Title:-

Legal Protection for Computer Programmes in EU, US and Pakistan & Software Piracy as a Challenge in Pakistan

Candidate number:

Supervisor: **Pro, Dr Jurist Jon Bing**

Deadline for submission: ….. (1st/Oct / 2008):

Number of words: 18,626 (max. 18.000)

27.11.2008

UNIVERSITY OF OSLO

Faculty of Law

Contents

Chapter 1

1. Introduction. Law and computer science have typically and traditionally been disparate, however this separation is no longer appropriate. Copyright law in particular has increasing application to computer science.

1.1. Historical Background. Computers are not new. Charles Babbage conceived of a mechanical "difference engine" in Victorian England, although the first computer actually made was probably the Turing machines at Bletchley Park during World War II. Computer programs are also not new. Ada Byron, Countess of Lovelace, wrote programs for her colleague (and possibly lover) Babbage's difference engine[1].

Intellectual property is likewise not new[2]. The doctrine of copyright, for example, can be traced back to a monopoly given to stationers by the Tudor and Stuart monarchs in England. Copyright law in its modern form was internationally agreed upon towards the end of the nineteenth century with the Berne Convention for the Protection of Literary and Artistic Works.

The nexus between computers, computer programs and intellectual property is however comparatively new. Only recently has the tension graduated from theoretical concern to popular news. It has even been suggested that hackers will be the pornographers of the new Millennium pushing the boundaries of First Amendment protection in the United States to the benefit of the public at large.

There are numerous reasons for the rise of this tension, including the rise of the personal computer, the ubiquity of the Internet (propelled by the popularity of the World Wide Web) and the rise of digital music (and, to a lesser extent, digital video) as a viable data transfer medium. Within the space of less than a decade, science fiction has become science fact. Concomitant with the growing popularity and wide appeal of computing technology, government regulation has increased. This has taken the form of legislation reflecting the interests of powerful media conglomerates to the exclusion of previously established checks and balances. The poster child for this movement is the Digital Millennium

[1] Michael B. Feldman and Elliot B. Koffman. Ada (1996): p95

[2] Brad Sherman and Lionel Bently, (1999) p1

Copyright Act, passed by the United States Congress in 1998. The criminalization of conduct neither necessary nor sufficient for copyright infringement ignores the rights to which the populace (and especially the computing populace) has become accustomed, and gives well-funded media copyright holders unprecedented power over their works.

The emergence of a dialogue on the appropriate protections for computer programs and computer data is an opportunity to critically evaluate the multitude of purposes for which computers are now used. Politicians and law-makers are still, for the most part, ignorant of issues in the computing community and the computing community can still, for the most part, not persuasively communicate with politicians and regulators. This is something which must change.

The importance of computer software has immensely emerged due to the vast development in information technology throughout the world. Accordingly, the protection of the right of the creator of the computer software was realized, because in the absence of the protection of the right of the creator it is difficult to imagine real development in this field. The rapid evolutions of computer technology raises difficult questions about the scope of the protection the law should afford computer programs.

Computer programs are uniquely different from traditional literary works protected by copyright law because they have machine-like properties, are primarily functional in nature and frequently distributed in a form that human cannot read. Despite these differences, however, computer programs have received protection under the copyright paradigm along with literary and artistic works.

Today's central controversial issue is whether the law should allow competitors to reverse engineer a computer program to ascertain its underlying ideas, interface specification and protocols. Many computer experts and legal scholars contend that the fair use doctrine permits the reverse engineering of computer programs. Others disagree instead believe that this type of copying always infringes the rights of the copyright owner. This discrepancy highlights the basic tension between an author's rights control and the public right of access to the ideas and functions of a copyrighted work.

Complementary to the protection of computer software is the protection of computer data. The effect of the World Intellectual Property Organization Copyright Treaty (an international treaty), the Digital Millennium Copyright Act (United States legislation), The Copyright Ordinance 1962 (Amendment) Ordinance 2000 and Directive 2001/29/EC (European Union legislation) is explicated.

Building upon the preceding understanding of the extent copyright law, copyright law is then applied to four separate common behaviours in computer science: reverse engineering, peer-to-peer networking, technological protection measures and academic research. The extent of the legal protection is then critiqued and improvements to the law suggested. The thesis concludes with suggestions for remedial action and future research directions. My Honours thesis explores the issues underpinning this tension, critically evaluates the legal measures developed in response to the perceived problems and critically values a selection of technological protection measures which can be used to enforce controls on the use and distribution of digital information.

1.2 Research Problem. There are a number of examples of this tension which will be explored in this thesis. These same examples will be considered in greater detail in Chapter 4.

1.2.1 Reverse engineering. Reverse engineering is “the process of analyzing an existing system to identify its components and interrelationships, to create a representation of the system at a higher level of abstraction. It is a valuable tool for computer scientists—it is often used to examine interfaces in order to create interoperable products, sometimes in order to identify potential security problems. Copyright law restricts the ability of computer scientists to reverse engineer computer software.

1.2.2 Peer-to-peer networking. Napster, a peer-to-peer network for the sharing of music files, also attracted legal scrutiny. Copyright law restricts the ability of operators of networks because of the content which they may carry.

1.2.3 Encryption schemes. Increasingly, digital data is being protected by means of encryption. Examples of this are Digital Video Discs (DVDs) and Adobe eBooks. Publishers of the data use these schemes to control the use of the data, with the protection of copyright law. Circumventing the technological protection schemes may attract civil and criminal liability, regardless of the legality of any subsequent use of the data.

1.2.4 Trusted systems. In recent times, publishers have investigated the possibility of only distributing data through "trusted" channels—channels where constraints on the use and further distribution of works are enforced.

The extent to which these trusted systems are protected under the law is largely a concern of copyright law.

1.2.5 Academic research. Encryption research and security testing have long been domains of academic research. Academics study implementations, provide critical analyses and publish their findings. This long-standing collegial tradition is under threat due to the operation of copyright law.

1.3 Overview of contents. Chapter 2 introduces the basic concepts of copyright law and details the application of copyright protection to computer software. This chapter, Chapter 3 and Chapter 4 are dispassionate expositions of the state of the law or technology; analysis and criticism is contained in Chapter 5. Chapter 3 investigates recent changes to copyright laws, largely concerning the protection of digital data. The changes on the international level, in the United States of America and in Pakistan are identified and analyzed. Chapter 4 discusses the application of copyright law (as detailed in Chapters 2 and 3) to common behaviours of computer scientists and computing professionals. Chapter 5 critically analyses the protection given to computer programs (as detailed in Chapter 2) and the protection given to computerized data (as detailed in Chapter 3) in light of the applications detailed in Chapter 5 also concludes the thesis, summarizing the findings, suggesting a course of remedial action and suggesting further research topics.

1.4 Limitations and methodological considerations. Complementary to the protection of computer software is the protection of computer data. The study is limited to Legal Protections for computer Programmes under copyright Law of three different jurisdictions. The effect of the World Intellectual Property Organization Copyright Treaty (an international treaty), the Digital Millennium Copyright Act (United States legislation), The Pakistan Copyright Ordinance 1962 (Amendment) Ordinance 2000(Pakistan legislation) and Directive 2001/29/EC (European Union legislation) is explicated. Building upon the preceding understanding of the extent copyright law, copyright law is then applied to four separate common behaviours in computer science: reverse engineering, peer-to-peer networking, technological protection measures and academic research. The extent of the legal protection is then critiqued and improvements to the law suggested. The thesis concludes with suggestions for remedial action and future research directions.

Computer scientists are increasingly subject to the nuances of copyright law; ignorance is no longer bliss. Computing professionals (and computer scientists) often reproduce computer programs for the purposes of studying their behaviour and gleaning the principles of their operation. Oftentimes, reverse engineering is used to create interoperable products, to correct errors or to do security testing. Even academic research may attract the threat of legal action. Because of the recent encroachment of copyright law into the realm of day-to-day computer science, an examination of the issues of this thesis is relevant.

Due to the limited sources and time, this work relies on documentary evidence as the main source of data collection. The literature in the thesis is consulted includes books, articles reports, journals, and relevant case law. Due to the short time and limited resources I was unable to survey in Pakistan upon the core issue for the computer programmes i-e Software piracy. But anyhow I have try with my best efforts according to my Knowledge and guidance by My Honourable supervisor Dr. Jon Bing at University of Oslo Norway.

Chapter 2

Understanding the Concept of Legal protection for computer Programmes in EU, US and Pakistan

2. Copyright. As the name “copyright” may imply, copyright is a species of intellectual property rights concerning the reproduction of works. In a doctrinal sense, copyright protects the expression of ideas, not ideas themselves. (For example, copyright protects the text of a Mills & Boon book, but does not protect the basic plot of romance found and experienced.) A copyright holder has a bundle of exclusive rights, including the right to reproduce the work and the right to make adaptations of the work (or derivative works). The copyright holder—initially the author—may assign or license these rights to others.

2.1 History. Copyright has a long and storied history. In England, the Stationers Guild developed a monopoly over the printing of books. The Tudor and Stuart monarchs, as a convenient means of censorship, extended this to cover the importation of books. Members of the Guild, on registration of the work, obtained a perpetual right to publish the work. With the Glorious Revolution of 1688 and the exile of James II, Parliament, and not the monarch became the ascendant organ of government. The Statute of Anne was passed in 1709, granting a limited term (twenty eight years) of copyright that originally vested in the authors, rather than printers. The copyright could be subsequently assigned to the printers. Copyright evolved piecemeal until the end of the nineteenth century. The British Parliament passed an omnibus copyright act, essentially in similar terms to the Berne Convention, which essentially is the form of copyright protection in the world today.

2.2. Berne Convention. The Berne Convention for the Protection of Literary and Artistic Works was completed at Paris on 4 May 1896[3] It established “a Union for the protection of the rights of authors in their literary and artistic works.”[4] Member States of the Union agreed to a base level of intellectual property protections. Under the Berne Convention, copyright protection is automatic. The term of protection granted for literary works is “the

[3] The text of the treaty and a list of parties is available at <http://www.wipo.int/treaties/ip/berne/index.html>.

[4] Article 1

life of the author and fifty years after his death."[5] Authors of literary works are granted the exclusive right to authorize:

- Of their works;[6] "adaptations, arrangements and other alterations of their works",[7] including cinematic adaptations; [8]
- Broadcasting, "communication to the public by wire" or "public" communication by loudspeaker or any other analogous instrument" of their works;[9] and
- Public recitation of their works.[10]

A treaty is an instrument of international law, not national law. Generally, international treaties become law not when signed or ratified by governments but when (or if) they are implemented domestically. As such, international treaties are not generally a source of law. That is not to say, however, that they are completely irrelevant. It is often in governments' interests to implement treaties in domestic legislation. Principles of international comity play a part, as can the more practical motive of wishing to avoid trade sanctions[11].

In the area of intellectual property, conventions are important. The Berne Convention is widely implemented and reflects the base line of international intellectual property protection. One hundred and forty-eight countries are parties to the Berne Convention: Australia became a member of the Union on 14 April 1928, the United Kingdom on 4 December 1887 and the United States of America on 1 March 1989.

2.3 Computer programs. As computers and computer software became more prevalent during the 1970s, the question arose as to what intellectual property protection applied to computer software. Computer programs in printed-out source code form were certainly

[5] Article 7(1)
[6] Article 9(1)
[7] Article 12(1)
[8] Article 14(1)
[9] Article 11 bis(1)
[10] Article 11 ter(1)
[11] D. J. Harris. Pages 1–14. (1998.)

literary works: they satisfied the requisite elements of originality and literary value. The logical deduction from this observation was that computer programs in all forms should attract copyright protection as if they were literary works just the same as novels. This is indeed the approach that was taken (some criticisms of this approach are detailed in Section 5.1).

2.3.1 United States. In the United States, copyright law was consolidated and reformed in 1976 with the passing of the Copyright Act,[12] subsequently codified as Title 17 of the United States Code. The legislative history suggested that computer programs were included as literary works.[13] A report commissioned shortly thereafter recommended that the computer programs be explicitly mentioned to remove any doubt as to the applicability of copyright protection to computer programs.[14] Congress adopted the suggestion. (The conclusions and investigations of the report which led, in particular, to the 1980 amendments to the Copyright Act are robustly criticised. [15]

This general history is recounted in the decision of the Court of Appeals for the Third Circuit in Apple Computer, Inc. v. Franklin Computer Corporation.[16] That decision also removed any doubt as to the application of the statute, holding that computer programs in

[12] Act of Oct. 19, 1976, pub L.No, 94-553, 90stat. 1251

[13] H.R. Rep. No. 1476, 94th Cong., 2d Sess. 54.

[14] National Commission on New Technological Uses of Copyrighted Works, Final Report 1 (1979)

[15] Greg Aharonian. Deconstructing software copyright: 30 years of bad logic.<http://www.bustpatents.com/aharonian/softcopy.htm>, visited Aug 2008.

[16] 714 F2d, p1240, 46(3d cir 1983)

object code, a computer program embedded in a ROM chip and operating systems programs are covered by copyright.[17]

2.3.2 Pakistan. In Pakistan, copyright protection is governed by the provisions of the Copyright Ordinance, 1962 ("the Ordinance") Amendment 2000, which is modeled on the English Act of 1914. Pakistan is a member of Berne Copyright Union and the Universal Copyright Convention.

