Intellectual Property Brief

Volume 2 | Issue 2 Article 4

9-25-2012

Reverse Engineering: Exploitation for Benefit of All

Daniel Lee
American University Washington College of Law

Reverse Engineering: Exploitation for Benefit of All

Keywords
Kewanee Oilv. Bicron, Semiconductor Chip Protection Act, SCPA, Sega Enterprises v.Accolade Inc., Digital Millennium Copyright Act DMCA, fair use

Reverse Engineering: Exploitation for Benefit of All

by Daniel Lee[1]

I. Introduction

Technology is evolving every day as consumers spend countless amounts of money buying new products and companies compete to produce better products. One catalyst of this technological innovation is reverse engineering by both developers and consumers. Reverse engineering is a method of recreating existing engineering concepts by analyzing the design and components of a final product to ascertain how the product operates.[2] Although this is clearly distinguishable from the traditional concept of forward engineering—which requires creating a product from abstract engineering ideas and concepts—it has been practiced as a useful tool to learn how to build a technology and make improvements.[3] Reverse engineering is well-exemplified in the computer software industry, where programmers constantly examine existing software to better understand the structure and make improvements on its operability.[4]

However, the legal threshold of reverse engineering is still unclear and controversial.[5] The scope of using existing protected technology differs depending on both the type of technology and the organizations devising regulations on reverse engineering.[6] The U.S. courts have allowed reverse engineering in a few occasions in the past, favoring competition for the development of technology over exclusive property rights.[7] On other occasions, courts have disallowed reverse engineering where a contract provision prohibited reverse engineering practices for unfair competition reasons.[8] Congress also has enacted laws that allow reverse engineering in several areas, such as semiconductor chips, but it remains relatively silent on other technological areas.[9] The legal issue becomes increasingly more complex today, as more consumers start exploring devices that they purchased in order to customize, maintain, and improve the devices using aftermarket components.[10]

This Article will examine the current legal scope of reverse engineering in the United States and present recommendations to better serve consumer interests without deterring innovation by companies.

II. The Supreme Court and Congress endorse the concept of reverse engineering

The Supreme Court and Congress have each allowed reverse engineering to promote competition and innovation of technology in the marketplace.[11] The first time that the Supreme Court dealt with the concept of reverse engineering was in *Kewanee Oil v. Bicron*, a case involving trade secret protection for synthetic crystal manufacturing.[12] In Bicron, a division of the plaintiff company, Harshaw Chemical, developed a seventeen-inch crystal for detection of ionizing

1. Daniel Y. Lee is a 2011 J.D. Candidate and an Article Writer for the Intellectual Property Brief at American University's Washington College of Law. He received his B.S. in Biochemistry/Cell Biology from the University of California, San Diego.

2. *See* Craig Zieminski, *Game Over for Reverse Engineering?: How the DMCA and Contracts Have Affected Innovation*, 13 J. Tech. L. & Pol'y 289, 292 (2008) ("Reverse engineering is the practice 'of starting with the known product and working backward to divine the process which aided in its development or manufacture.'").

3. *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 160 (1989).

4. Daniel Laster, *The Secret Is Out: Patent Law Preempts Mass Market License Terms Barring Reverse Engineering for Interoperability Purposes*, 58 Baylor L. Rev. 621, 635–36 (2006) (arguing reverse engineering of an original developer's software is necessary to obtain information for interoperability purpose).

5. *See* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L.J. 1575, 1577-78 (2002) (discussing that the implicit reverse engineering rules in the Agreement on Trade-related Aspects of Intellectual Property Rights and Economic Espionage Act of 1996 may be contrary to current trade secret law).

6. *Id.* (explaining the legal challenges to using direct molding to reverse-engineer boat hulls and using decompilation to reverse-engineer software).

7. *See id.* at 1578; *See also* Bradley E. Abruzzi, *Copyright, Free Expression, and the Enforcement of "Personal Use-Only" and Other Use-Restrictive Online Terms of Use*, 26 Santa Clara Computer & High Tech. L.J. 85, 90 (2010) (stating that the fair use doctrine allows courts to grant fair use privilege of copyrighted material in some occasions).

8. *See* Samuelson, *supra* note 4, at 1582 (noting that the Restatement of Unfair Competition protects trade secrets against wrongful acquisition, including where the disclosure breaches an agreement between the parties).

9. *Id.* at 1595–96 (discussing the Semiconductor Chip Protection Act's protection for the reverse engineering of computer chips).

