



Judicial Support for Semiconductor Reverse Engineering (I)

[Terry Ludlow](#)

date: Tuesday, October 10, 2006



The lights are bright in the 'surgery', but this isn't a hospital. A man in a lab coat is engaged in a delicate operation. By means of a precise and rigorous exploratory surgery, he will find out exactly what he needs to know.

Let's take a closer look. He's operating on... a cell phone?

The expert analyst in our scenario is not employing a surgical procedure to repair the cell phone; in fact, he is making use of reverse engineering to determine how the phone works in order to gain competitive intelligence on it and possibly, to see if it

might be infringing any patents.

The First Question

The first question people ask when they hear about semiconductor reverse engineering is invariably: Is it legal?

In fact, reverse engineering is entirely legal. Reverse engineering is a means of maintaining competition that is fair and healthy for the marketplace.

Historically, the ethical basis for reverse engineering is linked to the importance that copyright law ascribes to copying as an integral step in advancing knowledge. "If man has any 'natural' rights, not the least must be a right to imitate his fellows... Education...proceeds from a kind of mimicry and 'progress'...depends upon generous indulgence of copying." (B. Kaplan, *An Unhurried View of Copyright 2*, 1966)

In 1989, in *Bonito Boats, Inc. v. Thunder Craft Boats*, Justice Sandra Day O'Connor of the U.S. Supreme Court stated: "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. The novelty and nonobviousness requirements of patentability embody a congressional understanding, implicit in the patent clause itself, that free exploitation of ideas will be the rule, to which the federal protection of a patent is the exception."

"The public at large remains free to discover and exploit the trade secrets through reverse engineering of products in the public domain or by independent development... Reverse engineering of chemical and mechanical articles in the public domain often leads to significant advances in technology."

"The competitive reality of reverse engineering may act as a spur to the inventor creating an incentive to develop inventions which meet the rigorous requirements of patentability."

Reverse engineering is widely accepted in industry as a means for companies to obtain competitive intelligence. Every year, General Motors, for example, strips down dozens of brand new vehicles from their competitors to see what those competitors are doing.¹ In this way, they can find new ways to improve their own processes and perhaps lower costs. Every progressive company does competitive intelligence as a means to anticipate or respond to their competitors, whether in manufacturing or advanced technology. Reverse engineering for competitive intelligence is a completely acceptable and legal practice throughout industry.

In addition, reverse engineering is an efficient and effective way for your company to protect your patents by monitoring your competitor's technology, to detect if they are using your patented technology.

Nearly every large, successful corporation in the world uses reverse engineering in these two important ways: as a tool for competitive analysis and as a means to uncover possible patent infringements.

Competitive Intelligence and Innovation

Today, we live in a corporate world where business ethics are ever more crucial. Despite overheated competition in numerous markets, companies understand the need to follow strict ethical guidelines. They demand the maintenance of a fair and level playing field that is industry-wide. One way to guarantee fairness among competitors is for all parties to have equal access to technical competitive intelligence and patent intelligence through the use of reverse engineering.

The world's most innovative and creative companies are constantly in need of competitive intelligence to support rapid and continuous innovation. Those who are standing still are, in truth, moving backwards. Innovation is critical to a healthy economy. Anticipating, responding to, or adopting a competitor's innovations is an essential part of a successful business.

Innovative companies also protect their intellectual property by acquiring patents to prevent any misappropriation of their inventions. Obtaining the patent, however, is only the first step. Companies must aggressively monitor industry and competitive products in order to ensure that no one is using their patented innovations without permission.

The most effective way to gain competitive intelligence as well as monitor patents is simply to obtain the competitor's product, tear it open and look inside. Or, in other words, to reverse-engineer the product.

Not just GM but all automakers disassemble and inspect competitors' vehicles, telecommunications companies reverse-engineer cell phones, electronics companies reverse-engineer games systems and chipmakers put semiconductor dies and packages under the microscope.

Reverse engineering is a widely used, legally accepted means to gain competitive information. What you do with the information you gather from reverse engineering is the determining legal factor.

Historical Context

Since the advent of the semiconductor chip, several pieces of legislation have attempted to modernize the nature of copyright and intellectual property protection in an age of new technologies. At the same time, these legislative enactments have helped to clarify the meaning of 'fair use' in a digital age and most significantly have consistently provided support for legitimate reverse engineering activities.