2.3.3 Recent Developments. One of the most significant developments in relation to the protection of copyright in Pakistan is the recent promulgation of the Copyright (Amendment) Act, 2000 ("the Amendment Act"). Copyright protection originally available to literary, dramatic, musical, artistic, cinematographic and architectural works, books, photographs, newspapers, engravings, lectures, records (defined as "any disc, tape, wire, perforated roll or other device in which sounds are embodied so as to be capable of being reproduced there from, other than a sound track associated with a cinematographic work") and sculptures is now extended to computer software, periodicals, video films and all kind of audio-visual works.

The Ordinance now provides stiffer penalties for offenders and better compensation to the persons whose rights have been infringed. The manner in which the copyright is breached has also been extended. Entirely new offences have been created through the Amendment Act which, inter alia, include penalties for publishing collections or compendiums of work (the Ordinance defines "work" to include literary, dramatic, musical, artistic, cinematographic works and a record) which have been adapted, translated or modified in any manner without the authority of the owner of the copyright.

Section 37[18] of the Copyright Ordinance 2000 has been amended to restrict granting of licences to produce and publish translation of a literary or dramatic work in English, French or Spanish, hence an applicant requesting the grant of license, upon granting of the licence

[17] Apple computer 714 , F2d at p1249

[18] Sec. 37 The Copyright Ordinance 1962,(Amendment) Ordinance 2000

and payment of prescribed royalty to the author, can produce and publish translation of a literary or dramatic work in any Pakistani language or any language not being English, French or Spanish.

2.3.4 Copyright for Computer programmes in Pakistan. In Pakistan, computer programmes are excluded from patent protection under the patent laws. Protection under the copyright laws is the only safeguard available for the computer software industry. Under the provisions of the Copyright Ordinance, 1962, Copyright protection is only available for `works' which fit within one of the categories of works or subject matters specified in the Ordinance. Section 10[19] of the Ordinance provides that copyright subsists, inter alia, in original, literary, dramatic, musical and artistic works.

2.3.5 What is computer program? As regard to the computer programmes the definition of `literary work' is amended by the Copyright (Amendment) Act, 1992 ("the Amendment Act") to include computer programmes. Section 2(p) of the Ordinance defines literary work to include work, inter alia, on complications and computer programmes, "that is to say programmes recorded on any disc, tape, perforated media or other information storage devices, which, if fed into or located in a computer or computer based equipment is capable of reproducing any information".

2.3.6 Infringement of Computer Programmes. Pursuant to the restrictions imposed under Section 56 of the Ordinance, even the purchasers of computer programmes may not copy, adapt or make copies of adaption of the programmes in connection with their use by themselves or their employees. The unauthorised use of a computer programme in a computer is also infringement of the copyright. Accordingly, if a duplicate of a computer programme is acquired by someone who has no licence to use it, the copyright owner has the right to prevent him using it. Section 56[20] also restricts rental of computer programmes to un-authorised users. Intention to copy computer programmes is not an essential ingredient of infringement; nor is it essential that the copying be in the same medium. Thus, a computer programme stored on diskettes (or any other magnetic media) can be infringed by copying the same on paper, or taking a print-out of the same.

[19] Sec. 10 The Copyright Ordinance 1962,(Amendment) Ordinance 2000

[20] Sec. 56 The Copyright Ordinance 1962,(Amendment) Ordinance 2000

2.3.7 Liability for Infringement. In the event of infringement, liability of infringement falls upon the person who, without the consent of the owner of the computer programme does any of the restricted acts; or authorises any other person to do any such acts; or commits any acts of infringement.

2.4. International consensus. The Berne Convention was last amended in 1979; the definition of literary and artistic works in Article 2(1) does not expressly include computer programs. Further treaties have addressed this gap, proscribing that computer programs should be protected by copyright law as literary works. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) is Annex 1C to the World Trade Organization Agreement. It must be agreed to by any nation wishing to join the WTO. The WTO was established on 1 January 1995; as of 26 July 2001, there were 142 member countries of the WTO. Regarding computer software, TRIPS reflected the orthodoxy of the time:[21] Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).

The World Intellectual Property Organization Copyright Treaty, completed in 1996, also contains a similar provision:[22] Computer programs are protected as literary works within them earning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression. Again, this does little beyond recognize the way that computer programs had been dealt with in national law and, indeed, in TRIPS.

2.4.1 Software licensing. The protection of computer programs as literary works is automatic in all Berne Convention countries, requiring no registration or extra effort on the part of the author. As noted in Section 2.2, one of the exclusive rights granted to the author of a literary work is the right to reproduce the work. Without the consent (or license) of the copyright holder, no one can substantially reproduce the copyrighted work. For computer programs, this is pervasive: the execution, backing up and downloading of computer software all involve the making of reproductions. Many of these necessary reproductions

[21] TRIPS Article 10(1)

[22] WCT 1996 Article 4

are now expressly protected by copyright legislation; other uses require a license from the author of the software.

Accordingly, a license is the general way that software is distributed. Computer software is rarely sold for several reasons. First, selling computer software involves the copyright holder relinquishing control over the work. Additionally, in the United States, the “first sale doctrine”[23] provides that after the first sale of a copy of a work, the buyer can further sell or dispose of the work as he or she sees fit. This is obviously undesirable for computer software authors, so licensing is the preferred means of retaining control over the copyrighted software.

2.4.2 Shrink-wraps, click-wraps and browse-wraps. For bundled, packaged computer software, the computer industry licensed their software by the use of “shrink-wrap” licenses. A consumer went to their software store of preference, exchanged money for a pack-age containing the software in question, then came home to install it. Enclosed within the shrink-wrapped package was a license (hence the name “shrink-wrap license”). Via a dialog box, or something similar, in the initial installation of the software, the user agreed that they had read the license (another copy may be displayed as part of the installation process).

This was accepted by courts as being a binding license. An extension on this same theme was the so-called “click-wrap” license. These are a feature of online software distribution. With online software, there are no boxes—nothing to shrink-wrap. The user is informed of the software license by displaying the license and forcing the user to manifest their assent to the terms of the license (or “click-through”). The trend of courts in the United States is to accept these licenses as legally binding. In Pakistan, the validity of shrink-wrap or click-wrap licensing has not been decided, however copyright notices in a prominent place in distribution is sufficient.

A recent attempted extension to this notion is that of a “browse-wrap” license, where the license terms are pointed to by a link on the download page, or somewhere similar. Licenses like this have only recently been litigated. In the two cases decided in the United States, their validity has been impugned on both occasions. The distinction between the

[23] 17 U.S.C. ss 109

valid click-wrap licenses and invalid browse-wrap licenses is that users did not have to see, let alone agree to, the browse-wrap license's terms. As there are valid means to dictate a license agreement for computer software, some attention needs to be drawn to what the contents of license agreement can be.

2.4.3. Proprietary software. Typically, software produced by large vendors is widely known as "proprietary" software. This software is licensed under terms which give the users of the software as few rights as possible. Key features of a proprietary software license (also known as an End-User License Agreement, or "EULA") are:

- Limitation of liability: The vendor requires the user to waive or limit the extent to which the user holds the vendor liable for any damages caused by the software.
- Limitation of warranty: The vendor disclaims all warranties and guarantees which it can under law. This includes warranties such as fitness for purpose and quality which are customarily implicit in commercial transactions.
- Limitation of activity: The vendor restricts the use of the software to that which is necessary for the normal use of the software. Importantly, reverse engineering (except to the extent allowable by law) is invariably forbidden.
- Limitation of modification: The vendor restricts the ability of the use to modify the software, regardless of the purpose of any such modification.
- Limitation of transfer: The vendor often restricts the user from further copying the software for someone else or even from transferring the software to someone else.
- Limitation of law or forum: Many proprietary EULAs also include clauses as to the forum or substantive to be applied when there is a dispute about the license or the software. The forum is where someone can sue—this is typically a convenient forum for the vendor. Additionally, the substantive law which governs the license is also typically favourable to the vendor. The key features noted above are present in the sample EULAs.

2.4.4. Open software. A completely different tack to proprietary licensing can be taken—instead of keeping the code as secret, closed and proprietary as possible, it can be kept open so that users can see the source code and oftentimes modify it for their own purposes.

2.4.5. Open Source. “Open source” is a term used by the Open Source Initiative to refer to software licensed under conditions which fulfil a set of criteria.[24] The Open Source Initiative believes that open source software is of better quality and more rapidly developed than proprietary equivalents. They make a business case for open source software. From their Web site, <http://www.opensource.org/>: When programmers can read, redistribute, and modify the source code for a piece of software, the software evolves. People improve it, people adapt it and people fix bugs. And this can happen at a speed that, if one is used to the slow pace of conventional software development, seems astonishing. We in the open source community have learned that this rapid evolutionary process produces better software than the traditional closed model, in which only a very few programmers can see the source and everybody else must blindly use an opaque block of bits. [25]The Open Source Initiative also has a certification program. Open Source Initiative exists to make this case to the commercial world Open Source software is licensed under conditions completely unfamiliar to typical proprietary software. The key components of the Open Source Definition are:

- Freedom of distribution: The software must be able to be distributed without restriction. This includes being able to sell the software at a profit.
- Availability of source code: The source code to the software must be available. The source code must not be deliberately obfuscated, and must be the preferred form for modification of the program.
- Freedom of derivation: Making derived works from the software must be allowed, and the derived works must be able to be distributed under the same terms as the original software.

(An exception to this is that the author of code can insist that any derived works are labelled as such. Further, it is possible that the author can only allow modifications to be distributed as “patch files” to the original software. In this way, the origin of the software can be clearly identified for end users.)

[24] Open Source Initiative. Open source definition.<http://www.opensource.org/docs/definition.html>.Visited 30 Aug 2008

[25] Karen E. Georgenson. 1996, p 320

- No discrimination: There must be any discrimination in the license terms against persons, groups or fields of endeavour.
- Generality: The license must not be dependent on the software being included in a larger distribution or part of another piece of software.

2.4.6. Free software. “Free software” is a subset of open source software, premised on a more ideological basis. The Free Software Foundation, in contrast to the Open Source Initiative’s commercial pitch, focuses on the freedom of software consumers to modify their software and otherwise deal with it in a collegial and co-operative manner. The Foundation identifies four desired freedoms [26]

0. The freedom to run the program, for any purpose;

1. The freedom to study how the program works and adapt it to specific needs;

2. The freedom to redistribute copies to help others;

3. The freedom to improve the program and release your improvements to the public for the entire community to benefit.

The freedoms are numbered from zero because the zeros freedom is more fundamental than the others. Access to the source code for computer software is necessary for freedoms one and three. The philosophical and ideological basis for free software is essentially voluntary cooperation amongst computer users.

2.4.7. Comparison with proprietary software. As a cursory comparison with the features of a proprietary license above should indicate, there is a significant difference between the permissible uses of software licensed under a proprietary license and those permitted under an open source license agreement. The quantum shift which open source (and free software) provides has attracted the attention of some legal academics, many of whom effuse about the possible implications of the widespread use and distribution of open source software[27].

[26] Free Software Foundation. The free software definition<http://www.gnu.org/philosophy/free-sw.html>.Visit July 2008

[27] David McGowan. (2001) p241–304,

2.5 Protected uses. In order to deal with the limitations customarily included in proprietary software licenses, it is necessary to protect some basic uses of computer programs. Copyright law recognises this, ensuring that some basic uses are always available to end users.

2.5.1 Ordinary course of operation. Running a computer program involves it being copied from the secondary storage on which it resides into RAM. Being a reproduction, this is prima facie a copyright infringement. In the United States, such copies were held to infringe copyright. Copyright law was amended to overrule this decision.[28]

In the European Union, acts done by the lawful acquirer necessary for the use of the program are protected from infringing copyright.[29]

2.5.2. Study. Being able to study a computer program is important. Indeed, the essence of copyright protection is that it only protects the expression of an idea, not the idea itself. It should therefore be permissible to reproduce a computer program in order to study it. In the United States, this is covered by fair use. In Pakistan, this is permitted by statute the studying must be done by the owner of the copyright or a licensee. It does not apply where the copy being studied is an infringing copy. An important restriction on the operation of the exception: the "reproduction" cannot, however, be de-compilation, disassembly or any other form of reverse engineering.

This reduces the ability to study a computer program except to, effectively, just use it normally. In the European Union, this has been permitted since 1991. If someone has the right to use a computer program, they cannot be precluded from "observ[ing], study[ing] or test[ing] the functioning of the program in order to determine the ideas and principles which underlie any element of the program".[30] However, like the Pakistani provision, a restriction on the operation of the provision is that the user can only make their observation, study or testing while performing permitted acts (which can exclude reverse engineering, except for the purpose of interoperability).