10. Todd C. Adelmann, *Are Your Bits Worn Out? The DMCA, Replacement Parts, and Forced Repeat Software Purchases*, 8 J. Telecomm. & High Tech. L. 185, 186 (2010) (stating that equipment manufacturers are often allowed to control customers' ability to access the software in their equipment).

11. *See Bonito Boats, Inc*, 489 U.S. at 160 ("the competitive reality of reverse engineering may act as a spur to the inventor, creating an incentive to develop inventions that meet the rigorous requirements of patentability.").

12. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

radiation using a secret process that took seventeen years to develop.[13] The defendant company, Bicron, hired the plaintiff's former employees, who executed an agreement not to divulge confidential information or trade secrets that they obtained while working for Harshaw Chemical.[14] Bicron started manufacturing the same seventeen-inch crystal, and Kewanee Oil brought a diversity action against Bicron to seek injunction and damages for misappropriation of the trade secret.[15] The Sixth Circuit reversed the district court's decision for Kewanee Oil, reasoning that the crystal manufacturing process was an appropriate patentable subject matter under the federal patent law that preempts Ohio's trade secret law, and the process lost its patentability after being in the market for more than one year before its patent registration.[16] The Supreme Court in *Bicron* reversed the Sixth Circuit's decision and held that Ohio state trade secret law is not preempted by federal copyright and patent law in this case since there is no conflict among them.[17] The Court further held that trade secrets do not protect discovery by reverse engineering, which is defined as "a fair and honest means of starting with the known product and working backwards to define the process which aided in its development or manufacture."[18]

Later, in *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, the Court re-acknowledged the concept of reverse engineering and its importance by striking down a Florida law prohibiting the application of the "direct molding process" that helped replicate design boat hulls.[19] In *Bonito Boats*, Florida passed a state anti-plug molding law to protect boat hull designers from threats of competitors duplicating unpatented hull designs using a direct molding process.[20] The Court reversed the Florida Supreme Court's decision and held that states cannot offer patent-like protection to subject matter that is not deemed to be protected under the federal patent law.[21] The Court further held that federal patent law protects inventors from reverse engineering; however, "reverse engineering of chemical and mechanical articles in the public domain often leads to significant advances in technology," and that "the competitive reality of reverse engineering may act as a spur to the inventor, creating an incentive to develop inventions that meet the rigorous requirements of patentability."[22]

Congress also acknowledged the concept of reverse engineering when it passed legislation in a number of different technological areas specifically permitting reverse engineering. Such legislation includes the Semiconductor Chip Protection Act ("SCPA") and the Competition of Contracting Act of 1984 ("COCA").[23] The SCPA grants a reverse engineering privilege, allowing semiconductor chip designers to examine the design of the chips and circuits and use the knowledge obtained to design new chips.[24] In return for this privilege, the SCPA requires the chip designers to engage in enough forward engineering to develop an original chip design that qualifies for SCPA protection, fulfilling the purpose of furthering competition and technological development.[25] Similarly, COCA allows the defense industry to examine the spare parts it has purchased to promote competition in government contracts.[26]

Although reverse engineering is an approved method of technological advancement, it can do the exact opposite if no clear limitation is given to its practice. For example, critics of *Bonito Boats* argue that the decision did not benefit the market because approving the direct molding practice allowed boat hull designers to directly copy other competitors' hull designs, like photocopying a paper.[27] They claim that simply allowing one to almost directly copy another's design involves little or no reverse engineering, and it deters other designers from innovating by removing incentives.[28] To resolve this concern, Congress enacted a unique intellectual property protection statute in 1998 to protect boat hull designers from exploitation of their hull designs by unauthorized copying.[29]

In sum, the concept of reverse engineering seems to rely on an economic cost-benefit analysis of each practice.[30] Reverse engineering is likely allowed

13. *Id*. at 473.
14. *Id*.
15. *Id*.
16. *Id*. at 474.
17. *Id*.
18. *Id.* at 476.
19. *Bonito Boats, Inc.*, 489 U.S. 141 (1989).
20. *Id.* at 144-45.
21. *Id*. at 156-57.
22. *Id*. at 159–60.
23. Samuelson, *supra* note 4, at 1595-96; J.T. Westermeier, *Reverse Engineering*, 984 PLI/Pat 289, 312 (2009).
24. Samuelson, *supra* note 4, at 1595–96 ("[The SCPA] permits the copying of protected chip designs in order to study the layouts of circuits, and also the incorporation of know-how discerned from reverse engineering in a new chip.").
25. *Id*. at 1296.
26. Westermeirer, *supra* note 22.
27. Zieminski, *supra* note 1, at 293
28. *See* Samuelson, *supra* note 4, at 1593 ("Professor Heald has . . . point[ed]out that the Florida law 'primarily discriminates against those interested in reproduction rather than innovation.'").
29. *Id.* at 1594.
30. *See* Zieminski, *supra* note 1, at 293 (arguing that reverse engineering protections are appropriate where innovative advancements can be cheaply reverse engineered, but that protections are not appropriate where the innovator can make an adequate return on their investment before their product could be reverse engineered).

