Journal of Harbin Engineering University Vol 44 No. 9
ISSN: 1006-7043 September 2023

Reverse Engineering: Unfair Competition Or Catalyst for Innovation?

Ms. Swati Pareek[1] and Prof. (Dr.) Mahesh Koolwal[2]
[1]Research Scholar, School of Law, JECRC University, Jaipur
[2]Professor and Dean, School of Law, JECRC University, Jaipur

Abstract-Reverse engineering is "a process almost as old as man-made artefacts themselves."[i] Peopleof all ages have been curious to find out how things work. As long as the object of humancuriosity is nature itself, society esteems the curious person as a scientist whose work benefitsthe common good. As soon, however, as a technician takes apart a machine made bysomeone else there is less unanimity about whether this activity is commendable or whether itis an act of piracy which the law should enjoin. While in the US "reverse engineering has along his-tory as an accepted practice",[ii] German courts and most commentators still follow ajudgment handed down by the Reichsgericht (Supreme Court until 1945)[iii] in which the courtregarded the reverse engineering of a complex product as unfair competition.

I. Introduction

In an era of globalised research this fundamental difference is astonishing for at least tworeasons. First, restrictions on reverse engineering sit uneasily with one of the patent system'smain objectives, namely the disclosure of technical information. Secondly, reverseengineering seems to be common practice in many fields of engineering. Nevertheless,surprisingly little research on reverse engineering has been done in Europe. Around 1990 theCommission's proposal for a Directive on the Protection of Computer Programs sparked somediscussion about the conditions on which the decomplication of programs should bepermitted.[iv] This debate, however, remained restricted to the software field, did not treat reverseengineering as a matter of principle and quickly died down after the adoption of the directive.[v]In the US, arguably the issue of federal pre-emption has helped to uncover potential conflictsbetween patent law and trade secrets law. Several Supreme Court judgments and otherdecisions have shed some light on this issue and have given rise to academic work on the lawand the economics of reverse engineering.

This article will define reverse engineering, will look at the different approaches adopted by US and German trade secrets and intellectual property law and at policy reasons for and against allowing reverse engineering. Joseph Straus, to whom this contribution is dedicated, has always taken great interest in fundamental issues of patent law. He is also one of the few German law academics who are equally at home in German, European and US law. Since this analysis will uncover tensions between trade secret law and patent law and divergences between German and US law, this author hopes that his article might find Joseph Straus's interest.

II. Reverse engineering: definition and practical significanceReverse Engineering defined

Engineering is the creative application of scientific principles to design or develop structures, machines, apparatus, or manufacturing processes or works.[vi] It is a process which starts from principles and ends up with the product as a result. Reverse engineering is just the opposite: it is a process starting with the known product and working backward to find out the technical principle behind it.[vii]

In traditional branches of engineering this analysis may be carried out by taking a machine apart and by analysing its components. More modern methods include the chemical analysis of components or the electronic scanning of the shape of the product or of its parts. Since the advent of computer technology, the decomplication or disassembly of computer programs has become the perhaps most important area of reverse engineering. At least "proprietary" software is generally distributed in the form of a binary object code, whereas only the source code which is written in a programming

language is understandable to humans. With the help of specific software, it is possible to decrypt the object code. However, significant effort may be necessary to interpret the data achieved in this process.[viii]

III. Why Reverse Engineering?

The driving force behind reverse engineering may be pure curiosity. In an academic environment, curiosity is the starting point of research: particularly in disciplines like information sciences and engineering reverse analysis may be an important research tool and may also be used in teaching. When, however, reverse engineering is carried out in the course of business activities, there is usually a commercial motive for being curious. Three main reasons can be distinguished.

The first scenario is that of the "innovative analyst", who seeks to further his or hertechnological knowledge in order to devise new, innovative products or to improve existingproducts. If the common purpose of patent and trade secrets law is the enhancement ofinnovation, there seems to be a prima facie case for allowing "innovative" reverseengineering, particularly if the analyst would not have been able to gather the information byother means.

The second scenario that of the "copycat analyst", is more mundane. This person uses reverse engineering in order to copy a product. The leading German case of 1935[ix] is an example in point. A company which had bought a complex machine manufactured bythe plaintiff needed another machine of this sort but did not want to pay the monopoly price. Thus,the company asked the defendant to take the machine apart, to produce exact drawings of all components and to manufacture a similar machine. There is a grey area between reverse engineering and pure copying here,[x] as one of the leading US cases shows. The Bonito Boats case[xi] was about the copying of boat hulls by a moulding technique. The construction of the boat hull was not secret, but the moulding procedure allowed cost-cutting copying of the hull. While we will have to analyse the different reactions of the German and the US courts in detail later, we can already note thatthe "copycat's" behaviour may be less desirable from an economic point of view, as it deprives the original manufacturer of the possibility of recouping its investment in the development of a new machine.