[28] D. J. Harris. 1998, p1–14

[29] Directive 91/250/EC Article. 5(1)

[30] Directive 91/250/EC Article 5(3)

2.5.3. Back-up copies. Making a back-up copy of a computer program is also important, yet is technically forbidden by copyright law. In the United States, it is permitted to keep a copy of a computer program for "archival purposes", providing any archived copies are destroyed should the original copy become unlicensed. In Pakistan, making back-up copies is expressly permitted as well. The section only applies to bona fide back-up copies, however: the software being backed up must have a valid license. In the European Union, the right of a user of a computer program to make a back-up copy is likewise protected[31].

2.5.4. Reverse engineering. For some purposes, reverse engineering of computer software is also protected in the United States, Pakistan and the European Union. This is discussed in detail in Section 4.1.

2.6. Summary. International orthodoxy is that computer programs are protected by copyright as literary works, granting the copyright holder of a computer program the exclusive right to authorise the reproduction of the work. For computer programs, this is an extensive right because computer programs are useless unless reproduced. Although generally software distributors reserve as many rights as possible through their license agreements, a kernel of basic uses of computer software is protected by law in the United States, Pakistan and the European Union.

[31] Directive 91/250/EC Article 5(2)

Chapter 3

3. Protecting computerized data. Separately from the protection of computer programs, computerized data is also protected. In the last half-decade the protection of computerized data has been the subject of legislative consideration and promulgation.

3.1. International treaties. The basis for recent legislation in the United States, Pakistan and the European Union is two treaties from the World Intellectual Property Organization (WIPO). As these treaties have been signed by many countries, examination of the effects of the treaty obligations is germane.

3.1.1. WIPO Copyright Treaty. The WIPO Copyright Treaty (WCT), adopted in Geneva on 20 December 1996, is a re-negotiation of copyright law for a modern time (albeit influenced by the lobbying of rights holders such as record labels and movie studios). Building upon the Berne Convention[32] it re-iterates the basic premise of copyright law:[33]

Copyright protection extends to expressions and not to ideas, procedures, Method of operation or mathematical concepts as such.

Regarding computer software, the WCT re-states the orthodox position, that computer programs are literary works:[34]

Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression. Building upon TRIPS, the WCT contemplates the rental of computer software.[35] Articles 11 and 12 contemplate the widespread digital distribution of copyrighted material. Article 11 deals with technological protection measures, providing that parties to the treaty provide legal protection to technological measures: Contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

[32] Article 1 and 3

[33] Article 2

[34] Article4

[35] Article7

Article 12 communicates a similar sentiment vis-`a-vis rights management information:

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal and infringement of any right covered by this Treaty or the Berne Convention:

(i) To remove or alter any electronic rights management information without authority;

(ii) To distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

The Treaty goes on to talk about enforcement of these rights, stating in Article 14:

(1) Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

(2) Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements. There are also a series of Agreed Statements to the WCT. These are essentially aids to interpretation of the treaty. Concerning Article 1(4), it was agreed that converting data into digital form is a reproduction for the purposes of copyright law.

The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted there under, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention. Concerning Article 4, the contracting states agreed that the protection of computer programs under the WCT is consistent with other international treaties.

The scope of protection for computer programs under Article 4 of this Treaty, read with Article 2, is consistent with Article 2 of the Berne Convention and on a par with the relevant provisions of the TRIPS Agreement.

Concerning Article 12, it was agreed that rights of remuneration may also be protected by rights management schemes. Additionally, the rights management schemes should not impose additional formalities impeding the enjoyment of established rights.

It is understood that the reference to "infringement of any right covered by this Treaty or the Berne Convention" includes both exclusive rights and rights of remuneration. It is further understood that Contracting Parties will not rely on this Article to devise or implement rights management systems that would have the effect of imposing formalities which are not permitted under the Berne Convention or this Treaty, prohibiting the free movement of goods or impeding the enjoyment of rights under this Treaty. It is primarily this treaty which has provided the basis for national legislation in the United States, Pakistan and the European Union.

3.1.2 WIPO Performance and Phonograms Treaty. The WIPO Performances and Phonograms Treaty (WPPT) Exhorts the same course of action, primarily in the context of performers. The preamble records that the Contracting Parties:

Desiring to develop and maintain the protection of the rights of performers and producers of phonograms in a manner as effective and uniform as possible, Recognizing the need to introduce new international rules in order to provide adequate solutions to the questions raised by economic, social, cultural and technological developments, Recognizing the profound impact of the development and convergence of information and communication technologies on the production and use of performances and phonograms, Recognizing the need to maintain a balance between the rights of performers and producers of phonograms and the larger public interest, particularly education, research and access to information have agreed Performers, the focus of the WPPT, are defined as actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret, or otherwise perform literary or artistic works or expressions of folklore.

As the preamble notes, the WPPT recognizes that technology is increasingly used as a means of communicating music. To wit, it contains substantively identical provisions as the

WCT for obligations concerning technological measures8 and obligations concerning rights management information. Indeed, even the Agreed Statements at the Diplomatic Conference Echo each other.

The agreed statement concerning Article 12 (on Obligations concerning Rights Management Information)[36] of the WIPO Copyright Treaty is applicable mutatis mutandis also to Article19 (on Obligations concerning Rights Management Information) of the WIPO Performances and Phonograms Treaty.

The WIPO Performances and Phonograms Treaty, therefore, provides additional support in international law for nations to enact laws concerning technological protection measures of copyrighted works and rights management information embedded in, or associated with, copyrighted works.

3.2 United States. The WCT and WPPT were implemented in the United States by the Digital Millennium Copyright Act. Recently, further legislation has been proposed to extend further the reach of copyright law.

3.2.1 Digital Millennium Copyright Act. Passed in 1998, the Digital Millennium Copyright Act (DMCA) is, according to the preamble, “An Act . . . to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty”. For present purposes, the key provisions introduced to United States copyright law by the DMCA are contained in a new Chapter 12, entitled “Copyright Protection and Management Systems”.[37]

3.2.2. Technological protection measures. The primary provision of the DMCA concerns technological protection measures: measures which regulate access to copyrighted works.

3.2.3. Base prohibitions. The base provision of the DMCA is a broad prohibition: [38] No person shall circumvent a technological measure that effectively controls access to a work protected under this title. An additional violation is to “manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof that” is primarily designed to circumvent technological protection

[36] Article12 WCT

[37] 17 U.S.C. § 1201

[38] 17 U.S.C. § 1201(a)(1)(A).

measures,[39] has only a limited commercial purpose other than to circumvent technological protection measures[40] is marketed for the circumvention of technological protection measures.[41] Interestingly, despite the cries that the DMCA means the end of fair use, the DMCA itself pays lip service to the notion of fair use:[42] Nothing in this section shall affect rights, remedies, limitations, or defences to copyright infringement, including fair use, under this title.

However, it has been held that the circumvention provisions are a new balance struck by Congress. Indeed, fair use has effectively vanished under the DMCA[43]. This issue is further explored in Section 5.2.5.

3.2.4 Non-profit libraries, archives and educational institutions. A non-profit library, archive or educational institution can make a good faith determination as to whether acquire a "commercially exploited copyrighted work" for the sole purpose of engaging in conduct allowed by copyright law without worrying about the anti-circumvention provision.[44]

3.2.5. Law enforcement, intelligence and other government activities. Any officer, agent or employee of the United States, a State or a political subdivision of a State, or person acting pursuant to a contract with any of those entities is, for most relevant purposes, not constrained by the DMCA.[45]

3.2.6 Interoperability. A person can circumvent technological protection measures on a lawfully obtained copy of a computer program for the sole purpose of identifying and analyzing the program to create an interoperable product, providing the information was

[39] 17 U.S.C. § 1201(b)(1)(A).
[40] 17 U.S.C. §1201(b)(1)(B).
[41] 17 U.S.C. § 1201(b)(1)(C).
[42] 17 U.S.C. § 1201(c).
[43] David Nimmer. p673, (2000).
[44] 17 U.S.C. §1201(d).
[45] 17 U.S.C. § 1201(e).

.

not previously readily available.[46] Importantly, the circumvention must be for the "sole purpose" of creating an interoperable program. Any public dissemination of the information is impermissible.[47]

3.2.7. Encryption research. An important reason to attempt to circumvent electronic protection measures is to engage in encryption research. Technological protection measures can be circumvented on lawfully obtained works (including phono-records) where necessary for security research.[48] The researcher must have made a good faith effort to obtain authorization from the copyright holder first,[49] and the circumvention cannot otherwise be unlawful.[50] In order to determine whether a person was, in fact, engaging in security research the DMCA provides three factors for a court to consider.[51]

First, whether and if so to what extent the information was disseminated and whether the dissemination facilitates copyright infringement.[52]

Second, the extent to which the researcher can be characterized, as a researcher in the field of encryption technology.[53]

Third, whether the copyright holder is provided with notice of the findings of the research and the timeliness of such notice.[54] These constraints are intended to limit the availability of the exception to academics and established researchers in the field.

3.2.8 To protect personally-identifying information. In accordance with the lasseiz-faire approach of the United States to privacy on the Internet, any circumvention of a protection measure where the information that is being protected is personally identifying information about the online activities of a natural person.[55] This license to circumvent is restricted: the collection of information must be surreptitious,[56] the circumvention must have the sole

[46] 1917 U.S.C. §1201(f)(1).
[47] 17 U.S.C. §1201(f)(3)
[48] 17 U.S.C. §1201(g).
[49] 17 U.S.C. § 1201(g)(2)(C).
[50] 17 U.S.C. § 1201(g)(2)(D).
[51] 17 U.S.C. § 1201(g)(3)
[52] 17 U.S.C. § 1201(g)(3)(A).
[53] 17 U.S.C. § 1201(g)(3)(B).
[54] 17 U.S.C. § 1201(g)(3)(C).
[55] 17 U.S.C. § 1201(i)(1)(A).
[56] 17 U.S.C. § 1201(i)(1)(B)

effect of identifying and disabling the information collection capability[57] and the circumvention is for the sole purpose of preventing the collection of the information and isn't otherwise prohibited.[58]

3.2.9 Security testing. Technological protection measures may have security implications, they are often kept secret and proprietary[59], therefore there is an exception for "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network"[60] as long as it does not otherwise constitute a violation of law.[61]

Like the encryption research provision, there are two factors to be taken into account by a court when considering whether the exception should apply.[62] First, whether the information resulting from the security testing is used to promote the security of the tested systems or networks.[63] Second, whether the information resulting from the security testing facilitates the infringement of privacy or other law.[64]

3.2.10. Copyright management information.

The DMCA provides that no person can, with the intent to induce, enable, facilitate or conceal copyright infringement, provide, distribute or import false copyright management information.[65] Further, no person can without the consent of the copyright owner or legal authority[66]

[57] 17 U.S.C. § 1201(i)(1)(C).
[58] 17 U.S.C. § 1201(i)(1)(D).
[59] <http://cryptome.org/sdmi-attack.htm> visited on September 2008 visited 15 july 2008
[60] 17 U.S.C. § 1201(j)(1)
[61] 17 U.S.C. § 1201(j)(2). [62] 17 U.S.C. § 1201(j)(3).
[63] 17 U.S.C. § 1201(j)(3)(A). [64] 17 U.S.C. § 1201(j)(3)(B).
[65]17 U.S.C. §1202(a).
[66] 17 U.S.C. §1202(b)

(1) Intentionally remove or alter any copyright management information

(2) Distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or

(3) Distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law, if they know it will induce, enable, facilitate or conceal copyright infringement. For civil actions, it is merely sufficient that the person had reason to know. There is also no liability for law enforcement or governmental agents.[67]

3.2.11. Civil remedies. “Any person injured” by a breach of one of the above sections can bring action in an appropriate United States District Court[68]. In such an action, the court can grant injunctions,[69] can impound[70] and subsequently order the destruction of devices,[71] award the recovery of costs[72] and attorney’s fee[73]. The court can also award damages.[74] The damages can consist of either actual damages (those suffered by the party bringing the action and the profits of the violator attributable to a violation) or statutory damages (a prescribed sum per violation).[75]The court can award triple damages for repeated violations,[76] and reduce the amount of damages for violation where the violator was not aware and had no reason to be aware they were violating the law.[77]

[67] 17 U.S.C. § 1202(d). This provision is substantively identical to 17 U.S.C. § 1201(e).

[68] 17 U.S.C. §1203(a).

[69] 17 U.S.C. §1203(b)(1).

[70] 17 U.S.C. §1203(b)(2).

[71] 17 U.S.C. §1203(b)(6).

[72] 17 U.S.C. § 1203(b)(4).

[73] 17 U.S.C.§1203(b)(5).

[74] 17 U.S.C. §1203(b)(3), (c).

[75] 17 U.S.C. §1203(c)(2)–(3).

[76] 17 U.S.C. § 1203(c)(4)

[77] 17 U.S.C. § 1203(c)(5).