where the technology takes much effort and time to replicate, giving the innovator enough leading time to benefit from his invention.[31] On the other hand, it is likely prohibited where replication of technology is simple and inexpensive, because reverse engineering may deprive the innovator of the benefit of his lead-time.[32] Additionally, the Court seems to allow reverse engineering where it is necessary to understand basic fundamentals of technology in order to produce a new competing product.[33]

III. Effect of Overprotective licensing and user agreements

Ever since the Supreme Court and Congress allowed practices of reverse engineering, many producers have tried to avoid losing their exclusivity by putting specific terms in their license agreements that prohibit reverse engineering.[34] This is particularly seen in the computer software industry, where reverse engineering is used to decompile the source codes of existing programs in order to create a new program using the mechanism learned from decompiled source codes, mostly for "interoperability" purposes between other programs.[35]

In general, the courts have allowed reverse engineering of computer software if it is necessary to "develop a program that will interoperate with the decompiled or disassembled program."[36] A leading case cited for this rule is *Sega Enterprises v. Accolade Inc*.[37] In *Sega Enterprises*, Accolade wanted to produce game titles that would be compatible to Sega's Genesis platform.[38] However, Sega only licensed the initialization code and interface protocols necessary to produce games for the Genesis platform to game developers that would agree make Sega the exclusive manufacturer of all games produced by them.[39] When negotiations failed between Sega and Accolade, Accolade reverse engineered Sega's video games to figure out the Genesis' interface specifications, and then released several unlicensed game titles on the Genesis platform.[40] The Ninth Circuit held that Accolade's conduct was fair use under copyright law because it was done "solely in order to discover the functional requirements for compatibility with the Genesis console–aspect of Sega's programs that are not protected by copyright."[41]

The Ninth Circuit reaffirmed *Sega Enterprises* in *Sony Computers Entertainment, Inc v. Connectix Corp.,* where it held that Connectix's reverse engineering of Sony's Playstation in order to make a competing platform—not compatible games—was permissible fair use.[42] The court discussed that due to the nature of the copyrighted work, fair use of software needs to copy protected expression within the software to access unprotected elements of the software.[43] The Ninth Circuit's decision in *Sega Enterprises* has been subsequently adapted in other circuits regarding similar issues.[44]

In order to discourage legitimate reverse engineering of software by competitors, as held in *Sega Enterprises*, many software developers began using license contracts attempting to limit reverse engineering of their software.[45] These limiting contract terms define permitted uses and are often contained in shrink-wrap, click-wrap, or browse-wrap agreements.[46]

The courts' rulings on the enforceability of these license contracts are in conflict among themselves and highly controversial.[47] Courts sometimes reject reverse engineering defenses in trade secrecy cases when the

31. *Id*.
32. *Id*.
33. *See infra* Part B (discussing courts' rulings allowing decompilation of software for interoperability purposes).
34. *See* Abruzzi, *supra* note 6, at 106 (asserting that licensing agreement prohibiting reverse engineering are frequent).
35. *See* Samuelson, *supra* note 4, at 1613-15 (noting that computer programs are often reverse analyzed to customize the program for the user's needs, among other reasons).
36. *See Id*. at 1609, 1612.
37. Zieminski, *supra* note 1, at 294 (asserting that *Sega Enterprises* is the most cited case establishing permissible reverse engineering of software in video game hardware).
38. Sega Enter. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514 (9th Cir. 1992).
39. *Id*. at 1514.
40. *Id*. at 1514–15 (stating that after reverse-engineering several Sega games to discover the compatibility requirements for compatibility with the Genesis console, Accolade released its own game, "Ishido" for the Genesis).
41. *Id*. at 1522–23.
42. Sony Computer Entm't, Inc v. Connectix Corp., 203 F.3d 596, 602 (9th Cir. 2000).
43. *Id*. at 603–04.
44. *See DSC Communications Corp. v. DGI Techs., Inc.*, 81 F.3d 597, 601 (5th Cir. 1996) (adopting the Fourth Circuit's characterization of the copyright misuse defense in *Lasercomb*); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1539 N.18 (11th Cir. 1996) ("we find the *Sega* opinion persuasive in view of the principal purpose of copyright . . . ."); Mitel, Inc. v. Iqtel, Inc., 896 F. Supp. 1050, 1056-57 (D.Colo.1995) (characterizing the *Sega* principle as fair use and adopting it), aff'd on other grounds, 124 F.3d 1366 (10th Cir. 1997)).
45. See Zieminski, *supra* note 1, at 301 (noting that during the *Sega* era many companies tried to limit reverse engineering by including 'shrinkwrap' licenses with their software although these were rarely if ever enforced).
46. Shrink-wrap agreements are contained in sealed boxes of software; click-wrap agreements appear on computer screens before installation; and browse-wrap agreements are listed online where the users visit or download software. Abruzzi, *supra* note 6, at 110–12.
47. Samuelson, *supra* note 4, at 1626-27 ("The case law in the United States is in conflict on the enforceability of anti-reverse-engineering clauses in software contracts. . . Legislative approaches, however, have also been contentious").