Semiconductor Chip Protection Act (1984)

The Semiconductor Chip Protection Act of 1984 was enacted to deal with fears that foreign companies were unfairly competing with American semiconductor companies by creating rote copies of their chips, particularly memory chips. At the time, there was no protection for the physical layout or "maskwork" of a chip and it was not clear that copyright protection extended to programs embodied in integrated circuit chips. Historically, the Copyright Office had refused to register copyrights for chips or designs for chips. Clarification was required.

Reverse engineering was integrated into this legislation, acknowledging that copying is a part of the accepted mode of competition in the semiconductor industry. Title 17, Chapter 9 of the Act reads:

Title 17. Copyrights

Chapter 9. Protection of Semiconductor Chip Products

§ 906. Limitations on exclusive rights: reverse engineering; first sale

(a) Notwithstanding the provisions of section 905, it is not an infringement of the exclusive rights of the owner of a mask work for –

(1) a person to reproduce the mask work solely for the purpose of teaching, analyzing, or evaluating the concepts or techniques embodied in the mask work or the circuitry, logic flow, or organization of components used in the mask work; or

(2) a person who performs the analysis or evaluation described in paragraph (1) to incorporate the results of such conduct in an original mask work which is made to be distributed.

(b) Notwithstanding the provisions of section 905 (2), the owner of a particular semiconductor chip product made by the owner of the mask work, or by any person authorized by the owner of the mask work, may import, distribute, or otherwise dispose of or use, but not reproduce, that particular semiconductor chip product without the authority of the owner of the mask work.

This exclusion reaffirms the right to reverse engineer a competitor's chip to understand its operation and structure and learn from what is revealed. It also affirms the right to create new chips based on the legitimate reverse engineering of a protected work.

During hearings on the legislation, semiconductor industry spokespeople testified in favour of reverse engineering. The House of Representatives heard testimony that "the twin goals of certainty and encouragement of innovation can be achieved only if legitimate reverse engineering is permitted. We feel that existing 'fair use' provisions of Section 107 of the Copyright Law may not be sufficient, however, as they tend to emphasize non-commercial purposes."² The House of Representatives concluded "that it is an established industry practice tomake photo-reproductions of the mask work in order to analyze the existing chip so as to design a second chip with the same electrical and physical performance characteristics as the existing chip (so called 'form, fit, and function' compatibility), and that this practice fosters fair competition and provides a frequently needed 'second source' for chip products, it is the intent of the Committee to permit such reproduction by competitors....[and to bar] mere wholesale appropriation of the work and investment in the creation of the first chip." Competition in the semiconductor industry includes the study of competitors' chips as an acceptable mode of rivalry in the marketplace and is considered to be a major contributor fueling the pace of innovation and the level of innovation in

the semiconductor industry. Since the passage of the Semiconductor Chip Protection Act in the US in 1985, almost every country that designs, manufactures or uses semiconductors has passed an equivalent law, all with the reverse engineering clause included.

Digital Millennium Copyright Act (1998)

The most recent updating of the Copyright Act was signed into law by President Clinton in 1998. The Digital Millennium Copyright Act (DMCA) intends to offer protection to copyright holders against the circumvention of technological measures used to protect their works.

The technological measures referenced include the following:

- Measures that prevent unauthorized access to a copyrighted work and
- Measures that prevent unauthorized copying of a copyrighted work.

It is prohibited to make or sell devices that are used to circumvent either category of technological measure. This 'anticircumvention provision' means that it is unlawful to descramble a scrambled work, to decrypt an encrypted work, or otherwise avoid, bypass, remove, deactivate or impair a technological measure without the authority of the copyright owner.

The Act includes two exceptions relevant to reverse engineering:

- 1.) An exception for de-encrypting, only if it is required for research and if the copyright owner's permission has been requested, and
- 2.) An exception for reverse engineering but only for the limited purpose of achieving interoperability amongst computer programs.

These exceptions to restrictions are for specified types of reverse engineering, as constituted in Section 1201 (f) of the DMCA, which reads as follows:

(f) Reverse Engineering.

(1) Notwithstanding the provisions of subsection (a)(1)(A), 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 circumventions, to the extent any such acts of identification and analysis do not constitute infringement under this title.