3.2.12. Criminal remedies. Any person (excepting a non-profit library, archive or educational institution)[78] who violates sections 1201 or 1202 "wilfully and for purposes of commercial advantage or private financial gain" is also liable for criminal penalties.[79] The first offence is punishable by $500,000 and five years imprisonment. [80] Subsequent offences attract a doubled maximum penalty.[81]

3.2.13. Intermediate copies during transit. Recognizing that intermediate copies are often made during the transfer of files over the Internet, the DMCA addresses the issue of intermediate liability. [82] "However, the DMCA's cumbersome and disorganized structure makes its provisions difficult to untangle". The DMCA recognizes and protects:

- Transitory network communications: Reproductions of copyrighted material made by a passive network provider who, without manual intervention, provides connectivity;[83]
- System caching: Network providers who provide caches of information (in accordance with relevant technological standards) to provide better network efficiency are protected against copyright infringement actions for the contents of their caches;[84]
- Safe harbour: Operators of networks containing user data are not liable for infringing content on the networks if the network operators (a) do not have actual

[78] 17 U.S.C. § 1204(b).
[79] 57 U.S.C. § x 1204(a).
[80] 17 U.S.C. § 1204(a)(1).
[81] 17 U.S.C. § 1204(a)(2).
[82] 17 U.S.C. § 512
[83] 17 U.S.C. § 512(a).
[84] 17 U.S.C. § 512(b).

knowledge of the infringement, (b) is not aware of facts or circumstances from which it would be apparent that infringement is taking place, or (c) upon learning of the infringement expeditiously acts to remove or disable access to the infringing material; [85]

- Search engines: Reproductions of copyrighted material made in order to facilitate linking or indexing of material are protected from copyright infringement.[86] These protections do not apply to the circumvention provisions—they are not available where an action has been brought alleging trafficking in a circumvention device.

3.2.14. Recent legislative proposals. The Security Systems Standards and Certification Act (SSSCA) is U.S. legislation proposed by Senator Fritz Hollings, chairman of the Senate Commerce Committee. A working draft of the proposed legislation is available. Essentially, it seeks to ensure all digital devices contain federally-mandated copy protection technology; to produce a device without such facilities would be illegal and to remove or alter the security technology would likewise attract sanction. The only defence available to infractions is the time-shifting network television. This exception is, however, exceedingly narrow and is essentially limited to the facts of Sony Corp. v. Universal City Studios, Inc[87]. Reaction to this legislation has largely been by way of condemnation; this is discussed in Section 5.3.5.

3.3 Pakistan. As a member of the WTO, Pakistan is committed to fulfil its TRIPS obligations. Pakistan is also a member of the Berne Convention on copyrights and the World Intellectual Property Rights Organisation (WIPO), but is not a member of Paris Convention for protection of intellectual property.

In order to fulfil its obligations under TRIPS, (January 2000 was the deadline for implementation of TRIPs for developing countries), Pakistan's Copyright Ordinance, 1962, was amended by the Copyright (Amendment) Ordinance, 2000. It deals with many of the TRIPS deficiencies noted in the US '2000 Special 301 report'[88], but it is not in effect as yet. Defining and identifying various products that constitute subject matter of copyright

[85] 17 U.S.C. § 512(c).

[86] 17 U.S.C. § 512(d).

[87] Sony Corp. v. Universal City Studios, Inc.,464 U.S. 417 (1984). The case is examined in more detail in Section 4.2.1.

[88] IIPA 2003 SPECIAL301 REPORT

ownership is crucial in establishing a right in this regard. For instance the copyright products are not just visible things but even ideas and themes. While such ideas and themes may not be registered as copyright doing so would make it easier to claim the same in a court of law.

3.3.1. Software Piracy in Pakistan - Building a case for ICT Software Freedom. At this point in time amidst the harsh implications that Pakistani citizens will shortly be facing after 20th May 2006 when the Anti-Software piracy crackdown is enforced by Business Software Alliance BSA (Mild least) in cooperation with the Intellectual Property Organization and Federal Investigation Authorities of Pakistan, this article is an effort to mobilize regional and international community support through media and the FOSS (Open Source Software is software which is liberally licensed to grant the right of users to study, change, and improve its design through the availability of its source code) advocates for FOSSFP so that FOSSFP may continue to massively educate and protect the citizens of Pakistan from the implications of Software Piracy by educating them on Free and Open Source Software as an alternative to pirated software.

3.3.2. What are the copyright act amendments, addition of Software? The government has rewritten and amended legislation in the areas of copyrights, patents, and trademarks. Copyright law in Pakistan was governed by the Copyright Ordinance 1962. Significant changes were made in it through the Copyright (Amendment) Act, 1992 and the Copyright (Amendment) Ordinance 2000 whereby Copyright protection originally available to literary, dramatic, musical, artistic, cinematographic and architectural works, books, photographs, newspapers, engravings, lectures, records (defined as "any disc, tape, wire, perforated roll or other device in which sounds are embodied so as to be capable of being reproduced there from, other than a sound track associated with a cinematographic work") and sculptures was extended to include computer software, periodicals, video films and all forms of audio-visual works.

As Pakistan is a signatory to Trade Related Intellectual property Rights, Agreement (TRIPs) under WTO, it was necessary to upgrade the national intellectual property infrastructure inline to the global trends. Accordingly the existing legislation on Intellectual Property i.e. Copyrights, Patents and Trademarks have been upgraded and the revised laws have been promulgated as follows,

- The Patents ordinance 2000

- The Registered Designs Ordinance 2000

- The Registered Layout-Designs of Integrated Circuits Ordinance, 2000

- The Copyrights Ordinance, 1962 (As amended vide Copyrights Ordinance 2000)

- The Trade Marks Ordinance 2001

3.3.3. Identifiable interests that were lobbying in favour of the amendment?

The amendment is definitely not one sided, there are a number of actors here

1. Business Software Alliance Members that are all multinational companies
2. Government actors who want to direct economic and monetary gains from foreign investments.
3. The Pakistani IT Industry, want to protect their IPR and exploit a local software industry
4. Entrepreneurs who know nothing about the innovative and knowledge benefits of Free and Open Source Software.

3.3.4. What are the penalties? Pakistan’s copyright law prohibits reproduction of software without permission from the owner of the copyrighted computer program. If caught with pirated software, you or your company may be prosecuted under the provisions of the Copyright Laws. The penalties under the law include a fine of up to Rs.200.000, seizure of products used for illegal copying, and a prison sentence of up to three years.

3.3.5. Your responsibilities as a user. Your first responsibility as a software user is to purchase original programs for your use every computer at your place of business must have its own set of original software and accompanying documentation. It is illegal to purchase a single copy of original software to load onto more than one computer, or to lend, Copy or distribute software for any reason without the prior consent of the software manufacturer. When purchasing software, make sure you buy legitimate products. Many counterfeit packaged products are designed to look similar to the original manufacturer’s products but are of inferior quality. Purchasers and users of counterfeit or copied software face unnecessary risks: viruses, corrupt disks, or otherwise defective software (or illegally copied).

3.3.6. Inadequate documentation. Lack of technical product support available to registered users Lack of software upgrades offered to registered users. In addition, if you purchase software that is counterfeit or copied, you not only deny the software developer its rightful revenue, you harm the industry as a whole. All software developers, both big and small, Pakistani or foreign spend literally years developing software for public use. A portion of every rupee spent in purchasing original software is funnelled back into research and development so that better and more advanced software may be produced. When you purchase counterfeit software, your money goes directly into the pockets of software pirates.

Government commitment to law enforcement The Pakistan Government will protect the rights of copyright owners. Surprise raids will be conducted and deterrent penalties will be imposed. These raids against software pirates will continue to encourage the purchase of original software.

In a nutshell copyright is an area of law that protects the original work of authors to encourage development of industrial and cultural enterprises as well as technological businesses based on computer software.

3.5 The European Union. The European Union has also taken steps to implement the WCT provisions. Despite work beginning soon after the passing of the treaty in 1996, the European Union Council has only recently (April 9, 2001) accepted a directive designed to comply with the requirements[89]. For the most part, the provisions are substantively similar to analogous provisions in the DMCA, as such, will only be briefly described here. Relevant provisions from The Directive 2001/29/EC is extracted.

In broad general terms, Article 5 provides for the indemnity of network access providers for the mechanical reproduction of online material. The protections of Article 6 of the Directive are of a similar scope to that provided for by the United States, and in Pakistan. Therefore, the provision on technical protection measures for computer programs applies in parallel to the more extensive regulation in the Copyright Directive[90].

[89] <http://www.eurorights.org/eudmca/>. Visited Sep 2008

[90] Jon Bing, Article upon Copyright protection of computer programs, p 16

3.6 Summary. Because domestic legislative reform for the copyright protection of computerized data came from a common base, namely the WCT, the protection in the United States, Pakistan and the European Union is substantially uniform.

Chapter 4

4. Applying the law to the technology. The heretofore latent tension between copyright and technology has recently been made apparent in several distinct factual scenarios. The facts and technology behind some of these scenarios will be examined in this chapter, as well as the legal implications.

4.1 Reverse engineering. Generally speaking, reverse engineering is a permitted use of copyrighted works. Reverse engineering is a lawful way to acquire know-how about manufactured products. Reverse engineering may be undertaken for many purposes. I will try to concentrate in this section on reverse engineering undertaken for the purposes of making a competing product because this is the most common and most economically significant reason to reverse engineer in this industrial context, this is the essence of copyright protection—it only protects the expression of a work, not the general ideas which underlie it. Computer software is, however, different. In order to examine how a computer program works, it needs to be reproduced. Therefore, a copyright holder in a computer program could—theoretically—preclude any reverse engineering as part of the license agreement, as reproduction is an exclusive right granted to the copyright holder. This would seem to be manifestly unfair. If the purpose of the reverse engineering is not to copy code but merely to re-implement concepts, then to prohibit reverse engineering would be to permit patent-like protection for the bargain-basement price of copyright[91]. The legal "right" to reverse engineer a trade secret is so well-established that neither courts nor commentators have perceived a need to explain the rationale for this doctrine. This would seem to be contrary to public policy, as well as the original stated goals of copyright protection.

4.1.1 European Union. The European Union was the first jurisdiction to acknowledge the utility of reverse engineering for the purpose of interoperability. With Directive 91/250/EEC, passed on 14 May 1991, expressly permitted the reverse engineering of computer programs "to achieve the interoperability of an independently created computer program with other programs"[92] There are conditions on this largess. The program being

[91] <http://www.bustpatents.com/aharonian/ softcopy.htm>, visited August 2008

[92] Article 6

reverse engineered must be a valid licensed copy,[93] the information required for creating an interoperable product must not be readily available,[94] the reverse engineering is limited to the extent necessary to achieve interoperability,[95] the information must not be used for any other purpose than to develop the interoperable product,[96] and unnecessary further dissemination is prohibited.[97]

The Directive also provides that reproduction is permissible, regardless of the license on the software, for the purposes of error correction,[98] or studying the program in order to determine the underlying principles of its operation.[99]

4.1.2 United States. In the United States, the epicentre of the computing revolution, this matter arose in litigation in the early 1990s. The United States Court of Appeals, the federal court immediately below the Supreme Court, used the "fair use" defence to copyright infringement to allow reverse engineering for interoperability. Section 1201(f) 0f DMCA provides three exemptions to the anti-circumvention provisions relating to reverse engineering and interoperability.

4.1.3 Reverse Engineering for Interoperability of an Independently Created Computer Programme. Section 1201(f) (1) of DMCA provides that, notwithstanding the prohibitions in Section 1201(a)(1)(A) of DMCA, a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

The language in Section 1201(f) requiring that the reverse engineering be for the sole purpose of "identifying and analyzing those elements of the program that are necessary to

[93] Article 6(1)(a)
[94] Article 6(1)(b)
[95] Article 6(1)(c)
[96] Article 6(2)(a)
[97] Article 6(2)(b)
[98] Article5(1)
[99] Article5(3)

achieve interoperability of an independently created computer program with other programs" comes directly from Article 6 of the European Union Software Directive, and appears to be the first time that language from an EU Directive has been incorporated verbatim into the United States Code.[100]

Development and Employment of a Technological Means for Enabling Interoperability, Section 1201(f) (2) provides that, notwithstanding the prohibitions in Sections 1201(a) (2) and 1201(b), "a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title."

The scope of this exemption is uncertain from its language in several respects such as:-

First, it is unclear what kinds of "technological means" Congress had in mind for falling within this exemption. The reference to allowing a person to "develop and employ" such technological means may suggest that the exemption is limited to only those means developed by the person desiring to circumvent, as opposed to commercially available circumvention means. It appears that the Copyright Office agrees with an expansive reading of the Section 1201(f) exemption. After the district court's decision in the Lexmark case "Lexmark International, Inc. v. Static Control Components, Inc"[101] came down, Static Control submitted a proposed exemption to the Copyright Office in its 2003 rulemaking proceeding under Section 1201(a)(1) to determine classes of works exempt from the anti-circumvention prohibitions. It is important to understand the purposes of this rulemaking, as stated in the law, and the role I have in it. The rulemaking is not a broad evaluation of the successes or failures of the DMCA.