Thirdly, reverse engineering may allow the owner of an intellectual property right to find out whether the manufacturer of the product has infringed the right (the "right owner analyst"). In this scenario reverse engineering may be a speedy and cheap possibility of securing evidence. While these three motives apply to all types of technology, there are additional reasons for the reverse engineering of software.[xii] The most important one is de-compilation or disassembly for the purpose of achieving interoperability. While many software producers publish interface specifications, some either do not publish this information at all or hold back at least some information which an independent programmer may need in order to produce an inter-operable program. In some cases, competition law may require the disclosure of information on programming interfaces, as the recent decision of the Court ofFirst Instance in the Micro soft case[xiii] shows. But the software market may be too dynamic to allow an independent producer to wait for a court injunction for several years. Reverse engineering may allow speedy self-help. It may also be necessary for adapting a program to different hardware or to another operating system or for repairing faults or detecting bugs.

It emerges that there is a wide range of possible motives for reverse engineering. In some cases, reverse engineering is a necessary or at least useful step in the process of further innovation, in other cases it may only enable imitation.

IV. The US approach and the German approach compared: Different principles: trade secrets and reverse engineering

International law

Reverse engineering is only necessary where the technical principles embodied in the product are not generally known or readily accessible. Thus, the first starting point of our legal analysis is the protection of undisclosed information, which all WTO member states are under an obligation to provide.

In art. 39 (1) TRIPS the protection of undisclosed information is classified as a part of unfair competition law in the sense of art. 10[bis] of the Paris Convention. Art. 39 (2) TRIPS definesthe concept of "undisclosed information" by listing three criteria: the information must be (a) secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, (b) has commercial value because it is secret and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. However, art. 39 (2) TRIPS also stresses that there is no absolute property right in undisclosed information. Disclosure or unauthorised use of the information only needs to be prevented if these acts are contrary to honest commercial practices. Note 10 explains that at least practices such as breach of contract, breach of confidence and inducement to breach are to be considered as dishonest.

The provision does not explicitly refer to reverse engineering. In particular, it does not decide whether information which can only be made available through a costly and time-consuming reverse analysis is to be considered as "undisclosed" and whether reverse engineering is always or at least in some situations "contrary to honest commercial practices". While US and German law both protect trade secrets in accordance with art. 39 TRIPS, they disagree fundamentally about whether reverse engineering is fair or unfair.

V. USA: Reverse Engineering as Proper Method of Obtaining the Secret

In the US, trade secrets are protected by state law, not by federal law. Many states have adopted the 1979 Uniform Trade Secrets Act, and some guidance is also given by the 1995 Restatement of Unfair Competition.[xiv] The Restatement defines a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others"[xv] and states that trade secrets are only protected against disclosure or discovery "by improper means".[xvi] Trade secrets are predominantly protected by private law, although the statutory law of some states also provides for criminal law sanctions. Patent law, on the other hand, is federal law. This raises the issue of pre-emption: states cannot give protection of a kind that clashes with the objectives of the federal patent laws.[xvii]Thanks to this specific feature of US law possible conflicts between patent and trade secret protection have arguably been analysed in greater depth in the US than anywhere else. Indeed, one of the purposes of patent law is the disclosure of technical information. If trade secret law is prepared to protect technical information which is kept secret, there seems to be primafacie conflict. This issue was discussed by the US Supreme Court inKewanee v. Bicron,[xviii] a classical trade secret case about the wrongful use and disclosure oftrade secrets by former employees. The court found that trade secret law did not interfere with federal patent policy. In the case of clearly unpatentable information the abolition of trade secret law would, according to the court, clearly not enhance disclosure, as a reasonable holder of the secret would rather hoard the information than disseminate it under an obligation of confidence. Patent law did not encourage espionage; on the contrary the state was under an obligation to protect privacy. In cases where patentability was doubtful the abolition of trade secret protection would force inventors to file even the most dubious inventions. But the court did not even assume a conflict between trade secret protection for patentable inventions and patent policy: the inventor could not just sit back and rely on secrecy protection because this type of protection was much weaker than patent protection. While patent protection was absolute, trade secrets were not protected against the discovery of the information by fair and honest means such as independent creation or reverse engineering. It can be inferred from this reasoning that a state statute which prohibited reverse engineering would be pre-empted by federal law.