Industry experts generally believed that the DMCA would prove to be a powerful anticompetitive tool, especially among OEMs (Original Equipment Manufacturers). At the time the anticircumvention provisions were being debated, there was concern that they would negate fair use of a copyrighted work, because if you cannot access the underlying copyrighted work without violating the anticircumvention provisions, you can't make a fair use of the work for reverse engineering and other purposes. But if you allow circumvention when the use is fair, there is no way to block the distribution of circumvention devices, as there is a legitimate purpose selling in them to support legal activities.

Nevertheless, the DMCA clearly states that, "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. § 1201(c)(1). This section, in particular, has been cited in succeeding cases brought under the DMCA. The conclusion that the courts have reached generally is that the DMCA does not eliminate fair use although it might make it less convenient.

To be continued. In Part II, we will find out about the courts' support of reverse engineering, and review a number of cases

FOOTNOTES:

1. "The Teardown Artists", www.wired.com/wired/archive/14.02/teardown
2. "The Semiconductor Chip Protection Act of 1983: Hearings before the subcommittee on Patents, Copyrights and trademarks of the Senate Committee on the Judiciary", 98th Congress, 1st session 75 (1983) Statement of Richard H. Stern.



Judicial Support for Semiconductor Reverse Engineering (II)

[Terry Ludlow](#)

date: Thursday, October 12, 2006



Courts Support Reverse Engineering

There are a clear line of cases that support reverse engineering for the purposes of understanding functionality and for reference in developing new versions of information or code. As long as a device or piece of software has been legitimately obtained, reverse engineering for the purposes of investigating and understanding the device or program is considered a legitimate purpose even if carried out in a commercial context.

Cases

The jurisprudential support for reverse engineering can be reviewed in a number of prominent cases.

Sega v. Accolade

One of the leading cases on fair use in the context of the reverse engineering of computer software is *Sega Enterprises Ltd. v. Accolade Inc.* 977 F.2d 1510 (9th Cir. 1992) ("*Sega*") decided by the Ninth Circuit Court of Appeal. The defendant, Accolade, had analyzed Sega's video game programs in order to determine the Genesis console compatibility requirements. Sega challenged Accolade's reverse-engineering process on the grounds that the intermediate copying during disassembly constituted a violation of Sega's copyright in the game cartridge object code.

The Ninth Circuit Court of Appeal held that Accolade's intermediate copying of the Sega object code would have constituted copyright infringement but was protected by the 'fair use' exception. The Court considered four relevant factors:

a) The purpose and character of the use

In considering the purpose of the use, the court determined that even though Accolade eventually used the information obtained by the copying to produce a competing product, this was not conclusive. Although the end goal was commercial in nature, the purpose was to study the functional requirements only, and therefore this use was legitimate.

b) The nature of the work

With respect to the nature of the work, the court noted that not all copyrighted works are entitled to the same level of protection. In particular, the protection provided by copyright does not extend to the ideas underlying the work. The fact that computer programs cannot be examined without a certain amount of literal copying proved to be a significant factor in this case.

c) The amount of the work copied

In considering the amount of the work copied, the court noted that even though Accolade copied the entire work, it would still not by definition preclude a finding of fair use.

d) The effect of the use upon the potential market for the copyrighted work

With respect to the effect on the potential market for the copyrighted work, the court cautioned against making this factor determinative. The court conceded that Accolade's entry into the game market undoubtedly affected the market for Genesis-compatible games in an indirect fashion, but further indicated that allowing Sega to try to monopolize the market by making it impossible for others to compete ran counter to the statutory purpose of the *Copyright Act* to promote creative expression. The court therefore found the fourth factor favored Accolade despite the minor economic loss that Sega might suffer.

Therefore, the court found that where disassembly is the only means to gain access to the ideas and functional elements embedded in a copyrighted computer program and where the reason for seeking such access is to achieve interoperability, disassembly is a fair use of the copyrighted work.

Atari v. Nintendo

In *Atari Games Corp. v. Nintendo of America, Inc.* 975 F.2d 832 (Fed. Cir. 1992) ("*Atari Games*"), a case decided shortly before *Sega*, the Federal Circuit Court reached a similar conclusion concerning the legality of reverse engineering. However, since the issue arose in the context of a preliminary injunction, the analysis was not as detailed

as in the Sega case. Further, in *Atari Games*, the fair use issue was complicated by the fact that Atari Games' lawyers lied to the U.S. Copyright Office to obtain the registration copy of Nintendo source code so that the firm's engineers could use it to finalize the development of compatible games. Nevertheless, the Federal Circuit Court ruled that the initial decompilation copying constituted fair use.