The purpose of the proceeding is to determine whether current technologies that control access to copyrighted works are diminishing the ability of individuals to use works in lawful, non-infringing ways. The DMCA does not forbid the act of circumventing copy controls, and therefore this rulemaking proceeding is not about technologies that control

[100] Section 1201(e) DMCA

[101] 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003), rev'd, 387 F.3d 522 (6th Cir. 2004), reh'g denied, 2004 U.S. App. LEXIS 27,422 (Dec. 29, 2004), reh'g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15,2005).

copying. Some of the people who participated in the rulemaking did not understand that and made proposals based on their dissatisfaction with copy controls. Other participants sought exemptions that would permit them to circumvent access controls on all works when they are engaging in particular non-infringing uses of those works. The law does not give me that power. The focus in this rulemaking is on whether people have been adversely affected by access controls in their ability to make non-infringing uses of particular classes of copyrighted works. Congress has directed me to exempt particular classes of works if the case has been made that such an adverse impact exists or will exist in the next three years. These exemption are in place for only three years, but may be renewed if a case has been made that they are needed.

In particular, Static Control asked for an exemption for the following classes of works:

1. Computer programs embedded in computer printers and toner cartridges and that control the interoperation and functions of the printer and toner cartridge.
2. Computer programs embedded in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product Fair use emerges.
3. Computer programs embedded in a machine or product and that control the operation of a machine or product connected thereto, but that do not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance.[102]

The Copyright Office set forth its analysis of Static Control's requested exemptions, among many other requested exemptions, in a lengthy memorandum[103] issued on Oct. 27, 2003 by the Register of Copyrights to the Librarian of Congress. Although it is not clear from the memorandum whether the Copyright Office took a position with request to Static Control's second and third proposed exemptions, the Copyright Office determined that no exemption was warranted for the first proposed exemption because "Static Control's purpose of achieving interoperability of remanufactured printer cartridges with Lexmark's … printers

[102] Section 1201(f) DMCA

[103] Memorandum from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress,"Recommendation of the Register of Copyrights in RM 2002-4; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," Oct. 27, 2003, p. 172,

could have been lawfully achieved by taking advantage of the defence found in §1201(f), the reverse engineering exemption.

The Copyright Office read the purpose behind Section 1201(f) broadly: "Not only did Congress intended that 'interoperability' include the exchange of information between computer programs; it also intended 'for such programs mutually to use the information which has been exchanged.' Interoperability necessarily includes, therefore, concerns for functionality and use, and not only of individual use, but for enabling competitive choices in the marketplace.

The Copyright Office elaborated that the statutory exemptions of Section 1201(f) afford broader exemptions than even the Copyright Office itself could grant by virtue of rulemaking. In particular, the Copyright Office's exemptions are limited to individual acts of exemption prohibited by Section 1201(a) (1), whereas the statutory exemptions of Section 1201(f) include the distribution of the means of circumvention into the marketplace

In Sega Enterprises Ltd. v. Accolade[104], Inc, Sega, a games console maker, sued Accolade, a game manufacturer, because Accolade did not license information about the Sega Genesis console from Sega. Instead, Accolade reverse engineered Sega's video game programs and looked closely at a Genesis console when the games were loaded. Accolade then produced a game development manual that was followed by its game developers. Sega sued for copyright infringement as Accolade had made unauthorized reproductions of Sega's computer programs. Accolade argued that their reproductions were a fair use of Sega's work. Fair use is a defence to copyright infringement in the United States.[105] In deciding whether the

Fair use defence is established, the court must look at four factors:

1. The purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;

2. The nature of the copyrighted work;

3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

[104] 977 F.2d 1510 (9th Cir. 1992), amended at 1993 U.S. App. LEXIS 78 (9th Cir. Jan. 6,1993)

[105] 17 U.S.C. § 107

4. The effect of the use upon the potential market for or value of the copyrighted work.

The Court of Appeals for the Ninth Circuit first noted that Accolade's commercial use tended against a finding of fair use.[106] However, despite the fact that Accolade was a commercial manufacturer of games cartridges, the information about the Sega internals was only incidental to the commercial use of Accolade—the originality of the games which Accolade was producing was not in issue. Second, with respect to the fourth factor, the court engaged in a similar analysis. Accolade, the court found, intended to become a legitimate competitor to Sega in the video games market. Within that market, it is the quality of the games which is the primary differentiation, not the information which Accolade had reverse engineered. Third, considering the second statutory factor, the court noted the dilemma of the Court of Appeals for the Second Circuit in Computer Associates International, Inc. v. Altai, Inc.[107], and accepted that not all aspects of computer programs are entitled to complete protection. The court accepted that Accolade's reverse engineering was primarily an identification of the functional aspects of the Sega system. The final statutory factor, the third, weighed against Accolade. Accolade reverse engineered Sega programs. However, this alone does not prevent a finding of fair use, and the factor is given little weight where the ultimate use of the work is minimal, as was the case with Accolade. Therefore, the court rejected Sega's copyright-based claims, stating. [W]here disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law.

This decision was consistent with a then-recent decision[108] of the Court of Appeals for the Federal Circuit, and has recently been applied by the Court of Appeals for the Ninth Circuit.[109]

4.1.4. The Licensing Arrangements for FOSS- An Overview of Intellectual Property Rights in Pakistan. Nowadays, the intangible products of human beings' creative activities

[106] citing Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 562 (1985)).

[107] 23 U.S.P.Q.2d (BNA) 1241 (2d Cir.1992).

[108] Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832 (Fed. Cir. 1992).

[109] Sony Computer Entertainment, Inc. v. Connectix Corp. 203 F.3d 596 (9th Cir. 2000), cert.n denied, 531 U.S. 871 (2000)

are considered to be a kind of property and protected as their tangible counterparts. The idea of intellectual property rights has been generally accepted, and legal institutes are built to offer protection to their possessors. Although copyrights, patents, trademarks and trade secrets all fall into the greater category of intellectual property, the essence of each differs from the other and legal instrument for each has introduced as under,

- **Trade Secrets**: A trade secret is protected by Pakistan Trade Marks Ordinance of 2001 to avoid being accessed by its owner's competing business entities. This can be done through a variety of civil and commercial means, such as confidentiality agreements or non-disclosure agreements signed by those who are given accesses to such special knowledge and information.[110]
- **Trademarks**: Pakistan Trade Marks Ordinance of 2001 deals Trademarks which having the distinctive names, phrases, symbols, designs, pictures or styles used by a business to identify itself, and its products or services, to its consumers. In many countries, colours, three-dimensional marks, sounds and even smells are also eligible for trademark protection.[111]
- **Patents**: Patents and Designs Act of 1911, Patents Ordinance of 2000 (As amended by Patents Amendment Ordinance, 2002) are the legal instruments for patent in Pakistan. While trade secrets promote the competency of a business by withholding certain information from the public, patents are designed to provide the inventor with the monopoly over newly-developed knowledge for a certain period of time (usually 20 years) in exchange for its disclosure. Typically, in order to gain such exclusive rights, the inventor is required to file a patent application, which is then reviewed by a designated patent examiner. The novelty of the invention is an essential element in granting a patent. [112]
- **Copyright:** Copyright Ordinance of 1962, as amended by Copyright (Amendment) Ordinance in 2000 this Copyright Ordinance is applied to various kinds of human creative works, such as literary works, music compositions, paintings and software. The copyright holder of a work is entitled to exclusive rights of the reproduction, modification, distribution and public display of the work. Unlike patent protection, copyright law is

[110] http://en.wikipedia.org/wiki/Trade_secret,visited on September 2008
[111] http://en.wikipedia.org/wiki/Trademark, visited on September 2008
[112] http://en.wikipedia.org/wiki/Patents, visited on September 2008

applied to a work upon its creation, regardless of its novelty. The ideas embraced in the work are not protected; copyright only prevents others from copying the copyright-holder's particular way of expressing the ideas.[113]

4.1.5 How is software protected? Software, like other literary works, is now protected under copyright law in Pakistan. Although in recently years it has been argued that the source code and algorithms should be patentable, and have already been granted patents in some case[114], software patents are still questioned and contested by many, especially from the FOSS community. This Thesis is focusing only on FOSS licenses; the software patent is itself too complicated an issue and will not be addressed much here.

4.2 Peer-to-peer networks. Peer-to-peer networking (or "P2P") has been widely adopted in recent times. A contextual definition is[115]. On the Internet, peer-to-peer . . . is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software. Corporations are looking at the advantages of using P2P as a way for employees to share files without the expense involved in maintaining a centralized server and as a way for businesses to exchange information with each other directly. Peer-to-peer networking is fundamentally different to the traditional model of networking: client-server or master-slave. In a peer-to-peer model, all machines in the network are essentially of equal status and any can initiate connections with any other. This model of networking, as alluded to in the definition, has been used to facilitate file sharing over the Internet. The most prominent example of this was Napster. Napster enabled the sharing of music between Internet users on an unprecedented scale, and in so doing polarised the Internet populace. Internet users loved it, record companies hated it. Some artists decried it, others enthused about it.

Enthusiasm, the epitaph for Napster may well read, is no substitute for reality. The reality for Napster was that they were skating on perilously thin legal ice and even the famed

[113] http://en.wikipedia.org/wiki/Copyright visited on September 2008

[114] Paper on Cyber Law Presented at the 50th Anniversary Celebrations of the Supreme Court of Pakistan International Judicial Conference by Zahid U Jamil (11-14 August, 2006) http://www.jamilandjamil.com/publications/pub_reports/article_for_scp_50_anniv_v5.0.pdf

[115] <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00%.html>. Visited on September 2008

advocacy of David Boies[116] Were not enough to save it. After losing the legal battle for its existence, Napster made peace with the record companies on the other side of the courtroom and reinvented itself as a subscription service.

4.2.1 Napster. To understand the phenomenon of Napster, one must first understand the phenomenon of MP3. "MP3" stands for Motion Picture Expert Group (MPEG) Format 1 Layer 3, a standard for the loss compression of audio data. The MP3 format is tailored for computationally inexpensive decompression at the expense of a computationally expensive one-time encoding. What made the MP3 standard popular was that it did a good job. A single could be encoded at a rate which provided similar-to-radio quality in about 3 or 4 megabytes—easily transferred over a high-speed LAN or a fast modem link.

Shawn Fanning[117] was one who recognised the potential of file swapping. Napster is software that lets users to create a virtual network in which they can see other users' MP3s and decide if they would like to download them or not. The Napster software also gives you the ability to chat with other users and create a set of preferences based on the users' own musical tastes. Napster was originally software which he wrote which provided a directory of files which people wanted to make available to "share" with others. As such, networks of song traders grew in college dormitories. The idea proved to be popular and Napster, Inc., emerged. Napster's central, what may make the MP3 standard unpopular in the future is that the MP3 standard is not unencumbered. The Fraunhofer Institute holds patents necessary to encode an MP3 file, the Use of which requires a royalty payment. An alternative, unencumbered audio format—servers registered computers sharing files and provided a search facility.

Client software made this readily accessible. Such rabid music swapping couldn't go ignored by the music companies (the owners of the copyright in the music), and thus the Napster litigation began. Before Chief Judge Marilyn Hall Patel of the United States District Court for the Northern District of California, Napster was comprehensively

[116] David Boies: the wired interview on Oct by (2000) at http://www.wired.com/wired/archive/8.10/boies.html

[117] Napster Creator Shawn Fanning, ZDNet March 2, 2000 <http://zdnet.com.com/2100-11-502047.html?legacy=zdnn>

defeated.[118] Chief Judge Patel found that, as a matter of fact, Napster caused significant economic damage to the record companies.[119]

Chief Judge Patel rejected the argument that Napster was engaging in fair use of the copyrighted music passing through its servers, as Napster provided for wholesale copying of the copyrighted works, and caused economic harm to the copyright owners.[120] The Napster service was distinguished from listening in a CD sampling booth because users kept copies of the music they were listening too.[121] Even the "substantial non-infringing uses" argument of Sony failed, as the non-infringing uses of Napster were held to be insubstantial.[122]And case Sony Vs Universal was just used as principle precedent against Napster in the case above but failed.

Many commentators have argued in favor of Napster on policy grounds. Recurring contentions rely on one or more of the following points…

1. The importance and inevitability of peer-to-peer technology.
2. Sony v. Universal stands for the principle that you do not outlaw new technology before all the implications and potential uses of the technology can be ascertained.
3. Even if Napster loses, the technology – and the file sharing that accompanies it – will not disappear.

After holding that Napster users were probably engaging in direct copyright infringement, Chief Judge Patel further held that Napster was liable for contributory infringement because of the encouragement and contribution of Napster to the copyright infringements.[123] Napster was even, notwithstanding no employment relationship, vicariously liable because it had a financial interest in the copyright infringement.[124]

Defences based on First Amendment,[125] copyright misuse[126] and waiver[127] has given short shrift. On appeal, the Court of Appeals for the Ninth Circuit upheld the record companies'

[118] A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000).
[119] Napster, 114 F. Supp. 2d at 909–11.
[120] Napster, 114 F. Supp. 2d at 912–13.
[121] Napster, 114 F. Supp. 2d at 913–14.
[122] Napster, 114 F. Supp. 2d at 916–17.
[123] Napster, 114 F. Supp. 2d at 918–920.
[124] Napster, 114 F. Supp. 2d at 920–922.
[125] Napster, 114 F. Supp. 2d at 922–23.
[126] Napster, 114 F. Supp. 2d at 923.
[127] Napster, 114 F. Supp. 2d at 923–25.

arguments on the same grounds as the District Court.[128] The only change the Court of Appeals made to the District Court decision was to limit the scope of the injunction on Napster's behaviour. The Court of Appeals put the burden on the record companies to identify copyrighted content on Napster's systems and for Napster to then remove the content upon notice from the record companies.[129] Faced with almost-complete defeat, Napster is attempting to settle with the record companies and re-invent itself as a pay service[130]. It remains to be seen whether Internet users will pay for such a privilege.