This conclusion was indeed drawn by the Court of Appeals for the Ninth Circuit in the Chicago Lock case.[xix] The plaintiff was a manufacturer of

high-quality locks. It kept the information of its key codes secret and did not disclose it to locksmiths. If the purchaser of a lock lost a key, he or she had to order a new one from the plaintiff. Another practical possibilitywas to ask a locksmith to "pick" the lock and to find out the key specification that way. Overtime locksmiths collected data on key codes. The defendants obtained this information andpublished it in a book. The District Court held that this practice amounted to an improperacquisition of trade secrets. The Court of Appeals set this judgment aside and stressed thatreverse engineering was a legitimate means of discovering a trade secret. Trade secretprotection in this case would in effect have created an intellectual property right, which wouldhave been pre-empted by federal patent law.[xx]

Eventually, the Supreme Court discussed the policy reasons behind allowing reverseengineering in the Bonito Boats case.[xxi] The defendant had copied the plaintiff's unpatentedboat hulls by a "direct moulding process", which a Florida statute prohibited. The SupremeCourt held that this statute was pre-empted by the supremacy clause. As already noted above,this is a borderline case between reverse engineering and the outright copying. Indeed, asubstantial part of the judgment is dedicated to the question whether the law should enjoin thecopying of products not protected by intellectual property rights by means of unfaircompetition law. The court rejected this idea, stressing the need for a careful balance betweenlegal protection of innovation and the freedom to imitate:

"From their inception, the federal patent laws have embodied a careful balance between the need to promote innovation and the recognition that imitation and refinement through imitation are both necessary to invention itself and the very lifeblood of a competitive economy."[xxii]

Freedom of imitation was the necessary corollary of intellectual property protection: the patent system would be undermined if unfair competition law granted protection without the careful protections and high standards inherent in the patent system. Imitation could be an essential part of innovation. Reverse engineering, in particular, often led to significant advances in technology.[xxiii]

By now it seems to be generally accepted in US law that the discovery of a trade secret bymeans of reverse engineering cannot be regarded as a discovery by improper means. TheRestatement explicitly stresses this point in § 43. It is less clear whether technical informationembodied in a product which is freely available on the market can be considered as a secret atall. The comments to the Restatement combine the issues of secrecy and disclosure byimproper means by stating that information is not secret which is generally known orascertainable by proper means. In an English decision about the reverse engineering of a coindiscriminator named "Cashflow", Jacob J. (as he then was) was more explicit:

"(…) does the encrypted information in the Cashflow have 'the necessary quality of confidence'? I think the answer is clearly 'no'. The Cashflow is on the market. Anyone can buy it. And anyone with the skills to de-encrypt has access to the information."[xxiv]

Later in his judgment, Jacob J. also rejected the second requirement existing under the English "breach of confidence" doctrine, namely the requirement of an obligation of confidence.[xxv]

VI. Germany: Reverse Engineering as Unfair Competition

One of the traditional features of German unfair competition law is its broad prohibition ofunfair trade practices, now set forth in § 3 of the Act against Unfair Competition of 2004(UWG). This provision has the great advantage of flexibility and the great disadvantage ofuncertainty. The latter has, however, meanwhile been reduced by the inclusion of a detailedlist of unfair acts into the statute. From this perspective it is rather surprising that trade secretsare not protected by an equally flexible rule but by a rather detailed criminal provision. While§ 17 (1) UWG proscribes the disclosure of trade secrets by employees, § 17 (2) No. 1 UWGprohibits the unjustified acquisition of a trade secret by (a) technical means, (b) producing atangible embodiment of the secret or by (c) stealing an item in which the secret is embodied. §17 UWG does not define the concept of "trade secret". The Federal Supreme Court regularlyapplies four conditions[xxvi]: a trade secret must relate to a particular business, the

informationmust neither be generally known nor easily available, the holder of the information must havethe intention of keeping it secret and there must be a legitimate economic interest in secrecy.There is no broad test of fairness. Rather, the acquisition of the secret is considered unjustifiedunless there are specific grounds of justification such as consent, state of emergency, acontractual claim for disclosure or a statutory duty of disclosure.[xxvii]