Sony Computer v. Connectix

The Ninth Circuit Court then reaffirmed the *Sega* ruling in *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000). The main difference between it and the *Sega* case was that Connectix disassembled Sony programs in order to develop emulation software to allow owners of Apple iMac computers to play Sony PlayStation games. That is, Connectix reverse-engineered in order to make a competing platform, not to make compatible games. The appellate court perceived no legal difference between the decompilation-for-interoperability considerations pertinent to development of competing platforms and those pertinent to games.

Lexmark v. Static Control Components

In *Lexmark International v. Static Control Components Inc.*, [253 F. Supp. 2d 943 \(ED Ky. 2003\)](#), Lexmark, a manufacturer of laser printers, alleged that Static Control had reverse-engineered Lexmark's "authentication" procedure in order to make its aftermarket laser printer cartridges work with Lexmark printers. Lexmark claimed that Static Control had manufactured, distributed and sold microchips for use with several of Lexmark's printers and toner cartridges, thus violating anticircumvention provisions of the Digital Millennium Copyright Act. At that time, Lexmark was granted a preliminary injunction that prevented Static Control from the sale of the microchips in question. The Sixth Circuit Court of Appeals ruled in 2004 that the injunction should not have been granted and that Static Control had not violated the provisions of the DMCA.

Circuit Judge Merritt, in his Concurrence, stated:

"We should make clear that in the future companies like Lexmark cannot use the DMCA in conjunction with copyright law to create monopolies of manufactured goods for themselves just by tweaking the facts of this case..."

"Lexmark would have us read this statute in such a way that any time a manufacturer intentionally circumvents any technological measure and accesses a protected work it necessarily violates the statute regardless of its 'purpose'. Such a reading would ignore the precise language – 'for the purpose of' – as well as the main point of the DMCA – to prohibit the pirating of copyright-protected works such as movies, music, and computer programs. ... Congress did not intend to allow the DMCA to be used offensively in this manner, but rather only sought to reach those who circumvented protective measures 'for the purpose' of pirating works protected by the copyright statute."

"As the Court explains, the fair use exception in copyright law explicitly looks to the purpose of the one making the copy in determining whether or not such copying violates the statute, and the DMCA itself contains a reverse engineering exception that also demonstrates Congress's aim merely to prevent piracy. ... A monopolist could enforce its will against a smaller rival simply because the potential cost of extended litigation and discovery where the burden of proof shifts to the defendant is itself a deterrent to innovation and competition. Misreading the statute to shift the burden in this way could allow powerful manufacturers in practice to create monopolies where they are not in principle supported by law. Instead, a better reading of the statute is that it requires plaintiffs as part of their burden of pleading and persuasion to show a purpose to pirate on the part of defendants. Only then need the defendants invoke the statutory exceptions, such as the reverse engineering exception.

"Finally, this reading of the DMCA is also supported by the provision in the Constitution that grants Congress the power to regulate copyright. Article I, section 8, of the Constitution gives Congress the power to regulate copyright in order to 'promote the Progress of Science and useful Arts.' U.S. Const. art. I, § 8, cl. 8. Congress gives authors and programmers exclusive rights to their expressive works (for a limited time) so that they will have an incentive to create works that promote progress. Lexmark's reading of the extent of these rights, however, would clearly stifle rather than promote progress. It would allow authors exclusive control over not only their own expression, but also over whatever functional use they can make of that expression in manufactured goods. Giving authors monopolies over manufactured goods as well as over their creative expressions will clearly not 'promote the Progress of Science and the useful Arts,' but rather would stifle progress by stamping out competition..."

Chamberlain v. Skylink

In *Chamberlain Group v. Skylink Technologies*, 292 F. Supp. 2d. 1040 (ND Ill. 2003) ("*Chamberlain II*"), Chamberlain alleged that Skylink reverse-engineered the protocol used to activate the controller for garage door openers manufactured by Chamberlain in order to sell their own compatible remote openers. Chamberlain sued under the DMCA but the court denied its case against Skylink in 2004.

The judgment from the United States Court of Appeals for the Federal Circuit states: "Chamberlain's proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use. It would therefore allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work—or even selected copies of that copyrighted

work. Again, this implication contradicts § 1201(c)(1) (of the DMCA) directly. Copyright law itself authorizes the public to make certain uses of copyrighted materials. Consumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software. What the law authorizes, Chamberlain cannot revoke."