4.2.2 MP3.com. Other music distribution networks have been, and remain, in the sights of the record industry. Although not a case of peer-to-peer networking, one case that went to trial was UMG Recordings, Inc. v. MP3.com, Inc.[131] The litigation concerned the "My.MP3.com" service offered by MP3.com. MP3.com bought thousands of CDs and, without any authorisation, created MP3 files of the music tracks on the CDs. By using the "Beam It service" provided by MP3.com, a person could put an audio CD in their drive for a few seconds and if MP3.com had the CD in its catalogue, the MP3s from that CD would be added into the user's "locker". The MP3s could then be played by that user from wherever that user had an Internet connection.

Importantly for the copyright analysis employed by the court, the music which was broadcast to users was not a reproduction of music from their own CDs. It was a copy which had been created by MP3.com. A prima facie case of copyright infringement was made out but MP3.com argued the defence of fair use. The defence was rejected by Judge Rakoff, who began his judgment memorably[132].

The complex marvels of cyber spatial communication may create difficult legal issues; but not in this case. A fair use analysis showed that MP3.com was commercially profiting from unauthorized reproductions of the plaintiffs' copyrighted works. Although it was argued that this was primarily a means of "space shifting" music recordings already legally acquired by the users of the service, "[c]opyright . . . is not designed to afford consumer

[128] A & M Records, Inc. v. Napster, Inc.,239 F.3d 1004 (9th Cir. 2001).
[129] Napster, 239 F.3d at 1027–28.
[130] <http://www.wired.com/news/culture/0,1284,47401,00.html>. visited on September 2008
[131] 92 F. Supp. 2d 349 (S.D.N.Y. 2000).
[132] MP3.com, 92 F. Supp. 2d at 350.

protection or convenience but, rather, to protect the copyright holders' property interests."[133]

The strict legal analysis applied in the MP3.com case has clear implications for other innovative content distribution methods. Importantly, it means that equivalent behaviours will not be protected equally by the law—courts may tend to a microscopic rather than macroscopic analysis. In the MP3.com case, the effect to the user was the same as if they had taken their CD collection with them and were listening to CDs from that collection. Indeed, it would have been the same as making MP3s from their CD collection, putting it on a portable MP3 player and listening to that.[134] Yet because the My.MP3.com service involved the commercial, essentially unadulterated reproduction of music by MP3.com, the service fell outside the ambit of fair use.

4.2.3 Other P2P networks. After the Napster decision, Electronic Frontier Foundation attorney and Berkeley academic Fred von Lohmann wrote a white paper about the impact of copyright law on peer-to-peer networks[135], In order to stay on the right side of copyright law Recording Industry Association of America, Inc.v, Diamond Multimedia Systems, Inc, network designers to maintain plausible deniability. By having no control over the content passing through the network, no commercial interest in the success of the network and ensuring the network has substantial uses apart from the infringement of copyright, legal liability is difficult to establish.

4.3 Technological protection measures While ex post legal action provides one remedy for copyright infringement or any other illegal act, it is not a complete solution. Legal action is expensive, and civil actions against impecunious plaintiffs are usually a waste of time. A far more seductive solution for rights holders is to prevent, by some technological means, the unwanted copying in the first place. A lesser adjunct would be to embed some form of identifying information in the material which would establish that a person had exceeded the copying permission.

[133] MP3.com, 92 F. Supp. 2d at 352.

[134] See Recording Industry Association of America, Inc. v. Diamond Multimedia Systems, Inc.,180 F.3d 1072 (9th Cir. 1999).

[135] Fred von Lohmann. IAAL: Peer-to-peer file sharing and copyright law after Napster.2001 <http://www.eff.org/Intellectual_property/P2P/Napster/20010227_p2p_copyr%ight_white_paper.html>, visited on September 2008

If an effective technological protection regime could be implemented (this is expressly contemplated by the WCT), then legal protections would almost become moot. Record companies could distribute their music electronically without worrying about widespread piracy; movie studios could do likewise.

Indeed, some believe that copyright is not under threat but is instead at its apogee. With the advent of technologies such as trusted systems, it can be argued that copyright has been perfected.

4.3.1 Encryption schemes. An important component of secure delivery of digital data is the use of encryption schemes to remove the ability to access the data without authorisation. These schemes are protected as technological protection measures by the legislation examined in Chapter 3 and the legal consequences of circumventing the encryption schemes is shown by two examples.

4.3.2 DeCSS. The discussion of Napster may have suggested that the music industry was the only intellectual property industry which was under threat. Not so. With the unleashing of DeCSS, the motion picture industry also got very scared very quickly. The motion picture industry supported the widespread use and deployment of Digital Video Discs (DVDs). A DVD holds more than a CD; an entire movie—and extra bonus features—can be encoded on a single disc. The video and audio could also be digitally enhanced: appealing for people with home cinemas.

4.3.3. The technology Data on a DVD is encrypted using an "incompetently designed stream cipher known as Content Scrambling System (CSS)". The DVD Copy Control Authority (DVD CCA) would be responsible for handing out keys to vendors of player hardware and software. The theory was that should a given key be compromised, it could be revoked in future DVD pressings, reducing the utility of the compromised player. As well as standalone DVD players, DVD drives were available for computers. Software DVD players were available for some operating systems, but not for Linux. This motivated a project to write such a player, in the spirit of co-operation alluded to in Section 2.4.2. A stumbling block for this project was the decryption of the CSS-encrypted data. In September 2000, this barrier was overcome courtesy of Jon Johansen, a 15-year-old

Norwegian. Johansen released onto the Internet code called DeCSS which decrypted CSS-encoded data. Et voil`a, DVDs under Linux.

Like a lot of other people, Jon believes that if somebody buy a DVD, he/she should be able to use it on anything, and in any way, they like. He, for instance, wanted to watch his own DVDs on his Linux box. But under CSS, he couldn't. So he developed DeCSS which both unlocks DVDs and lets users fast-forward (through commercials, for example), or copy.

Actually Jon is charged under the Norwegian Criminal Code section 145(2) which prohibits breaking into someone else's 'locked' property - for example a bank or telephone company system - to illicitly access data.

The discovery of the encryption algorithm and the ability to find keys to decrypt content at will had implications far beyond the mere ability to play DVDs on alternative operating systems. It meant that DVDs could be copied with digital precision, a feat previously thought impossible. Further, with the use of video compression, the content of the DVD could be Richard M. Stallman, head of the Free Software Foundation, urges that the term “Linux” refer only to the kernel and the complete system is more properly called “GNU/Linux”, to indicate the fact that most of the programs on the system are a part of the GNU project [136].Re encoded to a size which would enable it to fit onto a single CD. This made DVD content a tradable commodity online.

4.3.4. The litigation. The motion picture industry sued[137] in the United States District Court for the Southern District of New York, claiming that DeCSS was a “circumvention device” within the meaning of the DMCA. The plaintiffs did not sue the manufacturers of DeCSS (who were unknown) but people who hosted the DeCSS code on Web sites or linked to it. The Court agreed with the plaintiff’s arguments[138], and issued an injunction restraining the parties to the case from distributing DeCSS.

4.3.5 Effective control of access. Judge Kaplan first found that although CSS was not a strong cipher, it nonetheless effectively controlled access to DVDs within the meaning of

[136] Richard M. Stallman. <http://www.gnu.org/gnu/why-gnu-linux.html>. visited on September 2008

[136] Dana J. Parker copyrights vs. free speech http://findarticles.com/p/articles/mi_m0FXG/is_/ai_63500548, March(2000)

[137] Richard M. Stallman. <http://www.gnu.org/gnu/why-gnu-linux.html>. visited on September 2008

the DMCA. As the only purpose of DeCSS was to circumvent CSS, it was a prima facie violation of the circumvention provisions of the DMCA.[139]

4.3.6 DMCA defences. The defendants' primary defence was that DeCSS was not written to enable the piracy of DVD movies but to further the development of a DVD player under the Linux operating system[140]. However, contentions based on this argument failed. Primarily, this was because the defendants were trafficking in the circumvention device, not creating it. The traffickers did not do any reverse engineering, therefore could not avail themselves of the reverse engineering for interoperability exception.

Even if they did author them, it could not be contended that the sole purpose of DeCSS was to enable a Linux DVD player to be created: DeCSS was developed and ran under Windows and, additionally, the development of DeCSS was held to be "an end in itself"[141]. The existence of these subsidiary motivations vitiated the theoretical availability of the defence. Additionally, as noted in Section 3.2.1, any public disclosure of the information nullifies the availability of the defence[142]. Likewise, none of the defendants were engaged in bona fide encryption research or security testing and could therefore not avail themselves of those exceptions.[143]

4.3.7 Fair use. The defendants finally relied on fair use. DeCSS could, after all, be used to enable fair uses of material on DVDs which may not be possible with other DVD players. The DMCA, Judge Kaplan decided, had struck the balance of fair use in favour of upholding technological protection measures, "preventing lawful as well as unlawful uses of copyrighted material".[144] The long-standing test of substantial non-infringing uses (see Section 5.3.1) was not applicable to the analysis.[145] Indeed, the "trafficking" prohibition even extended to linking to copies of the code on the Web.[146]

4.3.8 First Amendment. Although the court found some support in the view that computer software is fundamentally expressive, it came to the view that the provisions of the DMCA

[139] Reimerdes, 111 F. Supp. 2d at 319.

[140] Reimerdes, 111 F. Supp. 2d at 320.

[141] Reimerdes, 111 F. Supp. 2d at 320.

[142] Reimerdes, 111 F. Supp. 2d at 320

[143] Reimerdes, 111 F. Supp. 2d at 320.

[144] Reimerdes, 111 F. Supp. 2d at 322.

[145] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 443 (1984).

[146]Reimerdes, 111 F. Supp. 2d at 324–26.

did not offend the freedom of speech guaranteed by the First Amendment.[147] Further, the liability for linking to DeCSS is constitutional providing the defendants know that the software is a circumvention device, as was the case.[148]

4.3.9 Appeals. The decision has been appealed. The appeal attracted wide attention, and Kathleen Sullivan, Dean of Stanford Law School, represented the appellants before the Court of Appeals for the Second Circuit.[149] At the time of writing, the appellate court had not yet delivered a decision.

4.3.10. Adobe eBooks. The first criminal prosecution the against a Russian programmer violate the DMCA and charged under criminal Law who developed software that circumvented the encryption of Adobe eBooks. Despite the manifest legitimate uses of the Advanced eBook Processor—to enable back-up copies of eBooks and to enable text-to-speech conversion to name but two—Dmitry Skylarov is facing five years imprisonment in a foreign jail for an act legal in his own country. At the time of writing, Mr. Skylarov is released on bail after pleading not guilty. Adobe has dropped its support of the suit, but as a criminal prosecution the progress of the prosecution rests solely with the discretion of the United States Attorney for the Northern District of California.

The indictment against Mr. Skylarov is available at,
<http://www.usdoj.gov/usao/can/press/assets/applets/2001_08_28_sklyarov_ind.pdf>.

The situation of Mr. Skylarov indicates the far-reaching nature of the DMCA. Mr. Skylarov is not accused of copyright infringement and, indeed there is no alleged use of Mr. Skylarov's software to engage in copyright infringement of eBooks . Nonetheless, a prima facie criminal case has been established. Furthermore, it shows the extra-territorial reach of the trafficking provisions of the DMCA: although the development of the software was in Russia and the marketing was over the World Wide Web, Mr. Skylarov has fallen foul of United States legislation.

4.3.11. Summary. It is clear from the above examples that encryption schemes, no matter how incompetent or flimsy the design (one of the Adobe eBook encryption schemes was

[147] Reimerdes, 111 F. Supp. 2d at 332–33, 339.

[148] Reimerdes, 111 F. Supp. 2d at 341.

[149] Declan McCullagh. Hackers vs. Hollywood, the sequel.
<http://www.wired.com/news/digiwood/0,1412,43450,00.html>.Visited September 2008

based on ROT-13), the WCT-based laws will protect them as technological measures. It is the law, not the technology, which therefore provides the protection.

4.3.12. Watermarking. Watermarking is often used in conjunction with encryption schemes and other forms of online content distribution. The aim of watermarking is to hide information in data in order to "protect the copyright of a product or to demonstrate its authenticity". Although it does not stop the reproduction of data, it can provide evidence trail should unauthorised dealing be suspected or detected. Watermarking techniques have been developed for the use with still digital images, digital video and rendered audio. Recent discussions of watermarking techniques include. Information encoded in watermarks is protected by the laws outlined in Chapter 3 as rights management information. The removal, alteration or other modification of watermarks is forbidden by the WCT[150] and national legislation implementing it.