The issue of reverse engineering was considered by the Reichsgericht, the German SupremeCourt before 1945, in the "boot iron press" judgment of 1935.[xxviii] The plaintiff producedmachines which were used to produce boot irons, i.e., irons used to strengthen the sole of boots.This machine had been patented, but the patent had already expired 36 years ago. A Polishcompany had bought one of the plaintiff's machines, needed a second one, but considered theplaintiff's price as excessive. Thus, the Polish firm asked the defendant to produce an identicalmachine. The defendant accepted the order, took the machine apart, made detailed drawings ofall components and was thus able to construct a similar machine. The plaintiffs asserted thatthis practice constituted unfair competition under § 17 UWG and under the doctrine of slavishimitation. The court upheld the claim on both counts. At first sight, the court's reasoning withrespect to § 17 UWG is entirely formal: the court found that all the requirements set forth in §17 UWG had been fulfilled. Information which was embodied in a product did not cease to besecret when the product was sold, provided that substantial effort was necessary in order todiscover the information; the plaintiff had acquired this information by technical means and noground of justification was made out. Between the lines, however, a substantive line ofargument can be detected. The court points out that the defendant, by taking apart a machine"which was not meant to be taken apart", had strengthened its own competitive position at theplaintiff's cost.[xxix] In other words: the defendant had reaped where it had not sown.

Considerable investment had gone into the development of the original machine and thedefendant had saved costs and had thus been enabled to undercut the plaintiff's price. Thedecision is very unsatisfactory because the court does not openly address the relevant policyissues, particularly the apparent conflict with patent policy.[xxx] The desire to protect the plaintiffagainst the misappropriation of its know-how is hidden behind vague notions of what an honestmerchant would have considered appropriate.

This judgment has been applied by the courts in later cases.[xxxi] Only the Düsseldorf and theHamburg Courts of Appeal have distinguished the "boot iron press case".[xxxii] However, bothcourts did not openly reject the old doctrine but held that in the cases at hand the defendant hadnot had to take substantial efforts in order to discover the secret. Most commentators cite theReichsgericht's decision with approval,[xxxiii] in particular the principle that information embodiedin a freely available product can remain secret where substantial effort is necessary in order todiscover the information. Policy reasons for allowing reverse engineering regularly remainunmentioned. In particular, the fact that trade secret law may in effect be relied upon in orderto protect an invention after the patent has expired, has met with surprisingly little criticism.[xxxiv]

In the discussion which was sparked by the Commission's plans for a Software Directivearound 1990, most authors applied the established principles of trade secrets law to the software field.[xxxv] In this context only few writers challenged the proposition that trade secret law grantedprotection against reverse engineering.[xxxvi]

It can only be guessed why German literature, whichis rather extensive and elaborate in most fields of intellectual property and unfair competition law, has paid so little attention to reverse engineering in particular and to trade secret protection in general.[xxxvii] One reason may be that both patent and unfair competition law are federal law in Germany. So, no issue of pre-emption forces courts and legal authors to investigate the relationship between patents and trade secrets more closely. Another reason may be that § 17 UWG is a criminal law provision. As such it falls between the chairs of criminal doctrine, which rather seems to focus on murder and fraud than on unfair competition law, and intellectual property law doctrine, which is so firmly rooted in

private law that it tends to neglect criminal provisions.

VII. Much Common Ground: The IP Framework

While US and German law take opposite positions on trade secret protection against reverseengineering, there is much more consensus when it comes to the intellectual property lawframework.

One of the fundamental assumptions of the patent system is that the grant of a patent is oneside of a deal between the inventor and society. As a quid pro quo for being granted an exclusiveright, the inventor discloses the invention. Thus, patent law enhances innovation in tworespects: by granting an exclusive right it allows the patentee to recoup its research anddevelopment investments and by insisting on the publication of applications it spreads technicalinformation.[xxxviii] This rationale militates in favour of allowing reverse engineering: from a patentlaw perspective there is nothing wrong with finding out how things work. Indeed, in an optimalpatent system there would be no need to reverse engineer patented inventions as they wouldhave been sufficiently described in the patent application. But even if the purchaser of apatented product wishes to analyse it, patent law will not prevent him or her from doing so.The purchaser is free to possess, use and investigate the patented product, since all patent rightsin the particular item are exhausted at first sale. While the reconstruction of a patented productmay infringe the patent, the reverse analysis as such does not.[xxxix] Finally, at least in mostEuropean jurisdictions reverse engineering would be covered by the research privilege,whereas in US law the commercial analysis of patented products may not be justified.[xl] Despitethis difference, reverse engineering will rarely, if ever, infringe a patent.

One highly specialised and at the same time internationally harmonised branch of intellectualproperty law[xli] even contains an explicit permission of reverse engineering. While thereproduction of semiconductor chip layouts without the authorisation of the right owner isprohibited by art. 6(1) of the Washington Treaty on Intellectual Property in Respect ofIntegrated Circuits and the corresponding EC[xlii] and national legislation,[xliii] art. 6 (2) allowsreproduction “for the sole purpose of evaluation, analysis, research or teaching”.[xliv] Theseprovisions strike an interesting balance: they allow learning while at the same time prohibitingfree-riding. They can be traced back to a more general principle the extension of which to otherareas of intellectual property and competition law will have to be discussed later: it maygenerally be permissible to find out technical information, even if it is not readily available,but the imitation of the original product may be prohibited where there are sound policy reasonsfor granting such protection.

