
4. presentations of information."

Paragraph 3 then says:

> "(3) The provisions of paragraph 2 shall exclude patentability of the subject-matter or activities referred to in that provision only to the extent to which a European patent application or European patent relates to such subject-matter or activities **as such**." (emphasis added)

The words "as such" have caused patent applicants, attorneys, examiners, and judges a great deal of difficulty since the EPC came into force in 1978. The Convention, as with all international conventions, should be construed using a purposive approach. However, the purpose behind the words and the exclusions themselves is far from clear.

An interpretation, which is followed by the Boards of Appeal of the EPO, is that an invention is patentable if it provides a new and non-obvious technical solution to a technical problem. The problem, and the solution, may be entirely resident within a computer such as a way of making a computer run faster or more efficiently in a novel and inventive way. Alternatively, the problem may be how to make the computer easier to use, such as in T928/03, Konami, Video Game System.

The position of the EPO can be contrasted with that of other patent offices with more liberal policies concerning the patenting of computer-implemented inventions such as the US Patent and Trademark Office and the Australian Patent Office. In these countries, the mere use of a computer is sufficient to make a business method patentable even if the computer is not being used in a novel or inventive way and only the underlying business method provides the patentable features. Such a position has been specifically rejected by the EPO in decisions such as T258/03 (Hitachi/Auction method).

Patentability under European Patent Office case law

Like the other parts of the paragraph 2, computer programs are open to patenting to the extent that they provide a technical contribution to the prior art. In the case of computer programs and according to the case law of the Boards of Appeal, a technical contribution typically means a *further technical effect* that goes beyond the normal physical interaction between the program and the computer.

Though many argue that there is an inconsistency on how the EPO now applies Article 52, the practice of the EPO is fairly consistent regarding the treatment of the different elements of Article 52(2). A mathematical method is not patentable, but an electrical filter designed according to this method would not be excluded from patentability by Article 52(2) and (3).

According to the jurisprudence of the Boards of Appeal of the EPO, a technical effect provided by a computer program can be, for example, a reduced memory access time, a better control of a robotic arm or an improved reception and/or decoding of a radio signal. It does not have to be external to the computer on which the program is run; reduced hard disk access time or an enhanced user interface could also be a technical effect.

Patentable subject-matter requirement

Some ten years before 2006, a shift occurs in the case law. The "contribution approach" or "technical effect approach", used to assess what was regarded as an invention within the meaning of Art. 52(1) and (2), was abandoned. According to the "contribution

approach", the claimed subject-matter did not concern an invention within the meaning of Article 52(1) EPC when no contribution was made in a field not excluded from patentability. The "contribution approach" was a disguised inventive step assessment.

Decisions such as T 258/03 and T 154/04 have made it clear that the contribution approach was no longer applicable. Indeed

The structure of the EPC (...) suggests that it should be possible to determine whether subject-matter is excluded under Article 52(2) EPC without any knowledge of the state of the art (including common general knowledge). (T 258/03, Reasons 3.1).

It now suffices that a physical entity or activity involves technical means to be considered as an invention within the meaning of Article 52(1) EPC. Having technical character is an implicit requisite of an "invention" within the meaning of Article 52(1) EPC (requirement of "technicality").

But the patentable subject matter test of Article 52(2) and (3) is only the first step towards patentability. Computer programs can also be refused and are often refused on the ground of lack of inventive step, which can be relatively easier to assess in certain cases. As a Board of appeal put it in T 258/03 (Reasons 4.6) in relation to the fact that the "contribution approach" was no longer applicable,

[we are] aware that [our] comparatively broad interpretation of the term "invention" in Article 52(1) EPC will include activities which are so familiar that their technical character tends to be overlooked, such as the act of writing using pen and paper. Needless to say, however, this does not imply that all methods involving the use of technical means are patentable. They still have to be new, represent a non-obvious technical solution to a technical problem, and be susceptible of industrial application.

Inventive step requirement

The interpretation of the term "invention" in the patentable subject-matter test, as used by the Boards of Appeal, has come with an adjustment of the case law relating to the inventive step requirement.

Any non-technical feature, i.e. a feature from a field excluded from patentability under Article 52(2) and (3) EPC, cannot be taken into account for the assessment of inventive step, unless they (the non-technical features) do interact with the technical subject-matter to solve a technical problem. Likewise, the "state of the art" (used as the starting point for the inventive step assessment) should be construed as meaning the "state of technology", the person skilled in the art is the person skilled in the relevant field of technology, and "for the purpose of the problem-and-solution approach, the problem must be a technical problem which the skilled person in the particular technical field might be asked to solve at the relevant priority date". Fields excluded under Art. 52(2) are not considered part of the technology for the assessment of inventive step.

Thus an expert in marketing or insurance policies for instance cannot be chosen as the fictional person skilled in the art, while a computer hardware or memory management expert may be chosen as the reference fictional person. This means that the mere implementation of a business method on a computer or computer network rarely involves an inventive step, while improving a computer-assisted industrial process or providing a more efficient memory management within a computer may involve an inventive step.

The case law of the EPO Boards of Appeal is not binding on the first instance departments of the EPO (i.e. the Examining Divisions), and different Examining Divisions of the EPO may assess patentability differently. Likewise, during an opposition procedure before the EPO, where the grant of a recently granted European patent may be opposed by a third party (opponent), the patent may be revoked if the Opposition Division form a different view on whether or not the invention in question was patentable.

Relevant decisions

Enforceability before national courts

The case law of the EPO Boards of Appeal is not binding on the EPO member states and different national courts acting on different cases may take a different view of patentability under Art. 52(2) EPC. Any European patent issued by the EPO may be revoked in a patent infringement lawsuit or revocation proceedings before a national court if for instance the court judges the invention as non-patentable in view of new prior art evidence or in view of a reconsideration of the available prior art.

UK

Peter Prescott QC, while sitting as a Deputy Judge in the UK High Court, and in consideration of *CFPH's applications* noted that the EPO decisions are prescriptive, but not binding on the UK courts, but also recalled the judgement of the Court of Appeal in *Fujitsu's application* which stated that it would be disastrous if there was any substantial divergence between the interpretations given by the UK courts and the EPO to Article 52(2) EPC.

The judgement in *CFPH's applications* was the first in a flurry of UK court cases since 2005 involving re-consideration by the High Court of patent applications refused by the UK Patent Office.

The two patent applications in question both involved networked interactive wagering on the outcomes of events. Each application was refused as relating to a method of doing business as such. The applications were not refused as relating to a computer program as such, because the computer program was simply a tool that was being used to implement a new set of business rules and the invention was not really about the computer program. Although the judgement stressed that the reasoning used was quite different from the type

that would have been applied by the EPO, the judge was satisfied that the EPO would have come to the same conclusion using their own reasoning.

The decision criticises the EPO's reliance on insisting that an invention must provide a technical contribution, and not merely a business based contribution. As evidenced by the judgment in *Dyson v Hoover* the commercial background to an invention may help to show that a certain technical advance was or was not obvious.

In *Research In Motion UK Ltd. v Inpro Licensing SARL*, the UK High Court had the opportunity to consider a patent that had been granted by the EPO. The patent involved the 'pretreating' of web pages before they were downloaded to machines of modest processing capacity. Mr Justice Pumfrey came to the conclusion that the claimed invention was obvious, but specifically rejected the allegation that it was excluded from patent protection as a computer program as such. He noted that "all modern industry depends upon programmed computers, and one must be astute not to defeat patents on the ground that the subject matter is excluded under Article 52 unless the invention lies in excluded subject matter *as such*" (emphasis added).

The UK Court of Appeal judgment in *Aerotel v Telco and Macrossan's Application* criticised EPO practice to deem non-technical subject matter, such as new music or a story, as part of the prior art as not being intellectually honest. The EPO Boards of Appeal have since responded by saying that the technical effect approach (with the rider) applied in the Aerotel/Macrossan judgement is irreconcilable with the European Patent Convention.

Germany

In Germany, in the case *Logikverifikation* (13 December 1999), the German Federal Court (German: *Bundesgerichtshof* or *BGH*) ruled on a case involving a national patent application claiming a computer-implemented invention, namely a "method for hierarchical logic verification of highly-integrated circuits". Going against the run of previous case law, it overruled the German Federal Patent Court (German: *Bundespatentgericht* or *BPatG*), and came to the conclusion that the claimed subject-matter did properly meet the 'technical' requirement, can not be excluded from patentability for that reason and that the court has to go into substantial examination. The question about the exclusion of "computer programs as such" [sic] was mentioned the first time, but set aside as the court did not see the need to determine that question.

BPatG objections were also overruled in the decisions *Sprachanalyseeinrichtung* (German BGH, 11 May 2000) and *Suche fehlerhafter Zeichenketten* (German BGH, 17 October 2001). In the civil law tradition of mainland Europe however, legal precedent does not necessarily acquire the same formally binding character that it assumes in the common law traditions typical of most English-speaking countries.

In fact, more recently the same court has repeatedly upheld the rejection of patent claims to computers and programs operating thereon, as in *Rentabilitätsermittlung* as well as in *Informationsübermittlungsverfahren*.

France

France was the first European nation that excluded **(French)** «les programmes ou séries d'instructions pour le déroulement des opérations d'une machine calculatrice» ("programs or series of instructions for the procession of operations of a calculating machine", i.e. computer programs) from being an industrial invention in 1968 in Loi n°68-1 Article 7. Two relevant decisions, namely *Mobil Oil Corp.*, and *SA SAGEM*, rejected the patentability for the reason of missing a technical character. In *Schlumberger*, it was decided that not any use of a computer program disallows patentability. In *Infomil*, the court declared that a claim for an information system always has technical character and is therefore protectible.