A Wide Scope

In sum, U.S. law favors a relatively wide scope for reverse engineering. According to current case law, reverse engineering is not prohibited. The use of reverse engineering knowledge as reference material for the creation of competing hardware platforms and interoperable computer programs is also fully protected.

Conclusion

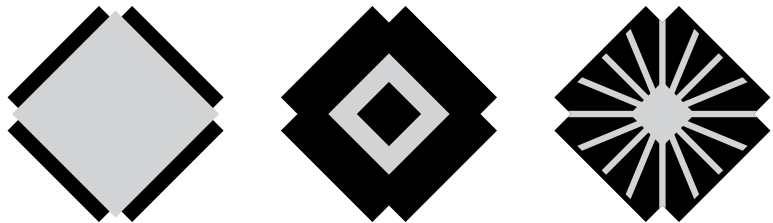
Reverse engineering for legitimate competitive research and the development of new innovations is a long-standing and respected method of gaining competitive information.

Numerous court decisions, including the key cases discussed above, have upheld the view that using reverse engineering to gain technical competitive intelligence and patent intelligence is justified under fair use provisions. Ultimately, reverse engineering is an important means of keeping companies ethical in highly competitive industries and, quite often, the only way to garner crucial patent intelligence.

There is no doubt that reverse engineering is essential for companies to maintain their competitive intelligence and to continue to innovate. In fact, reverse engineering is at the heart of all innovation in technology. No one works in a vacuum. Even Einstein's discoveries were based on the findings of earlier scientists. Discovery and innovation, or "the Progress of Science" as the Constitution so aptly puts it, depend on the ability to learn the most recent insights of one's competitors through reverse engineering.

For intellectual property attorneys, as well, reverse engineering can be a critical tool in helping them advise clients concerning patents and possible infringements. When the IP attorney needs to defend a client's patents against infringement by another party reverse engineering is often the only way to accurately determine the nature of the patents being employed in any particular product.

In all situations, reverse engineering is essential for success in gaining technical competitive intelligence and patent intelligence. Reverse engineering is one of the key factors for a company to ensure rapid innovation, whether that company is making cars, chips or drugs. The legislatures and the courts wholeheartedly agree with this view.



CHIPWORKS

CORPORATE HEADQUARTERS AND SALES

Canada

3685 Richmond Road, Suite 500
Ottawa, On K2H 5 B7 Canada
Tel: +1 613.829.0414 Fax: +1 613.829.0515
Email: info@chipworks.com

INTERNATIONAL SALES

Japan

Chipworks Kabushiki Kaisha (K.K.)
Ichigaya Tokyu Bldg., Suite 1011, 4-2-1 Kudan Kita, Chiyoda-ku
Tokyo 102-0073, Japan
Tel: +81.3.3511.7750 Fax: +81.3.3511.7751
Website: www.chipworks.co.jp Email: info@chipworks.com

Korea

Jae Ho, Kim
A-1121 DongYang Paragon, 17-2, JeongJa-Dong
BunDang-Gu, SeongNam, GyeongKi-Do, 463-842, Korea
Telefax: +82.31.782.8204 Mobile: +82.11.313.3204
Email: jhkim402@hanmail.net

Taiwan

Taipei International Business Center
Suite 620, 4F, 25, Sec. Tunhua S. Rd., Taipei, Taiwan, R.O.C.
Tel: +886.2.2577.4352 Fax: +886.2.2577.4157
Email: simonliu@chipworks.com

INTERNATIONAL REPRESENTATIVE

Israel

Tal Oren
Managing Director -Micon Lt.
Netcom Building, 8 Hanagar Street, Industrial Zone
Neve Ne'eman B, Hod-Hasharon 45240, Israel
Tel: +972.9.7756867 Fax: +972.9.7442386 Mobile: +972.52.3355497
Website: www.micon.co.il Email: tal@micon.co.il

OPERATIONS

Canada

3685 Richmond Road, Suite 500
Ottawa, On K2H 5 B7 Canada
Tel: +1 613.829.0414 Fax: +1 613.829.0515
Email: info@chipworks.com

Poland

ul. Krolowej Marysienki 90, 02-954 Warszawa Poland
Tel: +48.22.310.1250 or +48.22.310.1251 Fax: 48.22.310.1252