As long as copyright did not protect technical subject-matter there was no need to reverseengineer copyrighted works. Copyright protects the expression, not the idea;[xlv] and as regardsclassical types of works such as books, works of art or music the idea is readily ascertainableto the reader, viewer or listener. With the advent of copyright protection for computer programs,however, reverse engineering became an issue. As noted, before, at least “proprietary” softwareis usually distributed in machine-readable form only. Thus, the only form of expressionavailable to the user is a form which he or she cannot understand. The “programming idea” canonly be found out if it has been decrypted first. Technically, however, the decompilation of aprogram is an alteration, which, without the right owner’s authorisation, is prohibited bycopyright law unless an exemption from copyright applies.[xlvi] At this point US and Europeanlaw differ. Several US courts have regarded reverse engineering of computer pro-grams as fairuse, if done for legitimate purposes such as achieving interoperability[xlvii] or emulating thefunction of a PlayStation console on a regular computer.[xlviii] While the EC Software Directivealso allows decompilation for the purpose of achieving interoperability, the exception,[xlix] whichwas the subject of much controversy,[l] is more restrictive: decompilation must be indispensableto obtain the necessary information, the acts must be performed by a person having a right touse the program, the information must not have been readily available and the exception isrestricted to the parts of the original program which are necessary to achieve

interoperability.Decompilation for other purposes such as detecting copyright infringement, porting or repair[li]is not permitted. While the directive permits the user "to observe, study or test the functioningof the program in order to determine the ideas and principles which under-lie any element ofthe program", it is clear from the systematic structure of the directive that the permitted acts ofanalysis do not include decompilation.[lii]

VIII. Policy Considerations

Trade Secret Law Justified

The obvious tension between the patent system's objective of spreading technicalinformationand of trade secret law's purpose of preserving secrecy begs the question of whytrade secretprotection is justified. Indeed, powerful objections to secrecy protection havebeen voiced.[liii]This question, which is by-passed by many European authors, is so complexthat it cannot beanswered satisfactorily in this short article.[liv] Nevertheless some answers canbe gleaned fromthe analysis of US law conducted above.

First, particularly older cases on both sides of the Atlantic have frequently referred to thestandards of commercial honesty, arguing that anyone who obtains a competitive advantagethrough a breach of confidence acts unfairly.[lv] From a modern perspective, however, thisreference to honesty is inherently vague.[lvi] While there may be a generally shared convictionthat breaches of confidence or industrial espionage are dishonest, standards of honesty areeasier maintained than proven, and they are of little assistance for the resolution of borderlinecases.

Secondly, there is a parallel between personal privacy and trade secret protection. As much asevery person has the "right to be let alone", every business needs an internal sphere which isprotected from the public eye.[lvii]But whereas respect for personal privacy stems from theprotection of human rights, the reasons for respecting "business privacy" are more functional.Innovation does not happen overnight. Enterprises need a protected "laboratory zone" wheretechnology can be tested and where business strategies can be discussed confidentially. Publicattention and close monitoring by competitors would thwart these innovativeprocesses at thevery beginning. By protecting this sphere of confidentiality, trade secrets lawmakes sure thatthe developer has a natural lead time in the market,[lviii] thereby promotinginnovation. A thirdpoint is closely related: trade secret protection is the necessary corollaryof the noveltyrequirement in patent law. The applicant must be given the chance to developits invention upto the point where it is ready for application. Abolishing trade secretprotection wouldd ramatically increase the risk of a premature novelty-destroying disclosure of inventions. Afourth argument has been stressed in law and economics research:[lix] without legal protectionthere would be a strong incentive to invest into measures of maintaining secrecy. Trade secretslaw facilitated the disclosure of information to employees and licensees and discourageswasteful expenditure in the protection of business premises and in technical protectionmeasures. However, trade secrets law is not only relied upon to bridge the time before themarketing of a product. Many industries rely on trade secret protection as a substitute forintellectual property protection, either because a particular intangible subject-matter fallsbetween the chairs of intellectual property law (as is arguably the case with food recipes suchas Coca Cola's secret formula) or because trade secret protection is regarded as a cheaper andpotentially endless alternative to patent protection.