G 3/08

Under case number **G 3/08**, the Enlarged Board of Appeal of the EPO issued on May 12, 2010 an opinion in response to questions referred to it by the President of the European Patent Office (EPO), Alison Brimelow, on October 22, 2008. The questions subject of the referral related to the patentability of programs for computers under the European Patent Convention (EPC) and were, according to the President of the EPO, of fundamental importance as they related to the definition of "the limits of patentability in the field of computing." In a 55-page long opinion, the Enlarged Board of Appeal considered the referral to be inadmissible because no divergent decisions had been identified in the referral.

The referral had been quoted as relating to the "deeply contentious question about how to assess the patentability of software-related inventions". Alison Brimelow had been reported to have been considering referring the issue to the Enlarged Board of Appeal for almost two years.

Some amicus curiae briefs had anticipated that the referral would be considered inadmissible under the legal provisions of the EPC, and in particular Article 112(1)(b) EPC.

Background

In addition to the Boards of Appeal before which decisions of the first instances of the EPO can be contested, the EPO includes an Enlarged Board of Appeal. This board does not constitute an additional level of jurisdiction in the classical sense. This instance takes decisions only when the case law of the Boards of Appeal becomes inconsistent or when an important point of law arises. Its purpose is "to ensure uniform application of the law" and to clarify or interpret important points of law in relation to the European Patent Convention. Only the Boards of Appeal themselves and the President of the EPO can

refer a question to the Enlarged Board of Appeal. In the first case, the Enlarged Board issues a decision, while in the latter case it issues an opinion. G 3/08 is a referral of the President of the EPO under Article 112(1)(b) EPC.

Under Article 52(2)(c) EPC, the patentability of programs for computers is excluded. However, Article 52(3) EPC provides that this exclusion only applies to the extent to which a European patent application or European patent relates to such programs for computers "as such". The interpretation of the exclusion, including the words "as such", have caused applicants, attorneys, examiners, and judges a great deal of difficulty since the EPC came into force in 1978. An interpretation, which is followed by the Boards of Appeal of the EPO, is that an invention is patentable if it provides a new and non-obvious technical solution to a technical problem.

Referrals to the Enlarged Board of Appeal are said to be rare, happening only with the most complex questions. The patentability of software has provoked fierce debate in Europe over the recent years, especially in relation to the proposed European Union (EU) directive on the patentability of computer-implemented inventions. The directive was rejected in 2005 by the European Parliament, a decision that was welcomed by those on both sides of the debate, by those supporting the patentability of software in Europe as well as those opposing it.

Questions

Four questions have been referred by the President of the EPO to the Enlarged Board of Appeal. The four questions have been chosen to look at four different aspects of patentability in the field of computer programs.

Question 1: Claim category

Can a computer program only be excluded as a computer program as such if it is explicitly claimed as a computer program?

A divergence between decisions T 1173/97, making no distinction between categories of claims, especially between computer-implemented claims and computer program claims, and T 424/03, making a distinction between these two categories, is cited as justifying this question.

Question 2: Claim as a whole

(a) Can a claim in the area of computer programs avoid exclusion under Art. 52(2)(c) and (3) merely by explicitly mentioning the use of a computer or a computer-readable data storage medium?
(b) If question 2(a) is answered in the negative, is a further technical effect necessary to avoid exclusion, said effect going beyond those effects inherent in the use of a computer or data storage medium to respectively execute or store a computer program?

A divergence between decisions T 1173/97 and T 258/03 is cited as justifying this question. Under T 1173/97, computer programs are methods, and in order to have a technical character computer programs must demonstrate a further technical effect (which goes beyond the "normal" physical interactions between program (software) and computer (hardware)). Under T 258/03, a method acquires a technical character simply by involving technical means.

Question 3: Individual features of a claim

(a) Must a claimed feature cause a technical effect on a physical entity in the real world in order to contribute to the technical character of the claim?
(b) If question 3 (a) is answered in the positive, is it sufficient that the physical entity be an unspecified computer?
(c) If question 3 (a) is answered in the negative, can features contribute to the technical character of the claim if the only effects to which they contribute are independent of any particular hardware that may be used?

A divergence between, on the one hand, decisions T 163/85 and T 190/94, according to which a technical effect on a physical entity in the real world is required (to escape the exclusion under Article 52(2)(c) and (3)), and, on the other hand, T 125/01 and T 424/03, according to which the technical effects can be essentially confined to the respective computer programs, is cited as justifying this question.

Question 4: The activity of programming

(a) Does the activity of programming a computer necessarily involve technical considerations?
(b) If question 4 (a) is answered in the positive, do all features resulting from programming thus contribute to the technical character of a claim?
(c) If question 4 (a) is answered in the negative, can features resulting from programming contribute to the technical character of a claim only when they contribute to a further technical effect when the program is executed?

A divergence between decisions considering that a programmer's activity, i.e. writing computer programs, falls within the exclusions of Article 52(2)(c) (T 833/91, T 204/93, and T 769/92) and decisions having taken the opposite view (T 1177/97 and T 172/03) is cited as justifying the question.

*Statements by third parties (*Amicus curiae *briefs)*

On November 11, 2008, the Enlarged Board of Appeal decided to announce in the Official Journal of the EPO "further provisions concerning statements by third parties on the points of law concerning the patentability of programs for computers referred to it by the President of the European Patent Office". The expected announcement was made in the Official Journal of January 2009. Namely, any written statements, i.e. amicus curiae briefs, had to be filed by the end of April 2009.

Around a hundred amicus curiae briefs have been submitted, including briefs by Accenture, the Association for Competitive Technology (ACT), the American Intellectual Property Law Association (AIPLA), the International Association for the Protection of Industrial Property (AIPPI), Apple Inc., BT, BUSINESSEUROPE, Canonical Group Ltd, the Computer & Communication Industry Association (CCIA), Chartered Institute of Patent Attorneys (CIPA), the Computing Technology Industry Association (CompTIA), DIGITALEUROPE, Ericsson, the European Patent Institute (epi), the Foundation for a Free Information Infrastructure (FFII), the Free Software Foundation Europe (FSFE), the International Federation of Intellectual Property Attorneys (FICPI), France Télécom, IBM, the Irish Free Software Organisation (IFSO), ITechLaw, the Japan Intellectual Property Association (JIPA), Prof. Donald Knuth, Licensing Executives Society International (LESI), Microsoft Corporation and General Electric Company, Philips, the Pirate Party, Pitney Bowes, the Polish Patent Office, Red Hat, SAP, Siemens, Prof. Joseph Straus, the UNION of European Practitioners in Industrial Property, and the United Kingdom.

Reception to the referral and further developments

According to the *New York Times*, the referral has been welcomed "by lawyers and software engineers alike".

After the referral, the England and Wales Court of Appeal did not give the UK Intellectual Property Office (UK-IPO) leave to appeal to the House of Lords regarding the *Symbian's Patent Application* case, "because in its view it would be premature for the House of Lords to decide what computer programs are patentable before the issue has been considered by the Enlarged Board of Appeal of the [EPO]."

Interlocutory decision of 16 October 2009

In an interlocutory decision of 16 October 2009, the Enlarged Board of Appeal dealt with an objection of partiality raised in an amicus brief. The objection of partiality was against a particular member of the Board, Dai Rees, and against the Board as a whole. The Enlarged Board of Appeal concluded that there was "no reason to exclude Mr Rees from its composition in case G 3/08 or to replace further members." The original composition of the Board therefore remained unchanged.

Opinion

The reasons for the opinion first address the admissibility of the referral. After considering that the President of the EPO had not forfeited her right to a referral because the preceding President, Alain Pompidou, had declined in 2007 to refer questions to the Enlarged Board Appeal (when suggested to do so by British judge Lord Justice Jacob), the Board considered the referred questions to be undoubtedly of fundamental importance under Article 112(1)(b) EPC. The Board goes on by writing that the president's right of referral to the Enlarged Board does not extend to means of replacing Board of Appeal rulings with the decision of a putatively higher instance, as Article 112 EPC / Article

112a EPC does not constitute a further instance ranking above the Boards of Appeal within the EPC judicial system. According to the Board, "[the EPO's Boards of Appeal] are ... assigned interpretative supremacy with regard to the EPC in terms of its scope of application". The notion of "legal development" and its normal character are also addressed, in the context of the reference to "different decisions" in Article 112(1)(b) EPC, a requirement considered crucial for the referral to be admissible. The Board then concludes its "fundamental considerations on the interpretation of Article 112(1)(b) EPC" (before considering the questions of the referral themselves) as follows:

"the President [of the European Patent Office] has no right of referral under Article 112(1)(b) EPC simply in order to intervene, on whatever grounds, in mere legal development if on an interpretation of the notion of "different decisions" in the sense of conflicting decisions there is no need for correction to establish legal certainty.

First reactions

Justine Pila argued that the basis for this decision is an interpretation of Article 112(1)(b) that is inconsistent with the principles of Articles 31 and 33 of the Vienna Convention, and that it offends the constitutional principles from which it was expressly derived. Namely she critizises that the Boards' approach

1. suffers from the same faulty logic for which the EBA criticized the President's referral,
2. lacks doctrinal and theoretical coherence, and
3. is incapable of producing legal certainty, either within the EPC or national (European) patent systems.