4.3.13 Trusted Systems. Trusted systems are an integrated solution for managing the distribution of digitised, copyrighted data. Key elements of trusted systems are encryption schemes and watermarking. Batya Friedman, Peter H. Kahn, Jr., and Daniel C. Howe write: Common sense tells us that the barriers to trust are least inhibiting when the potential harm is minimal and the good will of the person(s) we trust is genuine . . . Conversely, barriers to trust occur when there is potentially significant harm and not much good will from the person(s) we trust . . .

Trusted systems are used where there is potentially significant harm and no goodwill from the persons whom the data is delivered to. This indicates that trusted systems have a high burden to surmount.

Nevertheless, Professor Lessig suggests [...][151] that trusted systems may, in fact, implement perfect copyright control. Appropriately, they were originally developed at Xerox Palo Alto Research Centre. The concept underpinning trusted systems is that communication only takes place between "trusted" machines. The most accessible description of the technology was published by Mark Stefik, one of the primary architects of the idea, in the Scientific

[150] Article 12.

[151] Lawrence Lessig. Code and Other Laws of Cyberspace. Basic Books, New York, N.Y., U.S.A., 1999.

American[152]. The motivation for the work is: [A]uthors and publishers cannot make a living giving away their work. It now takes only a few keystrokes to copy a paragraph, an entire magazine, a book or even a life's work. Uncontrolled copying has shifted the balance in the social contract between creators and consumers of digital works to the extent that most publishers and authors do not release their best work in digital form. Dr. Stefik accurately identifies a symptom of this fear—many publishers and authors do not release their best work, or the entirety of their work, in digital form. Trusted system-based frameworks have been enthusiastically adopted by industry with consortiums such as SDMI established.

To enforce the constraints on the distribution and use of data within a trusted system, digital rights management (DRM) is used. This involves expressing the permitted uses of a digital work in a machine-readable language.

The "trust" in a trusted system framework comes from the fact that all machines are trusted to honour the commands and restrictions of the DRM faithfully. Trusted system frameworks are protected by the laws outlined in Chapter 3 as technological measures and rights management information. The prohibition against circumventing controls imposed by the trusted systems can obviate lawful uses of information, for example fair use or fair dealing.

4.4 Academic research. Standard academic behaviour is to research issues and produce papers about the findings of the research. Where research is made into technological protection measures, however, the ability of academics to subsequently publish their research may be threatened.

4.4.1. In the United States. The issue first came to a head in the United States. The SDMI Consortium (see Section 4.3.13) in order to check the viability of differing watermarking measures ran a "Hack SDMI" challenge. Professor Ed Felten together with other researchers from Princeton University detailed their attacks on the SDMI watermarking measures in an academic paper and sought to present it to a USENIX conference in April 2001 but were threatened with legal action by the Recording Industry Association of America and the Secure Digital Music Initiative. Seeking to present their paper at another

[152] Mark Stefik. Trusted systems. Scientific American, 276(3):78–81, March 1997.

conference without legal reprisal, Professor Felten filed suit in the United States District Court for the District of New Jersey seeking a declaration that their paper was not a "technology . . . that . . . is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted] work . . . ."[153]

After Professor Felten filed suit, the Recording Industry Association America and the Secure Digital Music Initiative dropped their threats of legal action and argued that there was no dispute before the court. The District Court has not decided the matter yet, although it appears that at least in the case of Professor Felten and his team's paper, there is no threat of legal action. Nonetheless, the spectre of legal suit lingers over academic research in the area of encryption technology and security research.

4.4.2. In Pakistan

In Pakistan, it is unlikely that similar action would arise. The prohibition in the Copyright Act extends only to circumvention devices and circumvention services. An academic research paper can't be seen as a device facilitating the circumvention of any protection measure, neither is it performing a service.

4.4.3. In the European Union. The text of Article 6(1) of Directive 2001/29/EC is broad enough to sanction the regulation of academic research: Member States shall provide adequate legal protection against the circumvention of any effective technological measures. Although the Directive has not been implemented in any national legislation, it is not unreasonable to posit that the regulation of academic research may be part of "adequate legal protection against the circumvention" of effective technological measures. However without domestic legislation to implement the Directive, only the possibility of application to academic research is able to be discerned in the abstract.

[153] 17 U.S.C. § 1201(a)(2).

Chapter 5

5. Analysis and Conclusion

From the applications described in Chapter 4, it is clear that the laws regulating allowable behaviours of computer software are not perfect. Even laws which have laudable objects have flaws in their implementation. This chapter explores possible improvements to the legal landscape of computer software.

5.1. Is copyright the appropriate protection for computer software? Copyright, as noted in Chapter 2, protects the expression of ideas, not ideas themselves. As such, copyright is typically not used to protect functional objects—patent protection is typically the more appropriate protection for that. During the late 1980s and early 1990s, there were suggestions that copyright protection for computer software was not wholly appropriate; indeed, it has been suggested that copyright protection stunts innovation in software development […][154].

5.1.1 Patent protection. Computer software in addition to being expressive is also inherently functional. The traditional intellectual property protection for functional items is patent protection. Patents are exclusive rights for a manner or method of manufactured; awarded if the manner or method is novel or inventive. If a patent is awarded (when the application has been examined and found to be sufficiently novel and inventive), the term is shorter than patent protection (TRIPS requires a minimum term of twenty years1) but independent development is not a defence—the patent is a monopoly on the method. It is unquestioned that computer programs can be protected by patent. Computer software is therefore one of the few species of intellectual products which can double-dip for intellectual property protection. Greg Aharonian, the closest that patent law gets to a celebrity[155], is strident in his preference of patent protection over copyright law[156]. Likewise, Dan L. Burk notes that United States courts "have struggled with the paradox of

[154] Mark A. Haynes. Black holes of innovation in the software arts. Berkeley Technology Law Journal, p575, 1999.

[155] Evan Ratliff. Patent upending. Wired, 8.06:206, June 2000. http://www.wired.com/wired/archive/8.06/patents.html.

[156] Greg Aharonian. Deconstructing software copyright: 30 years of bad logic. <http://www.bustpatents.com/aharonian/softcopy.htm, October 2001.

applying intellectual property protection that explicitly does not extend to functional items to an item that is primarily functional"[157].

5.1.2. Sui generis protection. As computer programs are a unique combination of expression and functionality it is not unreasonable to suggest that compute programs are protected by a unique (or sui generis) form of intellectual property. This was suggested in[158]. In an exhaustive manifesto, they argued for a hybrid between patent and copyright protection. Protection for a short period of time should be automatic (or nearly automatic); particularly innovative developments can have extended protection whereby the author can receive a revenue stream for the development. In this way, computer software would receive pragmatic and useful protection. Despite the doctrinal and practical appeals of sui generis protection for computer programs, copyright protection is deeply entrenched in international and national law and, as such, is not likely to ever be implemented, despite recent well-considered opinion that it may be worth reconsideration.

5.1.3 Software as speech. In the United States, the First Amendment to the Constitution (when read with the Ninth, Tenth and Fourteen Amendments) guarantees freedom of speech. Speech can only be regulated if there is a compelling governmental or social interest. Recent appellate court decisions in the United States have held that computer program code may indeed by speech. This orthodoxy has been challenged by recent decisions of courts in the United States suggesting that, at least to some extent, computer software in source code form can be protected speech.[159] This suggestion has been followed by academics such as Brian Fitzgerald and Lawrence Lessig as cited in above discussion chapter 4.

In his article[160], Dean Fitzgerald, building upon the work of postmodernist philosophers including Jacques Derrida and Michel Foucault, notes that "the quintessential element of discourse, of language, of speech, in this information society is software"[161]. In the

[157] Dan L. Burk. Copyrightable functions and patentable speech. Communications of the ACM, 44(2):69–75, February 2001.

[158] Pamela Samuelson, Randall Davis, Mitchell D. Kapor, and J.H. Reichman.Columbia Law Review, p2308–2431, (1994).

[159] See, e.g., Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

[160] Brian Fitzgerald. Software as discourse: The challenge for information law? European Intellectual Property Review, page 47, 2000.

[161] Brian Fitzgerald. Alternative Law Journal, 24(3): p144, June 1999.

emerging information society, Dean Fitzgerald argues, it is software which will become the dominant form of discourse. Private law, rather than public law, is becoming "new constitutionalism"—intellectual property, contract and competition and privacy law are, Dean Fitzgerald posits, more important than governmental and constitutional law. As such, the constitutional need to be re-examined to account for the new form of discourse. In a case currently before the Supreme Court of the United States, whether computer-generated data can attract First Amendment protection is the issue before the Court[162]. If computer-generated data attracts First Amendment protection, an extension to other computer data can be made. In a similar vein, Professor Lessig recognises that code is the new form of regulation. It is code which is increasingly defining the constraints of our interactions. The primary purpose of their discussions is not to suggest a solution or an approach, but to explicate the ubiquity of computer software in the modern world and to suggest that a political decision needs to be made with this ubiquity in mind.

5.2 Could copyright protection for computer programs be improved? For the most part, the protection for computer programs is adequate. (This was not always the case—in Pakistan, the ability to create interoperable software was significantly curtailed for a long period of time.) Despite the improvement, some of the exceptions to copyright infringements are drafted in a myopic manner: although the drafting seems to be sensible, it is not when applied to common factual scenarios.

5.2.1 Subsequent unauthorised use in Pakistan. The reason this section was included is to discourage initial reproductions or adaptations being protected, but then used for impermissible purposes later. This has the effect, however, of discouraging any dissemination of results gained from work which is protected. If research, say, for the normal use or study of a computer program is undertaken, the researchers cannot, say, give that information to assist someone attempting to create an interoperable product. This is despite the fact that both normal use and study and interoperability are separately protected purposes.

Rather than repealing the old law, the Copyright Ordinance 1962, with an object to incorporate the requirement of TRIPs, the existing law was appropriately amended by the

[162] Eric M. Freedman. Pondering pixelized pixies. Communications of the ACM, 44(8):27–29, August 2001.

Copyright (Amendment) Ordinance, 2000. The salient features, which emerged after amendment of Copyright Ordinance, are:

- Rights in audiovisual works in addition to dramatic and cinematographic works as well as musical works were recognised.
- The definition of literary work was changed to include works relating to physical sciences, compilation of data, as well as computer programs.
- Protection was given to owners of copyright in relation to computer programs, and cinematographic works were recognised with reference to rentals.
- Effective border measures were introduced to prevent infringement of copyright through importation and exportation of infringing material.
- Effective provisional measures were also introduced.

In comparison to trademark and patent infringement, only a few matters relating to infringement of copyright have reached the level of superior judiciary in recent times. However, whenever such matters have been heard, rights have been protected in the most effective manner.

For example, an appellate bench of the Lahore High Court, during the hearing of an appeal arising out of a judgment and decree by a trial court (judgment reported as 2003 CLD 1052), held that registration of copyright is not a mandatory requirement for copyright to subsist.

Recently, the Lahore High Court, while deciding another appeal, upheld the judgment and decree passed by the trial court on the point that the assignment or any licence for reproduction of the work must be in writing and not otherwise.

This is a significant legislative oversight. The requirement that the information must be "used, or sold or otherwise supplied to a person for a [different] purpose" should, however, protect most situations where information is published in academic journals. It remains, though, an unnecessarily vague part of the Copyright Act1962 (Amended as Ordinance 2000).

5.2.2. Software Piracy as Challenge. Presently, Pakistan is under increasing pressure from the industrialised countries, especially the US, regarding its the ongoing high level of piracy in its parallel economy and the lack of existing domestic legislation for copyrights and patent protection and trademark infringement. Pakistan is one of those countries, which are on the US ‘special 301’ watch list, due to widespread piracy especially of copyright material, and for its slow efforts to implement its patent obligations under the TRIPS agreement. The agreement makes protection of intellectual property as an integral part of the multilateral trading system, as embodied in the WTO. The agreement is regarded as one of the three pillars of the WTO and is subject to the integrated WTO dispute settlement mechanism. Presently, Pakistan is in the process of the implementation of the agreement, through amendments in existing legislature and if required creating new legislature. It is of crucial importance for Pakistan to study various aspects of the agreement and its implications for Pakistan at this stage. The present last part of my honours thesis attempts to take into account the following questions:

1. What are intellectual property rights? How are these related to trade through the WTO?   What are the main features of the agreement and the areas covered under TRIPS? What are the various obligations under TRIPS in general?
2. What is the present state of intellectual property protection in Pakistan as compared to other regional countries such as India and China?
3. What are the implications of enforcement of new intellectual property rules for Pakistan’s economy; the serious challenges in terms of transfer of technology from the developed countries in the pharmaceutical and agriculture sectors? How will the country face the challenges to protect its own industry in a competitive world of multinationals?
4. How Pakistan is required to cope with the challenges domestically in terms of enforcement of its obligations, which require extensive administrative tasks
5. What are the policy options for Pakistan in a knowledge-based global economy, as it needs to adapt its local manufacturing industry and agriculture sector and make it survivable and eventually duly competitive by stimulating extensive research and development?

5.2.3. What will be the impact of this change in the copyright rules on the software industry in Pakistan? There are three segments of the IT Industry can be analyze to understand software piracy issues and implications in Pakistan.