use of the software is out of the scope of the license.[48] In other cases, courts decline to honor the shrink-wrap restrictions against reverse engineering because either the conflict license provision under state contract law is preempted by the federal copyright law or the license provision is unenforceable under contract law itself.[49]

The Fourth and Fifth Circuits decided two notable cases concerning these principles. In *Vault Corp. v. Quaid Software LTD.*, Vault manufactured floppy disks with PROLOCK feature, which enabled software developers to require the original copy of the floppy disk inserted in a computer to run the program.[50] PROLOCK disks also contained a user license agreement, as allowed under the Louisiana License Act, which prohibited purchasers from making copies of software.[51] Quaid software developed a program called RAMKEY, which enabled the computers to run and copy unauthorized copies of PROLOCK protected software.[52] The Fifth Circuit held that Quaid's decompilation of PROLOCK source codes was allowed as it was an essential step and federal copyright law preempted shrink-warp licenses under Louisiana contract law, and thus, the restriction within the license was invalid.[53]

In *Lasercomb America, Inc. v. Reynolds*, Lasercomb sold copies of its CAD/CAM die-making software to Reynolds with a licensing agreement that prevented Reynolds from making their own CAD/CAM die-making software.[54] After purchasing four copies of Lasercomb's software, Reynolds developed their own CAD/CAM die-making software by almost entirely copying Lasercomb's software.[55] The Middle District of North Carolina issued Lasorcomb a permanent injunction and damages.[56] However, the Fourth Circuit reversed the district court's decision and struck down Lasercomb's shrink-wrap license, holding that Lasercomb's use of copyright to control competition within its license in an area outside copyright was a misuse of copyright.[57]

Thus, even though courts remain split on the enforcement of the limiting license contracts, more weight can be given to the opinion that these license terms unlawfully discourage competition, taking the benefits of competition away from the public. It seems unfair for the software producers to prohibit what is otherwise perfectly lawful and beneficial to society by taking a side step to change the legal scope of reverse engineering.

IV. Reasonable Interoperability exception for reverse engineering

A lot of consumer electronics today have aftermarket producers for replacement parts.[58] The aftermarket parts industry is quickly growing as consumers have started to look for aftermarket parts that they can use to fix or upgrade their belongings.[59] Replacement parts range from simple items such as coffee maker filters and vacuum cleaner bags to more complicated items such as automobile parts.[60] However, replacement parts are often time model specific, and for these technically complicated aftermarket products, reverse engineering is a necessary step for the interoperability of their product with the original product.[61]

The Digital Millennium Copyright Act ("DMCA") adopted by Congress in 1998 makes reverse engineering of copyrighted material illegal, except when authorized by another statute.[62] Other than several exceptions to circumvention, the DMCA prohibits both individual acts of circumvention and distribution of tools and products of circumvention.[63]

A controversial aspect of the DMCA from a financial perspective is that it denies consumers' access to sub-program or components that are part of what they legally purchased as a package.[64] The DMCA's restriction on reverse engineering puts consumers in a financial disadvantage because the price for replacement parts to maintain the host product significantly goes up due to monopolistic control of product design by the