She concluded by criticizing the opinion, stating notably that "the EBA [had] rendered a decision that is higher on democratic language than democratic content" and that "the only hope is for the European or national Legislatures to recognize that "judiciary-driven legal development" within the EPO has indeed met its limits".

Proposed Directive on the Patentability of Computer-Implemented Inventions

The **Proposal for a Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions** (Commission proposal COM(2002) 92, procedure number 2002/0047 (COD)) was a proposal for a European Union (EU) directive aimed to harmonise national patent laws and practices concerning the granting of patents for computer-implemented inventions, provided they meet certain criteria.

The proposal became a major focus for conflict between those who regarded the proposed directive as a way to codify the case law of the Boards of Appeal of the European Patent Office (unrelated to the EU institutions) in the sphere of computing, and those who asserted that the directive is an extension of the patentability sphere, not just a

harmonisation, that ideas are not patentable and that the expression of those ideas is already adequately protected by the law of copyright.

Following several years of debate and numerous conflicting amendments to the proposal, the proposal was rejected on 6 July 2005 by the European Parliament by an overwhelming majority of 648 to 14 votes.

History

Original draft

On 20 February 2002, the European Commission initiated a proposal for a directive to codify and "harmonise" the different EU national patent laws and cement the practice of the European Patent Office of granting patents for computer-implemented inventions provided they meet certain criteria (cf. software patents under the European Patent Convention). The directive also took on the role of excluding "business methods" from patentability (in contrast with the situation under United States law), because business methods as such are not patentable under the different European national patent laws or under the European Patent Convention.

Opponents of the original directive claimed that it was a thinly disguised attempt to make all software patentable. Supporters, however, argued that this was not the case since the proposal explained in several locations (pages 11, 14, 24, 25) that there should be no extension to the existing scope of patentability for computer programs and that pure business methods implemented in software would not be patentable. Only computer programs which provided a "technical contribution" would be patentable.

This reliance on the word "technical" was an important weakness in the directive, since it is not a word that has a well-defined meaning, and a "technical contribution" was only defined as being "a contribution to the state of the art in a technical field which is not obvious to a person skilled in the art." Nevertheless, the term has been used as a benchmark for what is and is not patentable by the European Patent Office and by individual national Patent Offices and courts in Europe (particularly the United Kingdom and Germany) since the early 1980s. A general understanding of its meaning can be gleaned from studying the resulting case law, summarised in Software patents under the European Patent Convention. The subsequent failure of the European Parliament to develop an acceptable definition of what was meant by the word technical illustrates the difficulty inherent in attempting to do so.

Transformation by the European Parliament

On 24 September 2003, the European Parliament passed the directive in a heavily amended form, which placed significant limits on the patentability of software. The most significant changes included:

- a definition of the "technicity" requirement for patentability which distinguishes between abstract information-processing processes and specific kinds of physical processes (only the latter are "technical");
- a blanket rule that patents cannot be used to prevent interoperability between computer systems.

Patent attorney Axel H. Horns, however, voiced concern that Parliament's wording might extend the ban on software patents to inventions potentially implementable in software, such as signal processing equipment.

Politically, these amendments were supported almost unanimously by small parties on both the right and left, while the larger groupings (socialists, liberals and conservatives) were all split, with the balance of socialists leaning in favour of amendment and the balance of conservatives leaning against.

Parliament's amendments were a major defeat for the directive's original proponents. Rather than confirming the practice of granting patents for computer programs which provide a technical contribution, the revised directive placed substantial limits on patentability.

Reversion by the Council of Ministers

Under the codecision procedure, both the European Parliament and the Council of Ministers (representing national Governments) must approve a text in identical terms in order for a proposal to become law. On 18 May 2004, the Council agreed in an advisory vote to resubmit to Parliament what was described as a "compromise version" of the proposal. The agreed version permitted patenting of computer-implemented inventions (providing the inventions have a "technical character") and overturned most of Parliament's amendments. Critics of the Directive argued that the "technical character" requirement was open to too much interpretation and could lead to almost unlimited patentability of software. Proponents, also, felt that the amended version contained too many ambiguities to be capable of meeting the original purpose of the Directive, which was to harmonise the law across Europe. Nevertheless, the Council formally approved this resolution on 7 March 2005. The revised proposal was resubmitted to Parliament.

Developments between first Parliament decision and Council decision

Subsequently, in an unprecedented move, the Dutch national parliament passed a motion requesting that the nation's ministerial representative on the Council, Laurens Jan Brinkhorst, change his vote on the Council's version of the directive, from "in favour" to abstention. Brinkhorst stated that he would not do this. The Council's confirmation (or otherwise) of its President's "compromise" had also been delayed.

The Polish government announced on 16 November, 2004, that it could not "support the text that was agreed upon by Council on 18 May 2004". A joint press release by the FFII,

the Internet Society Poland, and NoSoftwarePatents.com, supported the concerns of opponents of the Council directive, stating:

at a meeting hosted by the Polish government on the 5th of this month, everyone including representatives of the Polish Patent Office, SUN, Novell, Hewlett-Packard and Microsoft, as well as various patent lawyers, confirmed that the present proposal of the EU Council does make all software potentially patentable.

On 7 December 2004, the Belgian Minister of Economic Affairs, Marc Verwilghen, stated that no Council decision would be taken until 2005 "for the reason that the qualified majority does not exist anymore". However, amid rumours of a change in the Polish position, the 13-15 December meeting of the Council's Committee of Permanent Representatives determined that a qualified majority appeared to exist, and that the Council's revised version of the directive would be scheduled for formal adoption by the Council, without further debate, probably at the Agricultures and Fisheries Council meeting on the 21st and 22 December 2004.

Statements expressing reservations were attached to this Common Position by Belgium (which abstained), France (which hoped for further changes to the directive), the Netherlands (where the parliament requested their representative vote against), Poland (which was opposed until recent diplomatic pressure), Hungary and Latvia. Germany was ambivalent, saying that the text of the directive could benefit from improvements.

Due to the expressed reservations and especially to opposition from Poland, whose Minister of Science and Information Technology made a special journey to Brussels to demand that the directive be dropped from the agenda, the Council's vote was postponed "indefinitely".

Meanwhile, a group of 61 MEPs from 13 countries tabled a "motion for a resolution" to restart the entire legislative process. On 2 February 2005, JURI, the Legal Affairs Committee of the European Parliament, voted 19-1 in favour of asking the Commission to withdraw the directive and restart the process.

The next day, Nicolas Schmit, deputy foreign minister of Luxembourg (which at that time chaired the Council), said that he would instead ask the Council to formally adopt the draft directive at a meeting on 17 February. Although Poland stated it would only oppose this if other countries raised an objection, reports of opposition from Denmark, the Netherlands and Spain ensured that the common position was not on the agenda for that meeting of the Commission.

On 17 February, Parliament's Conference of Presidents (the President of the Parliament and the leaders of the political groups) approved JURI's request to restart the process, and agreed to pass the request to the European Commission. On 24 February, a plenary session of the European Parliament reinforced this message, inviting the Commission to reconsider, but on 28 February the Commission refused the parliament's request.

The "common position" reappeared on the agenda of the Council's 7 March meeting as an "A-item" for adoption without discussion. At the Competitiveness meeting of the Council, Denmark requested that this be removed. The President of the Council, seemingly in breach of the Council's procedures, opposed this, "for administrative reasons" and because it would defeat the logic of the directive. The Danish representative accepted this at face value, declined to object formally, and entered Denmark's objections into the record. The common position was thus adopted without debate, and referred to the European Parliament for a second reading, with dissenting statements and caveats from a number of countries. In the event, only Spain had actually voted against: Austria, Belgium and Italy abstained (which has the same effect as voting against, given the way Qualified Majority Voting works).

Second reading in Parliament

In June 2005, the legal affairs committee of the European Parliament discussed the directive and rejected plans for a complete overhaul of the directive. The vote by the committee took place on 21 June 2005, and narrowly decided not to substantially amend the Council version of the directive. According to the Financial Times, this "vote marks a turning point in the protracted battle over the law, which has split the software industry and sparked severe recriminations."

On 5 July 2005, the committee's report passed to a plenary session of Parliament for debate by all MEPs. On 6 July 2005, Parliament rejected the proposal by a very large majority (648 in favour of rejection, 14 against and 18 registered abstentions out of 729 total MEPS) without considering any of the other 175 proposed amendments. Under the codecision procedure, the legislative process ended with this rejection and the proposed directive did not become law in any form. This was the first and as of 2005 the only time a directive was ever rejected by Parliament at second reading.

The vote was the result of a compromise between the different parties: those in favour of software patents feared a text that would heavily limit its scope, while those against rejected the whole principle. Heavy defeat was the "least worst option" to both sides. In addition, some saw the defeat as an expression of Parliament's indignation about the handling of the proposal by the Council of the European Union and the European Commission as well as its concerns about the content of the proposal itself.

Consequences of the rejection

Parliament's decision to strike down the final draft has the effect that national laws will not be harmonised. National legislatures may continue to enact laws allowing patents on computer-implemented inventions, should they wish to do so, and national courts may enforce such laws. The European Patent Office, which is not legally bound by any EU directive but generally adapts its regulations to new EU law, has no reason or incentive to adapt its practice of granting patents on computer-implemented inventions under certain conditions, according to its interpretation of the European Patent Convention and its Implementing Regulations.

Reactions

Supporters of the proposal

Supporters of the proposed directive included Microsoft, IBM, Hewlett-Packard and the European Patent Office.