Segment 1: There is segment of the software industry that comes under documented software industry/economy. This segment is the lot of rich and high revenue generating firms in Pakistan that are using licensed software for production as well as producing products and solutions for foreign clients keeping licensing and software code protection in view, these can be classified as members of the proprietary software industry who have the money to buy software licenses and produce licensed products. These companies will benefit the most from the Anti-Software Piracy regime. Another major beneficiary will be the software developers and hi-tech innovators/entrepreneurs who rely on developing software products on proprietary software platforms as resellers or development partners or inventors, earlier; they would invest in very expensive software development activity but would not benefit from local market sales as their work would immediately be pirated and made available as part of a series of pirated software CDs locally as well as globally. The Anti-Software Piracy campaign would stop this and help the nation in generating revenue from huge within the country software sales.

Segment 2: The second segment of the industry is the undocumented and low income/revenue generating companies that are neither complying to procuring licenses for their software production environments nor are producing valid software licenses/standards compliant software products. These companies are very small software houses comprising of 3-10 developers and as a whole constitute well over 50% of the actual software industry and produce revenues of well over US$145 million a year and the government has no track of them. These companies work mainly through e-lancing and renta-coder like websites or through personal contacts abroad. Though this segment is not documented but they still contribute economically to the nation and create that interest portion that motivates foreigners to recognize Pakistani software development talent. Still most of the small developers will filter out who cannot afford licensed versions of proprietary software like Microsoft XP, MS Office, MS Visual Studio, MS SQL Server, Oracle Database and Developer Tools. These developers/software companies have been using pirated software platforms to develop pirated MIS applications for end users further drowning the end users into software piracy. The total rate of piracy in Pakistan as identified by BSA and IIPA is

82% as of 2005 but it is reducing after crackdown against software piracy in 2007 by FIA (Federal Investigation Agency).

Segment 3: The third segment of the industry is the user segment. The users are mainly users of the unlicensed versions of MS Windows XP Operating System, MS Office Tools, end user MIS applications built on pirated software development platforms, Corel Draw, 3DS Max, Adobe Products etc. They don't have any knowledge or literacy of licensed software. This constitutes most of the software users in Pakistan and in some cases, includes the government departments and academic institutions, for example, the constituent college of the University of the Punjab (Pakistan's largest and oldest public sector university) Punjab University College of IT is running 700 desktops on pirated operating systems, application development platforms including Visual Studio.net and Oracle DB/Developer. So this the actual portion of the 82% of software piracy in the region.

Another segment is emerging as part of the Open ICT Software Ecosystem, that is, the Free and Open Source Software User community. This segment has no issues whether there are Anti-Software Piracy campaigns or not. The proprietary software industry calls me the FOSS Mullah of the Free Software movement, due to the fact that I announce that we have our copyrights too, but these are different, they are meant to protect the freedom of the software and not block sharing. This pinches the opposition a lot. According to FOSSFP partners, supporters, mailing lists and volunteer community members, the Free and Open Source Software community marks well above 15,000 users, developers, administrators, professionals throughout the nation. 7,000 alone are with FOSSFP http://www.fossfp.org, 3,500 are on http://www.linuxpakistan.net, some are at http://www.osrc.org.pk etc. These users are adopting the Ubutnu-Linux OS as their preferred desktop as compared to Windows, Open Office as compared to MS Office and Firefox and Thunderbird instead of MS Internet Explorer and MS Outlook. The FOSS movement is changing the way people perceive software not only in Pakistan but around the globe.

5.2.4. Can the guarantees be side-stepped? Both in EU and the United States, users of computer software have rights granted to them. If these guarantees can be—forgive the pun— circumvented, they are of little import. It does not appear that they can.

5.2.5. Val´e fair use and fair dealing? In the United States, despite the lip-service paid to fair use in the text of the DMCA,[163] it is apparent that where data is protected by a technological protection measure, fair use is all but dead. In Pakistan, a similar process has occurred. Although Pakistan does not have a "fair use" provision based on the United States model (despite advocacy to that effect), it does have a set of fair dealing provisions. Fair dealing with a copyrighted work for the purposes of research or study, criticism or review, or reporting news, is not an infringement of copyright. Yet it is not permissible to circumvent the technological protection on works for the purposes of fair dealing.

5.3 Conclusion. In sum, copyright owners may have potentially unprecedented rights over use of their copyrighted material on the Internet or like computer software. One can expect that the fair use and implied license doctrines (and their international equivalents) will take centre stage in resolving the balance between copyright owners' and users' rights for computer Programmes. How broadly these doctrines will be applied, and whether they will be consistently applied in various countries, protecting computer programmes remains to be seen. Copyright lawyers will continue to be busy.

5.3.1. Summary. This thesis has detailed the extensive protection granted by copyright law to computer programs and computer data. Applying these legal protections to not atypical computer science behaviours has shown the existence of tension between the protection of copyright law and uses of computer programs. Further, copyright law has elevated digitised data to a protected species. The circumvention provisions, finding their genesis in the WCT, have wider consequences than merely protecting digital data from widespread piracy.

5.3.2 Remedial action. A dialogue needs to be established across the chasm of understanding that separates the computing community from the legal community. An open discourse between the two sides will inform future actions on both sides and make future legislation and future political decisions in this area less problematic especially in Pakistan. One way to insure a more balanced debate on intellectual property issues in the future is to introduce computer science students to intellectual property concepts. Conversely, the same

[163] 17 U.S.C. x 1201(c). See Section 3.2.1.

reasoning suggests that it would beneficial if legislators, judges and other such regulators became more computer-savvy.

Some of the more startling decisions in intellectual property law are decided that way because of a fundamentally specious distinction about the technology. As there has been noted in Chapter 3, computer software and computerised data are playing an increasingly important part in the fundamental interactions in today's world. It is timely and apt that computer scientists and legislators attempt to meet in the middle and develop a legally, technically and socially sound structure for future innovation.

5.3.3. Further research. This thesis has attempted to fully describe the application of copyright law to computer software and computer data in three different jurisdictions EU, US & Pakistan. There are several issues, ancillary to this thesis, which seem to suggest further research. On a purely technological basis, many of the technologies noted in this thesis (for example watermarking, trusted systems, digital rights management) are also still being actively studied and refined by the commercial and academic spheres. More eclectic is further research with both legal and computer science components. Patents: This thesis focused on copyright law and the application of copyright law in EU, US & Pakistan.

Patent law also applies to computer programs, and a similar technological and comparative analysis could be performed for patent law and computer programs. Doing it in reverse, this thesis started with a discussion of the law and then applied it to conceivable applications of computer science.

A reverse analysis should discover weaknesses in the legal case-by-case approach. Legally robust networking: Another practical research direction would be to critically analyse the infrastructure of peer-to-peer networks, and more conventionally structured networks, for legal liability. A corollary for this would be to design (or, from an existing network adapt a design) for a network with the lowest possible legal footprint; a network which is resistant to legal attacks. The nexus between law and computer science is a dynamic one: law continually changes and technology continually advances. Copyright law has a far-reaching effect on the allowable uses of computer software and computer data; the scope of which will change as technology progresses and laws are refined.

A List of Abbreviations used in Honour Thesis

EU European Union

US United States

DMCA Digital Millennium Copyright Act

WCT WIPO Copyright Treaty

FOSSFP Free Open Source Software in Pakistan

FOSS Free Open Source Software

IT Information Technology

ICT Information and Communication Technology

FIA(Pakistan) Federal Investigation Agency (Pakistan)

MS Micro Soft

IIPA International Intellectual Property Alliance

CDs Compact Discs

WTO World Trade Organization

TRIPs Agreement on Trade Related Aspects of Intellectual Property Rights

CLD Case Law Decision

DVDs Digital Video Discs

EULAs End-User License Agreements

RAM Random Access Memory

WIPO World Intellectual Property Organization

WPPT WIPO Performances and Phonograms Treaty

SSSCA Security Systems Standards and Certification Act

IPR Intellectual Property Right

P2P Peer to Peer

MPEG Motion Picture Expert Group

LAN Local Area Network

CCA Copy Control Authority

CCA Content Scrambling System

DeCSS Decrypting Content Scrambling System

DRM Digital Right Management & SDMI Secure Digital Music Initiative

References:-

1. Michael B. Feldman and Elliot B. Koffman. Ada 95: Problem Solving and Program Design. Addison-Wesley, Reading, Mass., U.S.A., second edition, 1996.
2. Brad Sherman and Lionel Bently: The Making of Modern Intellectual Property Law: The British Experience, 1760–1911. Cambridge University Press, Cambridge, U.K., 1999.
3. D. J. Harris. Cases and Materials on International Law, chapter 1, pages 1–14.Sweet & Maxwell, London, U.K., fifth edition, 1998.
4. Greg Aharonian. Deconstructing software copyright: 30 years of bad logic. <http://www.bustpatents.com/aharonian/softcopy.htm>, October 2001.
5. National Commission on New Technological Uses of Copyrighted Works, Final Report 1 (1979)< http://www.copyright.gov/circs/circ21.pdf>
6. Apple Computer Inc. Apple Computer, Inc. software license. <http://store.apple.com/Catalog/US/Images/swlicense_apple.html>. Visited on Aug 2008.
7. Open Source Initiative. Open source definition. <http://www.opensource.org/docs/definition.html>. Visited 30 Aug 2008.
8. Karen E. Georgenson. Reverse engineering of copyrighted software: Fair use or misuse? Albany Law Journal of Science and Technology, 5:291–320, 1996.
9. Free Software Foundation. The free software definition. <http://www.gnu.org/philosophy/free-sw.html> Visited 30 July 2008.
10. David McGowan. Intellectual property challenges in the next century: Legal implications of open-source software. University of Illinois Law Review, pages 241–304, 2001.
11. David Nimmer. A riff on fair use in the Digital Millennium Copyright Act. University of Pennsylvania Law Review, 148:673–742, 2000.
12. Application Hardening with Guard IT. Defend, Detect and React Guard Technology <http://cryptome.org/sdmi-attack.htm> visited on 15 July 2008.
13. IIPA 2003 Special 301Report Pakistan. Available at, http://www.iipa.com/rbc/2007/2007SPEC301PAKISTAN.pdf
14. Sony Corp. v. Universal City Studios, Inc.,464 U.S. 417 (1984)
15. Jon Bing, Article upon Copyright protection of computer programs, p 16
16. Memorandum from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress, “Recommendation of the Register of Copyrights in RM 2002-4; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies,” Oct. 27, 2003, p. 172,
17. Citing Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 562 (1985)).
18. Sony Computer Entertainment, Inc. v. Connectix Corp. 203 F.3d 596 (9th Cir. 2000), cert .n denied, 531 U.S. 871 (2000)

19. Paper on Cyber Law Presented at the 50th Anniversary Celebrations of the Supreme Court of Pakistan International Judicial Conference by Zahid U Jamil (11-14 Aug 2006) http://www.jamilandjamil.com/publications/pub_reports/article_for_scp_50_anniv_v5.0.pdf
20. David Boies: the wired interview on Oct by (2000) at http://www.wired.com/wired/archive/8.10/boies.html
21. Napster Creator Shawn Fanning, ZDNet March 2, 2000 <http://zdnet.com.com/2100-11-502047.html?legacy=zdnn>
22. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000).
23. See Recording Industry Association of America, Inc. v. Diamond Multimedia Systems, Inc.,180 F.3d 1072 (9th Cir. 1999).
24. Fred von Lohmann. IAAL: Peer-to-peer file sharing and copyright law after Napster.2001 <http://www.eff.org/Intellectual_property/P2P/Napster/20010227_p2p_copyr%ight_white_paper.html>, visited on September 2008
25. Richard M. Stallman. Why GNU/Linux? <http://www.gnu.org/gnu/why-gnu-linux.html
26. Dana J. Parker copyrights vs. free speech http://findarticles.com/p/articles/mi_m0FXG/is_/ai_63500548, March(2000) Visited on October 2008.
27. Declan McCullagh. Hackers vs. Hollywood, the sequel. <http://www.wired.com/news/digiwood/0,1412,43450,00.html> Visited September 2008
28. Lawrence Lessig. Code and Other Laws of Cyberspace. Basic Books, New York, N.Y., U.S.A., 1999.
29. Mark A. Haynes. Black holes of innovation in the software arts.Berkeley Technology Law Journal, 14:567–575, 1999.
30. Evan Ratliff. Patent upending. Wired, 8.06:206, June 2000<http://www.wired.com/wired/archive/8.06/patents.html>.
31. Greg Aharonian. Deconstructing software copyright: 30 years of bad logic. <http://www.bustpatents.com/aharonian/softcopy.htm, October 2001.
32. Dan L. Burk. Copyrightable functions and patentable speech. Communications of the ACM, 44(2):69–75, February 2001.
33. Pamela Samuelson, Randall Davis, Mitchell D. Kapor, and J.H. Reichman. Columbia Law Review, p2308–2431, (1994).
34. Brian Fitzgerald. Software as discourse: The challenge for information law? European Intellectual Property Review, page 47, 2000.
35. Brian Fitzgerald. Software as discourse? A constitutionalism for information society. Alternative Law Journal, 24(3): 144–149, June 1999.

36. Eric M. Freedman. Pondering pixelized pixies. Communications of the ACM, 44(8):27–29, August 2001.

Annex (optional)