48. *Id*. at n.230.
49. *Id*.
50. *Vault Corp. v. Quaid Software LTD*., 847 F.2d 255, 256 (5th Cir. 1988).
51. *Id*. at 257.
52. *Id*.
53. *Id.* at 270.
54. Lasercomb America, Inc. v. Reynolds, 911 F.2d 970, 971 (4th Cir. 1990).
55. *Id*.
56. *Id*.
57. *Id*. at 978 (noting that although the licenses were negotiable, the presence of one such license was adverse to the public policy motivating copyright law).
58. *See* Adelmann, *supra* note 9, at 187–88 (citing printers and toner cartridges as an example)
59. *Id* at 188 (noting that in 2004 toner supplies made up more than 80% of Hewlett Packard's profits).
60. *Id*. at 188.
61. *Id*. at 190 (stating that such reverse engineering is generally allowed as long as the underlying software's copyrights are not infringed).
62. Samuelson, *supra* note 4, at 1635-36 (explaining that the DMCA permits circumvention for seven purposes: "legitimate law enforcement and national security purposes, achieving program-to-program interoperability, engaging in 'legitimate' encryption research, testing the security of computer systems, enabling nonprofit libraries, archives, and educational institutions to make purchasing decisions, allowing parents to control their children's use of the internet, and protecting personal privacy").
63. *See id*. at 1630.
64. Adelmann, *supra* note 9, at 203 (asserting that the DMCA's continuing protection for copyrighted material after its lawful purpose depends on whether the end user is within the bounds of his first sale rights).

producers.[65] This is especially so where certain software is needed to communicate between a replacement part and the host product.[66] For example, a printer cartridge often requires original cartridge software that allows the printer to recognize the cartridge as the original manufacturer's cartridge.[67] Even if mechanical specification of a third party's cartridge is the same as the original manufacturer's cartridge, the third party's cartridge would not function unless it could mimic the software signals generated by the original manufacturer's cartridge software.[68]

Aftermarket producers are allowed to use reverse engineering on manufacturer's software for interoperability purposes.[69] However, this is challenging because many manufacturers use security features, known as technological protection measures, to make it harder for aftermarket manufacturers to break into their copyrighted software.[70] These electronic security measures are protected by the DMCA's anti-circumvention provision, which generally prohibits circumvention of the technological protection measures for copyrighted material regardless of the existence of a copyright violation.[71] In addition, DMCA also contains an anti-trafficking provision, which makes development and distribution of tools for circumvention of protected work illegal.[72] This makes developers of circumvention tools liable even if they do not ever use these tools to infringe copyrighted materials.[73] Today, DMCA protection can be extended to all software that has electronic locks, which is most.[74] Unless some exceptions are clearly outlined for circumvention of the electronic lock protection, aftermarket part producers would be reluctant to enter into the market, losing potential competition. This could lead consumers to suffer greater economic loss from expensive original manufacturer's tangible aftermarket parts.

Many inventors agree with the strict protection mechanism in the DMCA.[75] On the other hand, some scholars argue that a reasonable degree of reverse engineering should not be banned unless the activity is parasitic or market destructive.[76] However, if we want to achieve the goal of a greater public good by promoting competition, there must be more flexible interoperability exceptions to tangible aftermarket parts to ease the entry into the market and bring the cost down for consumers.

V. Conclusion

Reverse engineering is an effective tool to drive competition and innovation, when a reasonable limit can be found. The Supreme Court and Congress have both acknowledged its usefulness and tried to draw a clear line in which reverse engineering constitutes infringement or fair use. Regardless of much effort, however, reverse engineering is still a controversial topic. If we want to promote a greater good for consumers and the public at large, we need to focus on bringing in more competition to best utilize our innovation. One way to do this is by providing more flexible interoperability exceptions for reverse engineering to expand choices and reduce costs for consumers.

65. *Id*. at 187–89 (emphasizing that manufacturers may maintain a monopoly on aftermarket parts necessary to operate a host device or intentionally cause non-communicative parts to function poorly, creating a monopoly on competitive parts).
66. *Id*. at 189.
67. *Id*.
68. *Id*.
69. *Id*. at 194–95.
70. *Id*. at 190; *See also* Samuelson, *supra* note 4, at 1631–32 (citing cable and satellite television as examples of technology with copy-protection measures).
71. Adelmann, *supra* note 9, at 190.
72. *Id*. at 193 (stressing that this is the most discussed, debated, and novel aspect of the DCMA).
73. *Id*.
74. *Id.* at 191.
75. *See generally* Samuelson, *supra* note 4, at 1634–35 (implying that copyright industry representatives agreed with DCMA protection but "opposed any exception for fair uses").
76. *Id*. at 1653.