The European Information and Communication Technology Association (EICTA) stated that the directive "is extremely important for the future of innovation in Europe as it concerns two-thirds of all inventions in the European hi-tech industry". This position was characterised by opponents of software patents as "dominated by patent lawyers from the patent arms of large corporate members", "most of which qualifying as non European companies" and "with a patent policy (...) tailored to the special interests of a few large corporations (...)". After the heavily modified draft directive was finally rejected, EICTA's Director General said, "This is a wise decision that has helped industry to avoid legislation that could have narrowed the scope of patent legislation in Europe. ... Parliament has today voted for the status quo, which preserves the current system that has served well the interests of our 10,000 member companies, both large and small."

Opponents of the proposal

The proposal provoked public disagreement by diverse opponents of software patents, who argued that software patents were neither economically desirable nor mandated by international law. The FFII and the EuroLinux Alliance played key roles in coordinating this campaign, which drew support from some free software and open source programmers, some academics, some small business groups, and some proprietary software developers. Many of these organisations expressed concern over what they saw as abuses of the software patent system in the USA, and argued that although some software patents might be beneficial, the net effect of the Commission's proposals would be to suppress innovation and dampen legitimate competition. The opponent's campaign in its turn was characterised by supporters of the directive as "a small but highly organised and vocal lobby", with EICTA stating that "Those who depict the draft directive on the patentability of computer-implemented inventions as some sort of 'software patent law' are at best misinformed and at worst dishonest, malicious and disrespectful of the European democratic process".

Figures who have supported the campaign against software patents in Europe include Tim Berners-Lee, developer of the World Wide Web, and Linus Torvalds, creator of the Linux kernel. Politicians opposed to the directive included Michel Rocard. Political opposition was founded both on opposition to software patents and towards what was considered heavy-handed management by the Commission.

Concerns about the balance of power

Apart from the issue itself, the legislative process for this directive generated concerns about the balance of power between the European Commission and the European

Parliament. It also raised concern about the balance between the Council (of member state governments) and Parliament (of elected members from member states). When the Commission rejected Parliament's request to restart discussion on the directive, this led to debates over how much power the Commission should have compared to Parliament and member states. Some MEPs saw the affair as part of a power struggle between the two bodies. Others believed that the real debate was more about whether Council should be able to overrule Parliament, or vice versa.

Statistics

According to a European Commission press release of 2002, "since the EPC came into force in 1978, at least 30,000 patents for computer-implemented inventions have already been issued [by the EPO]".

Chapter 10

Software Patents under United Kingdom Patent Law

There are four over-riding requirements for a patent to be granted under United Kingdom patent law. Firstly, there must have been an invention. That invention must be novel, inventive and susceptible of industrial application.

Patent laws in the UK and throughout Europe specify a non-exhaustive list of excluded things that are not regarded as *inventions* to the extent that a patent application relates to the excluded thing as such. This list includes *programs for computers*.

Despite this, the United Kingdom Intellectual Property Office (UKIPO) regularly grants patents to inventions that are partly or wholly implemented in software. The extent to which this should be done under the current law and the approach to be used in assessing whether a patent application describes an invention has been settled by the Court of Appeal. The UK approach is quite different from that of the European Patent Office (EPO). The significance of this is hotly debated.

Globally, the extent to which patent law should allow the granting of patents involving software (often referred to pejoratively as "software patents") is controversial and also hotly debated.

Substantive law

Although it is an implicit requirement of Section 1(1) of the UK Patent Act (1977) that patents should only be granted for inventions, "invention" is not defined anywhere in the Act.

Instead, Section 1(2) Patents Act provides a non-exhaustive list of *things* that are not treated as inventions. Included in this list is "*a program for a computer*". However these things are only prevented from being treated as inventions "*to the extent that a patent or application for a patent relates to that thing as such*"

Article 52(2) of the European Patent Convention (EPC) includes a slightly different list of non-inventions, although "programs for computers" are present. Article 52(3) EPC then states that patentability for the identified subject matter or activities is excluded

"*only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such*".

The wording of the Patents Act is slightly different from Article 52 EPC, but the UK Courts have taken the view that since the purpose of Section 1 of the Patents Act was to transpose the requirements of Article 52 EPC into UK law, any differences between the EPC and the Patents Act should be ignored. The text of the EPC itself should therefore be regarded as definitive.

Other things that are not regarded as inventions include mathematical methods, and schemes rules and methods for performing mental acts, playing games or doing business. These additional excluded categories often overlap with the exclusion of computer programs since they may be put into practice using a computer.

Case law

Summary

The case law in the United Kingdom relating to excluded subject matter in general, and computer programs specifically, has a somewhat sporadic history. For eight years, the leading case in the UK over whether or not a patent or patent application involving the use of a computer program related to an invention, or whether it instead related to a computer program "as such" was the judgment in Fujitsu's application from 1997.

Only in 2005, in the judgment in CFPH LLC's applications did the UK Courts again consider the issue of excluded subject matter in detail. In the meantime, the practice of the EPO and the UKIPO had diverged significantly. In some ways this judgment brought UK law closer to the practice of the EPO; but it also criticised the reliance of the EPO on paraphrasing the exclusions from patentability under the blanket heading of "technical".

Subsequently, in October 2006, the Court of Appeal heard their first case relating to the validity of computer programs in nine years and handed down their judgment on the matter of Aerotel v Telco and Macrossan's Application. This judgment reaffirmed the reasoning in Fujitsu and once again moved the practice of the UKIPO away from that of the EPO.

Court of Appeal Judgments

Fujitsu's Application

Fujitsu's Application was considered by the Court of Appeal in 1997. The case in question had been refused by the UKIPO and by J Laddie on Appeal before the High Court. LJ Aldous heard the appeal before the Court of Appeal and his judgment is notable for several reasons:

- It stated that the UK courts should look to the decisions of the European Patent Office for guidance in interpreting the exclusions.

- It confirmed that a "technical contribution" is needed to make a potentially excluded thing patentable, proclaiming that this was a concept at the heart of patent law and referring to the European Patent Office's decision in T 208/84, VICOM.

- It recognised the difficulty inherent in determining what is and is not "technical", such that each case should be decided on its own facts.

- It stressed that the substance of an invention should be used to assess whether or not a thing is patentable, not the form in which it is claimed. Thus a non-patentable method cannot be patented under the guise of an apparatus.

Fujitsu's claimed invention was a new tool for modelling crystal structures on a computer. A scientist wishing to investigate what would result if he made a new material consisting of a combination of two existing compounds would enter data representing those compounds and how they should be joined into the computer. The computer then automatically generated and displayed the new structure using the data supplied. Previously, the same effect could only have been achieved by assembling plastic models by hand - a time consuming task. The claimed invention was therefore certainly new and useful, but the fact that the same task could be achieved manually in the past was the application's downfall. As claimed, the invention was nothing more than a conventional computer which automatically displayed a crystal structure shown pictorally in a form that would in the past have been produced as a model. The only advance expressed in the claims was the computer program which enabled the combined structure to be portrayed more quickly. The new tool therefore provided nothing that went beyond the normal advantages that are obtained by the use of a computer program. Thus, there was no technical contribution and the application was rejected as being a computer program as such.

It is interesting to theorise whether there would have been any way for Fujitsu to have obtained a granted patent. If the invention as claimed had recited the particular steps carried out by the computer program, and if these were different from the steps which would have been carried out manually in the past, then there is the possibility that this could have represented a technical contribution. The particular technical contribution could have been that the claimed invention would not then have been merely a conventional computer for automatically carrying out a previously manual process, but rather a computer programmed in a specific way to perform a useful task.

The question then arises as to whether that invention would have been obvious or, conversely, inventive. Unfortunately, the Fujitsu judgment says nothing on the topic of inventive step or how inventive step should be considered when assessing inventions involving computer programs. The EPO decision in VICOM also did not discuss inventive step. These omissions resulted in some major divergences between the practice of the UKIPO and the European Patent Office over the next seven years. The EPO

modified the idea of a technical contribution to focus on inventive step and whether there was anything that provided a non-obvious technical solution to a technical problem. The UKIPO, in the meantime, remained rooted in a regime where the question of inventive step of computer program inventions was largely ignored in favour of rejections that there was no technical contribution and therefore no invention.

Menashe v William Hill

Menashe Business Mercantile Limited v William Hill Organisation Limited was considered by the Court of Appeal in 2002. The case in question related to EP 0625760 and a preliminary question of infringement. Questions of validity were never considered by the court.

This case is important because it considers the issues surrounding the infringement of computer-implemented inventions where the computer performing the claimed method is outside the UK, but a person inside the UK is making use of the invention.

The claimed invention required there to be a host or server computer. According to the judgment, it did not matter where the host computer was situated. It could be in the United Kingdom, on a satellite, or even on the border between two countries. Its location was not important to the user of the invention nor to the claimed gaming system. In that respect, there was a real difference between the claimed gaming system and an ordinary machine. The judge therefore believed that it would be wrong to apply the old ideas of location to inventions of the type under consideration. A person who is situated in the United Kingdom who obtains in the United Kingdom a CD and then uses his terminal to address a host computer is not bothered where the host computer is located. It is of no relevance to him, the user, nor the patentee as to whether or not it is situated in the United Kingdom.