Thus, it could be argued that the main purpose of trade secret protection was to protectinvestment as such against misappropriation and to fill gaps in the intellectual propertysystem,[lx] or, based on a Lockean theory, to secure to the owner of the secret the fruits of hislabour.[lxi] This argument, however, is fallacious, because it implies that every intangible subjectmatter should be protected against unauthorised exploitation if investment or creativity wentinto its generation. Whether the law should grant general protection against "reaping withoutsowing" is one of the most fundamental and most disputed questions of intellectual propertylaw. National approaches differ. English[lxii] and US law[lxiii] answer this question in the negative.In German law the copying of subject-matter which is not protected by an

intellectual propertyright is not proscribed as such, but can only be considered as unfair if additional factors ofunfairness are present.[lxiv] While art. 5 (c) of the Swiss Act against Unfair Competitionproscribes "the identical exploitation of the results of someone else's labour by means of atechnical reproduction process without reasonable personal efforts", the provision has beenapplied quite restrictively by the Swiss courts.[lxv] But independently of this question, the"reaping without sowing" argument is too unspecific to justify trade secret protection unlessthere are particular reasons why the unauthorised exploitation of undisclosed informationshould be treated differently from the use of disclosed information which, according to mostjurisdictions, everyone is free to use - even if he or she saves own efforts by using it.

IX. Conclusion

Reverse engineering is not unfair. Curiosity is one of the driving forces behind innovation. Itshould not be restricted, at least as long as the information is not obtained by a breach ofconfidence of by an interference with the internal sphere of a business. Intellectual propertylaw by and large does not restrict the access to information. While the law of trade secretsdoes prevent the access to undisclosed protection of innovation and freedom of imitation are the lifeblood of a competitive economy.

Reference

[1] *Mars UK Ltd v. Teknowledge Ltd.*, [2000] FSR 138 at para. 29 per Jacob J. SAMUELSON/SCOTCHMER, The Law and Economics of Reverse Engineering, 111 Yale L.Rev. 1575, 1577 (2002).
[2] RGZ 149, 329 = RG GRUR 1936, 183 – *Stiefeleisenpresse*.See HABERSTUMPF, Die Zulässigkeit des Reverse Engineering, CR 1991, 129; HART, Interfaces.
[3] Interoperability and Maintenance, [1991] EIPR 111; HARTE-BAVENDAMM, Wettbewerbsrechtliche.
[4] Aspekte des Reverse Engineering von Computerprogrammen, GRUR 1990, 657; TAEGER, SoftwareschutzdurchGeheimnisschutz, CR 1991, 449; VINJE, Threat to Reverse Engineering Practices Overstated,[1994] EIPR 364; WIEBE, Reverse Engineering und Geheimnisschutz von Computerprogrammen, CR 1992, 134.
[5] See LEHMANN, in: LOEWENHEIM (ed.), Handbuch des Urheberrechts (2003), § 76, para. 24.
[6] Definition given by the American Engineers' Council for Professional Development, found at www.wikipedia.org (last inspected March 17, 2023).
[7] See *Sinclair v. Aquarius Electronics, Inc*., 42 Cal.App.3d 216, 226, 116 Cal.Rptr. 654, 661 (1974).
[8] JOHNSON-LAIRD, Software Reverse Engineering in the Real World, 19 U. Dayton L. Rev. 843 (1994); HARTE-BAVENDAMM (*supra*, note 4), at 659-660.
[9] *Supra*, note 3.
[10] See also LANDES/POSNER, The Economic Structure of Intellectual Property Law (2003), p. 370: "Indeed,from an economic standpoint there is little distinction between information, it only provides protection against unfairdisclosure or exploitation; in this respect trade secret protection is a genuine part of unfaircompetition law. There should be no general presumption that obtaining a secret outsiderelations of confidence is unfair as such. Rather, the broad notion of "fairness" or "honestpractices" allows a balancing exercise which takes into account the interests of the owner ofthe information of the person interested in obtaining it and of the general public.
On this basis, US law has long accepted reverse engineering as a fair means of discoveringinformation. In German law the conflict between trade secret protection and intellectualproperty protection has not been fully recognised by the courts and many commentators yet,but the statutory provisions are broad enough to allow the necessary balancing exercise.Whether the use of the information so obtained as a "springboard" for identical copying ispermissible is a different matter. The answer to this question should not distinguish betweencopying enabled by reverse engineering and imitation by means of other technicalreproduction measures. When it comes to determining whether the law should prevent "unfaircopying", however, legislations and courts should keep in mind a central proposition of theBonito Boat judgment: both reasonable

really cheap reverse engineering on the onehand and piracy on the other."

[11] *Bonito Boats, Inc. v. Thunder Craft Boats, Inc*., 489 U.S. 141 (1989).