If the host computer is situated in Antigua and the terminal computer is in the United Kingdom, it is pertinent to ask who uses the claimed gaming system. The answer must be the punter. Where does he use it? There can be no doubt that he uses his terminal in the United Kingdom and it is not a misuse of language to say that he uses the host computer in the United Kingdom. It is the input to and output of the host computer that is important to the punter and in a real sense the punter uses the host computer in the United Kingdom even though it is situated in Antigua and operates in Antigua. In those circumstances it is not straining the word "use" to conclude that the United Kingdom punter will use the claimed gaming system in the United Kingdom, even if the host computer is situated in, say, Antigua. Thus the supply of the CD in the United Kingdom to the United Kingdom punter will be intended to put the invention into effect in the United Kingdom.

Aerotel v Telco and Macrossan's application

The judgment in Aerotel v Telco and Macrossan's application by the Court of Appeal, passed down on 27 October 2006, relates to a patent granted to Aerotel and a patent application filed by Neal Macrossan but refused by the UKIPO and the High Court.

Aerotel’s patent is GB 2171877, and has a January 1985 priority date. Macrossan's GB application 2388937, has a December 2000 priority date.

Aerotel's patent was found to relate to a patentable invention in principle because the system as a whole was new in itself, not merely because it is to be used for the business of selling phone calls. The judge felt that this was clearly more than just a method of doing business as such. The method claims were construed as relating to a use of the new system and were also deemed to relate to a patentable invention in principle.

The claimed invention in Macrossan's application was an automated method of acquiring the documents necessary to incorporate a company. Macrossan's patent application was rejected for not being an invention since it was found to relate to a computer program as such and to a method of doing business as such. The Court's reason for this rejection was that there was no contribution made by the claimed invention that lay outside excluded subject matter.

Citing as reasons this clear divergence in reasoning between the UK courts and the European Patent Office, Neal Macrossan sought leave to appeal the refusal of his patent application to the House of Lords. Within the patent profession it was hoped that a ruling by the House of Lords would clarify the extent to which patent protection is available to computer-implemented inventions. To the disappointment of patent attorneys, the House of Lords have refused leave to hear the appeal, citing the reason that the case “does not raise an arguable point of law of general public importance".

High Court Judgments

After the judgement in Fujitsu's Application, the UK Courts did not hear another case relating to the exclusions to computer programs for eight years. The judgment in CFPH's applications was the first in a flurry of UK court cases starting in 2005 involving re-consideration by the High Court of patent applications refused by the UKIPO and made many references to the practice of the EPO.

Peter Prescott QC, sitting as a Deputy Judge in the UK High Court, noted that the EPO decisions are prescriptive, but not binding on the UK courts. With this in mind, the EPO's reliance on the word "technical" was criticised, but the judgment went on to say that the two modes of reasoning used by the UK courts and by the EPO, although different, would usually produce identical results on the same set of facts if properly applied. Another criticism suggests that the EPO are being too strict by insisting that an invention must provide a technical contribution to be inventive since, as evidenced by the judgment in Dyson v Hoover, the commercial background to an invention may be important when determining the presence or otherwise of an inventive step.

The two patent applications in question both involved networked interactive wagering on the outcomes of events. The applications were not refused as relating to a computer program as such, because the computer program was simply a tool that was being used to implement a new set of business rules and the invention was not really about the

computer program. Rather the only "advance" (defined as being those features which were novel and inventive) was found to be the new set of business rules and each application was refused as relating to a method of doing business as such. Although the judgment stressed that the reasoning used was quite different from the type that would have been applied by the EPO, the judge appeared satisfied that the EPO would have come to the same conclusion using their own reasoning.

Although briefly of great importance due to the UKIPO swiftly altering their practice to follow its recommendations , the idea in the CFPH judgment to consider whether an invention is excluded by looking at the novel and inventive advance has been disapproved by the more recent Aerotel and Macrossan judgment. This judgment therefore remains of interest only from an historical perspective.

Patent Office decisions

Decisions of the UKIPO, made by senior Hearing Officers, are not binding on the UKIPO in the way that judgments of the Courts are. Nevertheless, there are, by nature, many more Office decisions than there are court judgments. A full list is available on the UKIPO website

UK Intellectual Property Office practice

On 2 November 2006, following the judgment in Aerotel v Telco and Macrossan's Application, the UKIPO issued a Practice Note announcing an immediate change in the way patent examiners will assess whether inventions relate to patentable subject matter. This practice is considered to be a restrictive interpretation of the judgment by patent attorneys.

One aspect of the practice change was a reversal in the UKIPO practice concerning computer program claims. For several years previously, the UKIPO had allowed claims directed to a computer program if the method performed by the computer program was itself patentable. In light of the first step of the Aerotel/Macrossan four step test, to construe the claim, the UKIPO decided that claims to a computer program were not a permissible form of claim even if the underlying method was found to be patentable.

This practice remained in place until 7 February 2008 when, following the judgment in Astron Clinica and other’s Applications, the UKIPO issued a new Practice Note stating that they would return to their previous practice of permitting claims to computer programs if claims to a method performed by running a suitably programmed computer or to a computer programmed to carry out the method were themselves allowable. This change affirmed the established practice of considering the substance of the invention over the particular way it was claimed but it was not thought that it would cause a material change in the subject matter which would be deemed patentable by the UKIPO.

Comparison of EPO with UK Practice

Patents granted by the European Patent Office (EPO) may be brought into effect in the UK once certain formal requirements have been met. As soon as a European patent is granted (provided that no opposition is filed), then final authority to interpret Article 52(2) and (3) EPC rests with each national jurisdiction and any person may apply to the UKIPO or the UK courts to have a patent granted by the EPO revoked in the UK.

There is to date no supranational European system for patent litigation, so the courts of each EPC Contracting State retain the final say, and vary to some extent from one to another, as to just how far the exclusion should extend.

Compared to the EPO, the UKIPO have consistently taken a very different approach when deciding whether or not to grant patents involving software. This has sometimes drawn criticism from those advocating the need for harmony across Europe.

The most important difference between the two Offices is that the EPO will in general accept that any patent application relating to a computer-implemented method is "an invention", whereas the UKPO will reject an application on the basis that it does not describe "an invention" if the only contribution provided by the inventor is a computer program. The EPO instead only consider technical features when assessing the presence or otherwise of an inventive step and will therefore normally reject the trivial computer-implementation of a non-technical method as lacking an inventive step. The UKPO, in contrast, consider any feature, technical or not, as being capable of contributing to an inventive step.

Thus, for example, a patent application describing a new computer chip used to implement a faster method for calculating square-roots was rejected as not being an invention in the UK (Gale's Application), but would probably be deemed an invention in principle by the EPO. The EPO would instead consider whether the new method of solving square roots provided a technical solution to a technical problem and would only grant the application if such a solution were inventive.

It was noted by the Court of Appeal in Aerotel and Macrossan that using the reasoning of most of the EPO case law (such as T 258/03 - Hitachi) would result in the same final conclusion as the "contribution" approach. However, the reasoning in a particular Microsoft case was held up as being flawed. The UKPO have also expressed the opinion that the end result would normally be the same. This is disputed by groups such as the Foundation for a Free Information Infrastructure who consider that the EPO is consistently granting patents that would be refused by the Courts in the UK and elsewhere in Europe.

Chapter 11

Patentable Subject Matter

Patentable, **statutory** or **patent-eligible subject matter** is subject matter which is susceptible of patent protection. The laws or patent practices of many countries suggest that certain subject matter is or is not something for which a patent should be granted.

Together with novelty, inventive step or nonobviousness, utility and industrial applicability, the question of whether a particular subject matter is patentable is one of the fundamental requirements for patentability.

Legislations

The subject-matter which is regarded as patentable as a matter of policy, and correspondingly the subject-matter which is excluded from patentability as a matter of policy, depends on the national legislation or international treaty.

Canadian patent law

Canadian patent law is the legal system regulating the granting of patents for inventions within Canada, and the enforcement of these rights in Canada.

Background

A patent is a government grant that gives the inventor and his or her heirs, executors and assigns, the exclusive right within Canada, during the term of the patent, to make, use and/or sell the invention claimed in the patent, subject to adjudication.

The granting of Canadian patents is within the exclusive jurisdiction of the Canadian federal government and is governed by the federal *Patent Act*, the *Patent Rules*, and various international treaties and the regulations thereunder. The enforcement of Canadian patents is the responsibility of the Canadian Federal Court, or the Courts of the Canadian provinces.

Term

For patent applications filed prior to October 1, 1989, the patent expires 17 years after the patent *issues*. For patent applications filed on or after October 1, 1989, the patent expires 20 years after the patent application *was filed*.

Definition of a patentable invention

To be considered patentable, an invention must pass three criteria: novelty, non-obviousness and utility.

Novelty

To be patentable, an invention must be novel. That is, the invention must not have been described or claimed in a previously filed third party Canadian patent application, and must not have been previously publicly disclosed by a third party, anywhere in the world. The test for novelty is whether or not a single, publicly disclosed example of prior art that "contained all of the information which, for practical purposes, is needed to produce the claimed invention without the exercise of any inventive skill". If a third party previously filed a Canadian patent application disclosing the invention, or if a third party document or device previously publicly disclosed the invention anywhere in the world, then a subsequently applied-for Canadian patent application for that invention is lacking in novelty and is invalid. A lack of novelty is often referred to as "anticipation". For example, if a piece of prior art has each of the elements of a claimed invention, the piece of prior art is said to "anticipate" the claimed invention, or alternatively, the claimed invention is said to have been "anticipated by" the piece of prior art.

Non-obviousness

The test for non-obviousness (also sometimes referred to as "inventive ingenuity" or "inventive step") is whether a "unimaginative skilled technician, in light of his general knowledge and the literature and information on the subject available to him on (the date that the application is filed in Canada), would have been led directly and without difficulty to [the] invention."

Utility

For a product to have utility it must perform some useful function. The requirement for utility originates from the definition of invention as a "new and useful art" The requirement is generally easy to meet, however, it does limit the scope of protection by excluding methods that would not be useful.

Subject matter

There are number of matters that cannot be patented. Among such matters include certain new plant matters, some types of computer programs, and medical treatments within the body (diagnoses based on, for example, blood tests, are patentable).

The list of prohibited matters notably differs from the United States. With respect to patents for software, while mere algorithms are not patentable *per se* (mere algorithms may be protected by Canadian copyright law), software may be protected by Canadian patent law if it meets the traditional criteria for patentability (that is, it must be new, non-obvious and useful). In other words, if for example the software is new and non-obvious, it would be patentable in Canada if the software directly provided a functional *real world* useful result (and not merely the calculation of a mere algorithm).

First-to-file system

In Canada, since October 1, 1989, generally speaking, patents are granted to the first inventor to file an application for an invention (that is, Canada has a "first-to-file" system), which may result in a "race to the patent office" by inventors of competing technologies.

In some cases (referred to below under the heading Requesting an Earlier Filing Date), an application may effectively receive an earlier filing date, to improve the chances of an applicant winning the "race to the patent office".

One year grace period

In Canada, inventors have one year after their first public disclosure of their invention in which to file a Canadian patent application (this is sometimes referred to as the "one year grace period"). However, disclosing the invention to the public prior to filing a Canadian patent application will result in the loss of significant international patent rights. Additionally, as Canada has a modified "first to file" system, any delay in the filing of a Canadian patent application may result in "losing the race to the patent office".

Requesting an earlier filing date

To facilitate the international protection of inventions, by way of international treaties and the application of Canadian law, in some circumstances, priority may be requested in a subsequently filed patent application to an earlier filed foreign or domestic patent application by the same inventor for the same invention to provide an earlier "effective filing date" for the subsequently filed application.

For example, if a subsequently filed patent application is filed in Canada within 12 months of the earliest date on which any corresponding previously regularly filed application was filed in Canada, or in any country belonging to the Paris Convention, or in any World Trade Organization (WTO) member country, the subsequently filed patent

application can request priority back to the date of filing the earlier filed foreign or domestic patent application, effectively, for the purposes of determining patentability of the invention in the subsequently filed patent application, giving the subsequently filed patent application the filing date of the earlier filed foreign or domestic patent application to the extent that the claimed subject matter of the subsequently filed patent application overlaps with the disclosed subject matter of the earlier filed foreign or domestic patent application.

The Patent Cooperation Treaty

Since 1990, Canada has been bound by the provisions of the Patent Cooperation Treaty (PCT). Pursuant to the PCT, the Canadian Patent Office may receive an International Patent Application as a "Receiving Office" if the applicant is a national or resident of Canada (or if there is more than one applicant, at least one of the applicants is a national or resident of Canada). Additionally, the Canadian Patent Office acts as an International Searching Authority and as the International Preliminary Examining Authority. Where an International Patent Application has been filed in which Canada has been designated and elected, the Canadian Patent Office is the elected Office pursuant to the PCT. Additionally, the Canadian Patent Office receives Canadian *National Phase* patent applications in accordance with the provisions of the PCT and Canadian legislation, and the rules thereunder.

Public access

In Canada, all patent applications (unless they are withdrawn by the applicant) are made public eighteen months after filing. The goal of public access is to give the public the ability to learn new technological information while protecting the right of the inventor to profit from the invention.

Patent agents

The Canadian Intellectual Property Office maintains and publishes a list of Canadian Patent Agents who are registered with the Canadian Patent Office and who prepare and file patent applications in Canada on behalf of inventors.

European Patent Convention

The European Patent Convention does not provide any positive guidance on what *should* be considered an invention for the purposes of patent law. However, it provides in Article 52(2) EPC a nonexhaustive list of what are not to be regarded as inventions, and therefore *not* patentable subject matter:

The following in particular shall not be regarded as inventions within the meaning of paragraph 1:
(a) discoveries, scientific theories and mathematical methods;
(b) aesthetic creations;

(c) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers;
(d) presentations of information.

Article 52(3) EPC then qualifies Art. 52(2) EPC by stating:

The provisions of paragraph 2 shall exclude patentability of the subject-matter or activities referred to in that provision only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such.

(Some further items are excluded under Article 52(4) EPC, as formally being not industrially applicable).

Practice at the European Patent Office

Under Article 52(1) EPC, "*European patents shall be granted for any inventions which are susceptible of industrial application, which are new and which involve an inventive step.*" So, four questions need to be assessed:

1. Is there an invention?
2. Is the invention susceptible of industrial application?
3. Is the invention novel?
4. Does the invention involve an inventive step?

The first question "Is there an invention?" is equivalent to: "Is the claimed subject-matter as a whole excluded from the realm of patentable subject-matter?" The invention question or patentable subject-matter question necessarily precedes the three further questions, which cannot be assessed when there is no invention.

According to the case law of the Boards of Appeal of the EPO, the question "Is there an invention?" also implicitly implies the further question: "Does the claimed subject-matter have a technical character?" "*Having technical character is an implicit requirement of the EPC to be met by an invention to be an invention within the meaning of Article 52(1) EPC*".

Patentable subject-matter considerations also intervene again at a secondary level, during the inventive step examination. T 641/00 (Comvik/Two Identities) states that, "*An invention consisting of a mixture of technical and non-technical features and having technical character as a whole is to be assessed with respect to the requirement of inventive step by taking account of all those features which contribute to said technical character whereas features making no such contribution cannot support the presence of inventive step.*" The non-technical features are the ones that are excluded from the realm of patentable subject-matter as a matter of policy. T 258/03 (Hitachi/Auction Method) further developed this test for patentable subject-matter.

Under this test, a patent application or patent which does not provide a technical solution to a technical problem would be refused or revoked as lacking inventive step.

Practice in the United Kingdom

Following the 2006 Court of Appeal judgment in Aerotel v Telco and Macrossan's application, which contains a lengthy discussion of case law in the area, the UKPO has adopted the following test:

(1) properly construe the claim
(2) identify the actual contribution
(3) ask whether it falls solely within the excluded subject matter
(4) check whether the actual or alleged contribution is actually technical in nature.

The Court decided that the new approach provided a structured and more helpful way of applying the statutory test for assessing patentability which was consistent with previous decisions of the Court.

This test is quite different from the test used by the EPO, as expressed in T 641/00 (Comvik/Two Identities) and T 258/03 (Hitachi/Auction Method), but it is considered that the end result will be the same in nearly every case.

United States

Section 101 of Title 35 U.S.C. sets out the subject matter that can be patented:

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

In October 2005, the United States Patent and Trademark Office (USPTO) issued interim guidelines for patent examiners to determine if a given claimed invention meets the statutory requirements of being a useful process, manufacture, composition of matter or machine (35 U.S.C. § 101). These guidelines assert that a process, including a process for doing business, must produce a concrete, useful and tangible result to be patentable. It does not matter whether the process is within the traditional technological arts or not. A price for a financial product, for example, is considered to be a concrete useful and tangible result. However, on August 24, 2009, the USPTO issued new interim guidelines so that examination would comport with the Federal Circuit opinion in In re Bilski, which held that the "useful, concrete, and tangible" test for patent-eligibility is incorrect and that *State Street* is no longer valid legal authority on this point. Instead, the Federal Circuit and the new USPTO guidelines use a Machine-or-Transformation Test to determine patentability for processes. The Supreme Court determined that the claims in the Bilski case covered non-statutory subject matter as it was too abstract and broad.

The USPTO has reasserted its position that literary works, compositions of music, compilations of data, legal documents (such as insurance policies), and forms of energy (such as data packets transmitted over the Internet), are not considered "manufactures" and hence, by themselves, are not patentable. Nonetheless, the USPTO has requested comments from the public on this position. The Federal Circuit has ruled, in *In re Nuitjen*, that signals are not statutory subject matter, because articles of manufacture (the only plausible category under 35 U.S.C. § 101) do not include intangible, incorporeal, transitory entities.

The USPTO was prompted to issue the guidelines by a recent decision by their board of appeals, *Ex Parte Lundgren*. This decision asserted that according to US judicial opinions, inventions do not have to be in the "technological arts" to satisfy the requirements of 35 U.S.C. § 101. They must, however, produce a concrete, useful and tangible result. As indicated above, however, *In re Bilski* supersedes that legal test (as to the "useful, concrete, and tangible" test). The *Bilski* majority opinion also rejects the "technological arts" test, although three Federal Circuit judges (Mayer, dissenting, and Dyk and Linn, concurring) stated that they considered being technological an indispensable condition of patent-eligibility.

The algorithm exception and the patent-eligibility trilogy

The exception to patenting algorithms arose out of three Supreme Court cases commonly referred to as the "Supreme Court Trilogy" or "patent-eligibility trilogy". This is a designation for three Supreme Court cases decided within a decade on whether, and in what circumstances, a claimed invention was within the scope of the US patent system (that is, was eligible to be considered for a patent grant). The three cases of the trilogy can be harmonized on the basis of when a claimed implementation of an idea or principle is old or departs from the prior art in only a facially trivial way, the claim is patent-ineligible (as *Nielson* and *Morse* said, and *Flook* reaffirmed, it must be treated as if in the prior art).