[12] A more detailed analysis of these motives is given by HARTE-BAVENDAMM (*supra*, note 4), at659.

[13] CFI, September 17, 2007, case T-201/04, *Microsoft v. Commission*.

[14] American Law Institute, Restatement of the Law 3rd, Unfair Competition (1995).

[15] *Id*., § 39.

[16] *Id*., § 40.

[17] See art. VI, clause 2 of the US Constitution and *Sears, Roebuck & Co. v. Stiffel Co*., 376 U.S. 225, 231 (1964).

[18] 416 U.S. 470 (1974).

[19] 676 F.2d 400 (C.A.9 1982).

[20] *Id*. at 405.

[21] 489 U.S. 141 (1989).

[22] *Id.*, at 146.

[23] *Id.*, at 160.

[24] *Mars UK Ltd v. Teknowledge Ltd*., [2000] FSR 138 at para. 31.

[25] On reverse engineering as a limit to confidence liability in English law see CORNISH/LLEWELYN, Intellectual Property, 6th ed. (2007), para. 8-20.

[26] BGH GRUR 1955, 424, 425 - *Möbelpaste*; BGH GRUR 2003, 356, 358 - *Präzisionsmessgeräte*; ANN, Knowhow-Stiefkind des GeistigenEigentums? GRUR 2007, 39, 41; KÖHLER, in: HEFERMEHL/KÖHLER/BORNKAMM, Wettbewerbsrecht, 26th ed. (2008), § 17, notes 5-10; OHLY, in:PIPER/OHLY, UWG, 4th ed. (2006), § 17, note 5.

[27] See BRAMMSEN, in: HEERMANN/HIRSCH (eds), MünchenerKommentarzumLauterkeitsrecht (2006), §17, note 51; HARTE-BAVENDAMM, in: HARTE-BAVENDAMM/HENNING-BODEWIG (eds), UWG(2004), § 17, note; KÖHLER (*supra*, note 26), § 17, notes 21, 36.

[28] *Supra*, note 3.

[29] *Id.*, at 187.

[30] As was already pointed out early by BAUMBACH/HEFERMEHL, Wettbewerbsrecht, 22th ed. (2001), § 1, note 478. See also *infra*, note 41.

[31] BGH GRUR 1980, 750, 752 - *Pankreaplex II*; BayObLG GRUR 1991, 694, 695 - *Geldspielautomat*; BAG AP Nr. 1 zu § 611, Betriebsgeheimnis-*Thrombozyten-Reagenz*; OLG Celle GRUR 1969, 548, 549*Abschaltplatte*.

[32] OLGR Düsseldorf 1999, 55, 58; OLG Hamburg GRUR-RR 2001, 137, 139 - *PM-Regler*.

[33] See BRAMMSEN (*supra*, note 27), § 17, note 15; KÖHLER (*supra*, note 26), § 17, note 8; WESTERMANN, Handbuch Know-how-Schutz, para. 50 (2007).

[34] But see BEATER, UnlautererWettbewerb 2002, § 18, para. 16; MAIER, Der Schutz von Betriebs-undGeschäftsgeheimnissenimschwedischen, englischen und deutschen Recht (1998), p. 305; OHLY (*supra*, note 26), § 17, note 10.

[35] HARTE-BAVENDAMM (*supra*, note 4), at 660-664; TAEGER (*supra*, note 4), at 456.

[36] WIEBE (*supra*, note 4), at 140-141.

[37] ANN (*supra*, note 26), at 39, characterises know-how as a "stepchild of intellectual property". He rightlynotes, however, that this paucity is relative, not absolute, see KRABER, Grundlagen des zivilrechtlichenSchutzes von Geschäfts- und Betriebsgeheimnissensowie von Know-how, GRUR 1977, 177;MAIER (supra, note 34); SCHLÖTTER, Der Schutz von BetriebsundGeschäftsgeheimnissen und die Abwerbung vonArbeitnehmern (1997).

[38] See BEIER/STRAUS, The Patent System and Its Informational Function - Yesterday and Today, IIC 1977, 387, 392-394; BEIER, The Significance of the Patent System for Technical, Economic and Social Progress, IIC 1980, 563, 581-583; LANDES/POSNER (*supra*, note 14), at 13-14, 294-297;MACHLUP/PENROSE, The Patent Controversy in the Nineteenth Century, 10 J. Econ. Hist. 1 et seq. (1950).

[39] See KRABER, Patentrecht, 5th ed. (2004), § 33 IV b 2 (p. 813); SAMUELSON/SCOTCHMER (supra, note 2), at 1611, however, entertain doubts. In the field of software patenting this point may require some further consideration since, arguably, the program is "reconstructed" in the course of decomplication.