Gottschalk v. Benson

The invention in this case was a method of programming a general-purpose digital computer using an algorithm to convert binary-coded decimal numbers into pure binary numbers. The Supreme Court noted that phenomena of nature, mental processes and abstract intellectual concepts were not patentable, since they were the basic tools of scientific and technological work. However, new and useful inventions derived from such discoveries are patentable. The Court found that the discovery in *Benson* was unpatentable since the invention, an algorithm, was no more than abstract mathematics. Despite this holding, the Court emphasized that its decision did not preclude computer software from being patented, but rather precluded the patentability of software where the only useful characteristic was an algorithm. The Court further noted that validating this type of patent would foreclose all future use of the algorithm in question. Therefore, like the traditional exceptions to patentable subject matter, the purpose of the algorithm

exception was to encourage development of new technologies by not granting patents that would preclude others from using abstract mathematical principles.

Parker v. Flook

The invention in this case was a method of calculating alarm limits by using a "smoothing algorithm" to make the system responsive to trends but not momentary fluctuations in process variables (such as temperature). Because it was conceded that the implementation of the algorithm was conventional, the Court found that the inventor did not even purport to have invented anything on which a patent could be granted. The Court did so on the basis of the principle that the nonstatutory subject matter (the algorithm) must be regarded as already in the prior art. Therefore, there was nothing left on which a patent could issue. In a case in which a patent was sought on an implementation of a principle (the algorithm), the implementation itself must be inventive for a patent to issue. Since that was not so, the Court held that the patent office had properly rejected Flook's claim to a patent. The Court relied on the decision in *Neilson v. Harford*, an English case that the Supreme Court had relied upon in *O'Reilly v. Morse*, for the proposition that an idea or principle must be treated as if it were already in the prior art, irrespective of whether it was actually new or old. This approach is something like that of analytic dissection in computer-software copyright law, although its use in patent law preceded its use in copyright law by a century or more.

Diamond v. Diehr

In this case the Court backed away from the analytic dissection approach, and insisted that patent-eligibility must be decided on the basis of the claim (or invention) considered as a whole. That requirement is found in the statute, but only for section 103 (governing obviousness or inventive step) and not for section 101 (governing patent-eligibility). Despite this difference in emphasis, however, *Diehr* can be harmonized with *Flook* and *Benson*, and the *Diehr* Court studiously avoided stating that *Flook* and *Benson* were overruled or limited.

Bilski v. Kappos

On June 28, 2010, the United States Supreme Court ruled in *Bilski v. Kappos* that Bernard Bilski's patent application for a method of hedging the seasonal risks of buying energy is an abstract idea and is therefore unpatentable. However, it also said that business methods are not inherently unpatentable, and was silent on the subject of software patents. The majority opinion also said that the Federal Circuit's "machine or transformation" test, while useful, is not an exclusive test for determining the patentability of a process. Instead, the Supreme Court reviewed the "Supreme Court Trilogy" described above and said that future decisions should be grounded in the examples and concepts expressed in those opinions. As has been reported, the decision leaves many questions unanswered, including the patentability of many medical diagnostic technologies and software.

Controversies

The question of what should and should not be patentable subject matter has spawned a number of battlegrounds in recent years, setting against each other those in each area supporting patentability, claiming that patents would cause increased innovation and public good, against opponents with views that patentability was being sought only for private good but would do public harm.

Flashpoints have included the patenting of naturally occurring biological material; genetic sequences; stem cells; "traditional knowledge"; programs for computers; business methods.

In March 2010, a federal district court judge in the Southern District of New York ruled that purified DNA sequences and the inventions using them are unpatentable. As has been discussed, Judge Sweet relied entirely upon Supreme Court precedent and ignored contrary case law of the Federal Circuit Court of Appeals to conclude that isolated DNA is of the same fundamental quality as natural DNA and is thus unpatentable under section 101 of the Patent Act; and that the method claims of the patents were abstract mental processes that were also unpatentable. His rationale is controversial and his ruling has been appealed to the Federal Circuit.

In the process, different jurisdictions have come to different views as to what should be allowed and what should not.

Patents on business methods have proven to be a particularly controversial type of statutory subject matter. They have been criticized because the patents granted are perceived as being too broad, perhaps due to the difficulty in searching for prior art and recruiting suitably qualified patent examiners who have historically had a science background rather than a business background. Patent applications for business methods are also subject to delays in prosecution at the United States Patent and Trademark Office and other patent offices.

Chapter 12

Software Patents and Free Software

Opposition to software patents is widespread in the free software community. In response, various mechanisms have been tried to defuse the perceived problem.

Positions from the community

Community leaders such as Richard Stallman, Alan Cox, Bruce Perens, and Linus Torvalds and companies such as Red Hat, and MySQL, and community groups such as FSFE, IFSO, all believe that patents cause problems for free software.

Patent licensing

Patent holders can require infringers of their patents to take out a license to continue using an invention covered by the patent, which may or may not require payment of a fee. Otherwise, the infringer must stop infringing the patent, possibly by removing or modifying the patented feature so that the product no longer infringes. This possibility may be easier with software than other types of inventions since computer program often perform many different functions or a similar result may be achieved in a different, non-infringing manner. Nevertheless, the software may not be useful without the patented feature.

Benefits of free software

US patent attorney Dan Ravicher argues that free software's distributed development model which leads to fewer concentrations of wealth, plus free software's public benefit create economic and legal protections.

Problems for free software

Free software projects cannot agree to patent licenses that include any kind of per-copy fee. No matter how low the fee is, there is no way for a free software distributor to know how many copies are being made. Also, adding any requirements to pay or to notify someone each time a copy is made would make the software no longer free software.

A patent license that is royalty-free, or provides a one-time worldwide payment is acceptable. Version 2 of the GNU General Public License does not allow software to be distributed if that software requires a patent license that does not "*permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you*".

The 2004 OSRM study

In 2004, Open Source Risk Management commissioned a patent study, carried out by Dan Ravicher. For this study, Ravicher performed patent searches to estimate the patent-risk of the Linux kernel. His conclusion was:

In conclusion, he found that no court-validated software patent is infringed by the Linux kernel. However, Ravicher also found 283 issued but not yet court-validated software patents that, if upheld as valid by the courts, could potentially be used to support patent claims against Linux.

Techniques for opposing patents

Patent retaliation

"Patent retaliation" clauses are included in several free software licenses. The goal of these clauses is to create a penalty so as to discourage the licensee (the user/recipient of the software) from suing the licensor (the provider/author of the software) for patent infringement by terminating the license upon the initiation of such a lawsuit.

The Free Software Foundation included a narrow patent retaliation clause in drafts 1 and 2 of version 3 of the GPL, however, this clause was removed in draft 3 as its enforceability and effectiveness was decided to be too dubious to be worth the added complexity.

Examples of broader clauses are those of the Apache License and the Mozilla Public License.

Patent pools

In 2005, IBM, Novell, Philips, Red Hat, and Sony founded the Open Invention Network (OIN). OIN is a company that acquires patents and offers them royalty free "to any company, institution or individual that agrees not to assert its patents against the Linux operating system or certain Linux-related applications".

Novell donated the valuable Commerce One web services patents to OIN. These potentially threaten anyone who uses web services. OIN's founders intend for these patents to encourage others to join, and to discourage legal threats against Linux and Linux-related applications. Along with several other projects, Mono is listed as a covered project.

Lobbying for legislative change

Movements have formed to lobby against the existence and enforceability of software patents. The earliest was the League for Programming Freedom in the USA. Probably the most successful was the anti-software-patent campaign in Europe that resulted in the rejection by the European Parliament of the Proposed directive on the patentability of computer-implemented inventions which, the free software community argues, would have made software patents enforceable in the European Union. A fledgling movement also exists in South Africa.

Promises from patent holders

Some software companies who hold significant patent portfolios have made non-aggression pledges to the free software community. These have varied in scope and have received a variety of responses. IBM, Sun, and Nokia are three examples. These have been described by Richard Stallman as "significant", "not really anything", and "next to nothing", respectively.

Microsoft has pledged not to assert any claims against open source developers which CEO Steve Ballmer called "an important step and significant change in how we share information about our products and technologies." This pledge has been accepted with some skepticism.

Infringement claims

Microsoft has claimed that free software such as OpenOffice.org and the Linux kernel violate 235 Microsoft patents and said that it will seek license fees, but has so far failed to disclose which patents they violate. However, the 2009 lawsuit against TomTom involved the use of Microsoft's patents for long filenames on FAT filesystems, the code for which is in the Linux kernel, not in any TomTom-developed software.

In January 2008, Trend Micro accused Barracuda Networks of patent infringement for distribution of the ClamAV anti-virus software.

Microsoft's patent deals

In November 2006, a highly controversial agreement was made between Novell and Microsoft that included patent licensing. This led to much criticism of Novell by the free software community.

In June 2007, Xandros announced a similar deal

On June 13, 2007, a deal was reached between Microsoft and Linspire. In return, Linspire would change its default search engine from Google to Live search.

Ubuntu founder and director Mark Shuttleworth has said that Ubuntu will not be making any such deal, as have Red Hat. These have been joined by a weaker statement from Mandriva that "*we don't believe it is necessary for us to get protection from Microsoft*".

On October 2007, IP Innovation LLC, a company specialized in patent-protection, filed a suit for patent infringement against Red Hat and Novell. However, IP Innovation LLC is a subsidiary of a company classified by some as a patent troll, and commentators suspect a strong connection between this company and Microsoft.

In December 2007, Microsoft granted the Samba project access to certain proprietary documents and must maintain a list of related patents for a one-time fee of 10,000 Euros .