[40] See EISENBERG, Patents and the Progress of Science: Exclusive Rights and Experimental Use, 56 U. Chi. L. Rev. 1017, 1023 (1989); HOLZAPFEL, Das VersuchsprivilegimPatentrecht und der SchutzbiotechnologischerForschungswerkzeuge, p. 110; RUESS, Accepting Exceptions? A Comparative Approach to Experimental Use in U.S. and German Patent Law, 10 Marq. Intell. Prop. L. Rev. 82, 87 et seq.

[41] Which is, however, of limited practical importance, see NIRK/ULLMANN, Patent-, GebrauchsmusterundSortenschutzrecht, 3rd ed. (2007), p. 183; RISBERG, Five Years without Infringement Litigation under theSemiconductor Chip Protection Act, 1990

Wis. L.Rev. 241, 277.

[42] Art. 5 (1) of Council Directive of 16 December 1986 on the legal protection of topographies ofsemiconductor products (87/54/EEC).

[43] § 6 I HalbleiterschutzG (Germany); 17 U.S.C. § 905 (USA).

[44] Parallel provisions: Art. 5 (3) of the EC Semiconductor Topographies Directive; § 6 II No. 3 HalbleiterschutzG (Germany); 17 U.S.C. § 906 (USA).

[45] Art. 9 (2) TRIPS.

[46] DREIER, in: DREIER/SCHULZE, Urheberrechtsgesetz, 2nd ed. (2006), § 69e, note 1; LOEWENHEIM, in:SCHRICKER (ed.), Urheberrecht, 3rd ed. (2006), § 69e, note 17.

[47] *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1520 et seq. (9th Cir. 1992).

[48] *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000).

[49] Art. 6 of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122, May 17, 1991, p. 42.

[50] On which see CORNISH/LLEWELYN (*supra*, note 25), para. 20-19.; DREIER, The Council Directive of14 May 1991 on the Legal Protection of Computer Programs, [1991] EIPR 319, 324-326.

[51] See DREIER (*supra*, note 46), § 69d, note 10; LOEWENHEIM (supra, note 53), § 69d, note 3; in favour of allowing decompilation for the purpose of repair LEHMANN (supra, note 5), § 76, para. 30.

[52] See BLOCHER in: Walter (ed.), EuropäischesUrheberrecht (2001), Software-RL, art. 5, note 33.

[53] See BONE, A New Look at Trade Secret Law: Doctrine in Search of Justification; 86 Cal. L.Rev. 241 (1998); CHEUNG, Property Rights in Trade Secrets, 20 Econ. Inquiry 40 et seq. (1982).

[54] On this discussion see, on the one hand, CHIAPETTA, Myth, Chameleon or Intellectual Property Olympian:A Normative Framework Supporting Trade Secrets Law, 8 Geo. Mason. L. Rev. 69 (1999); RISCH, Why Do We Have Trade Secrets? 11 Marq. Intell. Prop. L. Rev. 1 (2007), on the other hand BONE (*supra*, note 58).

[55] These references are frequent in the German „boot iron press "case (*supra*, note 3); for US law see the references given in *Kewanee Oil v. Bicron* (*supra*, note 18), at 481-482.

[56] See BONE (supra, note 57), at 294.

[57] *Kewanee Oil v. Bicron* (*supra*, note 18), at 487.

[58] REICHMAN, Legal Hybrids between Patents and Copyright, 94 Colum. L. Rev. 2432, 2507 (1994).

[59] See LANDES/POSNER (*supra*, note 10), at 364; RISCH (supra, note 58), at 37 et seq.

[60] LANDES/POSNER (*supra*, note 10), at 359.

[61] RISCH (supra, note 58), at 28 et seq.

[62] *Hodgkinson & Corby Ltd. v. Wards Mobility Services Ltd.* (No. 1) [1995] FSR 169, 174 et seq.; *L'Oréal SA v. Bellure NV*, 2007 EWCA (Civ) 968 at paras 138 et seq.

[63] *Sears, Roebuck & Co. v. Stiffel Co*., 376 U.S. 225 (1964); *Bonito Boats, Inc. v. Thunder Craft Boats, Inc*., 489 U.S. 141 (1989), see also REICHMAN (*supra*, note 62) at 2476.

[64] See § 4 No. 9 UWG

[65] See HILTY, in: AHRENS/BORNKAMM/KUNZ-HALLSTEIN (eds), Festschrift für Eike Ullmann (2006), pp. 643 et seq.