Chapter 13

Software Patents under TRIPs Agreement and Computer Programs and the Patent Cooperation Treaty

Software patents under TRIPs Agreement

The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), particularly Article 27, is occasionally referenced in the political debate on the international legal framework for the **patentability of software**, and on whether software and computer-implemented inventions should be considered as a field of technology.

Article 27 of TRIPs

Article 27 paragraph 1 of TRIPs states that:

"(...) patents shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application. (...) patents shall be available and patent rights enjoyable without discrimination as to the place of invention, the field of technology and whether products are imported or locally produced."

The only acceptable exceptions to this provision are laid down in the paragraphs 2 and 3 of the same Article 27. The following elements may be excluded from patentability by WTO members under TRIPs:

- (...) inventions, the prevention within their territory of the commercial exploitation of which is necessary to protect ordre public or morality, including to protect human, animal or plant life or health or to avoid serious prejudice to the environment, provided that such exclusion is not made merely because the exploitation is prohibited by their law. *(paragraph 2)*
- diagnostic, therapeutic and surgical methods for the treatment of humans or animals; *(paragraph 3(a))* and
- plants and animals other than micro-organisms, and essentially biological processes for the production of plants or animals other than non-biological and microbiological processes. (...) *(paragraph 3(b))*.

However as Paul Hartnack, then Comptroller-General of the UK Patent Office, commented in 1998:

Some have argued that the TRIPS agreement requires us to grant patents for software because it says "patents shall be available for any inventions.....in all fields of technology, provided they are.....capable of industrial application". However, it depends on how you interpret these words.
Is a piece of pure software an invention? European law says it isn't. Is pure software technology? Many would say no. Is it capable of "industrial" application? Again, for much software many would say no.
TRIPS is an argument for wider protection for software. But the decision to do so should be based on sound economic reasons. Would it be in the interests of European industry, and European consumers, to take this step?

The rules for in interpretation of international treaties, do not allow specific European perceptions on terminology to be considered for TRIPS interpretation: in art. 31(1) it requires "ordinary meaning to be given to the terms of the treaty". The same provision requires interpretation within the light of the object and purpose of the treaty, which leaves little room for "sound economic reasons" for legal interpretation purposes. The decision of the contracting states of the TRIPS Agreement was that patents should be granted in all fields of technology, without discrimination (Art. 27(1) TRIPS).

To date, the interpretation of Article 27 has been tested in the 2002 dispute between the U.S. and Argentina over patent protection for pharmaceuticals (which was solved by mutual agreement) and the 2000 panel report also on patent protection for pharmaceuticals, in a case brought by the EU against Canada.

However, there have been no dispute settlement procedures regarding software patents. Its relevance for patentability in the domains of, for example, computer-implemented business methods, computer science and software information technology remains uncertain, since the TRIPs agreement is subject to interpretation, like all legal texts.

Relationship with copyright protection

Article 10 paragraph 1 of TRIPs provides that a computer program is a type of work which is eligible for protection under copyright law:

"Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)."

This argument was used by some adversaries of software patents to contend that software patents would not be allowed by the TRIPS agreement. TRIPS textbooks don't see a conflict, for instance Correa & Yusuf notes that software patents complement copyright because copyright does not protect underlying ideas.

Computer programs and the Patent Cooperation Treaty

There are two provisions in the Regulations annexed to the **Patent Cooperation Treaty** (PCT) that relate to the search and examination of patent applications concerning **computer programs**. These two provisions are present in the PCT, which does not provide for the grant of patents but provides a unified procedure for filing, searching and examining patent applications, called international applications. The question of patentability is touched when conducting the search and the examination, which is an examination of whether the invention appears to be patentable.

These two provisions are Rule 39.1 PCT and Rule 67.1 PCT, and, in conjunction respectively with Article 17(2)(a)(i) PCT and Article 34(4)(a)(i) PCT, may have a concrete impact on the procedure under the PCT, in the search and examination performed under the PCT. Indeed, depending on the patent office which is in charge of the search or examination under the PCT, the application filed for an invention relating to a computer program may or may not be searched or examined. In addition, the ISA and IPEA that do not search such applications to a certain extent have diverging practices with respect to determinations of exclusions as to computer programs.

In addition to the consequences these legal provisions may have in practice, Rule 39.1 PCT is also significant from an interpretive perspective to understand the origin of the much debated Article 52(2) and (3) EPC. The computer program exclusion was indeed inserted in the EPC in line with Rule 39.1 PCT, so that Rule 39.1 predates Art. 52(2) and (3) EPC.

Background

The Patent Cooperation Treaty (PCT) is an international patent law treaty, which provides a unified procedure for filing patent applications. A patent application filed under the PCT is called an international application or a PCT application.

The filing of an international application results in an international search performed by a patent office, accompanied with a written opinion regarding the patentability of the invention which is the subject of the application. An applicant may also request an international preliminary examination performed by a patent office. The PCT does not provide that the searches and examinations are to be performed by one central patent office, as the WIPO does not perform searches and examinations. In contrast, the European Patent Convention (EPC) places the European Patent Office (EPO) in charge of performing searches and examinations for European patent applications.

Under the PCT, the international search and the optional international preliminary examination are conducted by different national or regional patent offices, referred to as the International Searching Authorities (ISA) and the International Preliminary Examining Authority (IPEA) Applicants, based on nationality and on the Receiving

Office where the application was filed, may have an opportunity to have the search performed by one of the ISAs.

The relevant provisions in the Regulations

The Regulations under the PCT do touch on the search and examination of computer programs.

Rule 39.1 PCT states that

"No International Searching Authority shall be required to search an international application if, and to the extent to which, its subject matter is any of the following:
(...)
(vi) **computer programs** to the extent that the International Searching Authority is not equipped to search prior art concerning such programs." (emphasis added)

Rule 67.1 PCT states that

"No International Preliminary Examining Authority shall be required to carry out an international preliminary examination on an international application if, and to the extent to which, its subject matter is any of the following:
(...)
(vi) **computer programs** to the extent that the International Preliminary Examining Authority is not equipped to carry out an international preliminary examination concerning such programs." (emphasis added)

According to the Board of Appeal 3.5.1 of the EPO, these provisions mean that the ISA and IPEA authorities are not required to carry out searches or preliminary examinations in respect of programs if, for example, they have no examiners trained to do so or are not equipped with appropriate search material. The Board went on to say:

"However, it is not to be inferred from these rules that searches or examinations in the software field are to be ruled out in international authorities. On the contrary, it seems (...) that according to the PCT searches and, if applicable, examinations of this type can and may very well (perhaps even should) be carried out if the competent authority is appropriately equipped."

These provisions deal only with the international searches and international preliminary examinations and not with the national and regional searches or examinations.

Practices by ISA and IPEA

The different ISA and IPEA have made use of the legal provisions of Articles 17(2)(a)(i) and 34(4)(a)(i) PCT in conjunction with Rules 39.1 and 67.1 in a different manner. In addition, as mentioned above, the ISA and IPEA that have made use of these provisions

have diverging practices with respect to determinations of exclusions as to computer programs.

For instance, the European Patent Office (EPO), acting as ISA and IPEA, is not be obliged to search, by virtue of Article 17(2)(a)(i) PCT, or examine, by virtue of Article 34(4)(a)(i) PCT, any international application to the extent that the EPO considers that such application relates to subject matter which does not comply with the provisions of the European Patent Convention to such an extent that it is not possible to carry out a meaningful search into the state of the art on the basis of all or some of the claims. The EPO acting as ISA or IPEA in the PCT procedure is therefore not obliged to search or examine some PCT applications when not equipped to do so.

Origin and interpretive significance of the provisions

The computer program exclusion of Rule 39.1 PCT, which originally appears to be for "equipment" reasons, dates from 1969:

"[The subject matter for which the International Searching Authority is not required to search] includes mathematical and scientific theories, plant and animal varieties except for microbiology, ornamental designs. It also includes computer programs but only to the extent that the International Searching Authority is not equipped to search prior art concerning such programs."

Rule 39.1 PCT is significant from an interpretive perspective to understand the origin of the much debated Article 52(2) and (3) EPC. The computer program exclusion was indeed inserted in the EPC in line with Rule 39.1 PCT, so that Rule 39.1 predates Art. 52(2) and (3) EPC. However, while the PCT condition for excluding computer programs is a question of equipment, the EPC condition is a question of "computer program as such".

According to some, the fact that the PCT does not deal directly with the scope of patentable subject matter, in relation to computer programs, adds "weight to the contention that, having been born out of administrative inconvenience rather than any great principle, restrictions on patentability of programs should be limited to the maximum possible extent."

In the judgment in *CFPH LLC's Applications*, Peter Prescott referred to Rule 39.1 PCT when discussing the motivation behind the exclusion from patent protection of programs for computers under UK law. He commented that, at the time the EPC was under consideration (during the 1970s), "it was felt that searching the prior art would be a big problem" and that "Rule 39(1) of the Patent Co-operation Treaty recognised that an International Searching Authority might not be suitably equipped".

Consequences on national and regional phases

These provisions have no legal consequence as regards the patentability in national or regional patent offices designated in a PCT application, as the law of most national or regional offices requires that they draw their own conclusions based on their own national or regional patent law. This is in complete compliance with the PCT since Article 27(5) PCT provides that, as far as substantive conditions of patentability are concerned, national and regional patent laws prevail:

"Nothing in this Treaty and the Regulations is intended to be construed as prescribing anything that would limit the freedom of each Contracting State to prescribe such substantive conditions of patentability as it desires. (...)"