Pamela Samuelson

# Reverse Engineering Under Siege

## Is reverse engineering a lawful way to acquire trade secrets?

Reverse engineering has always been a lawful way to acquire trade secrets embodied in mass-marketed products. This longstanding principle—on which software engineers as well as engineers in other fields so frequently rely—could be significantly undermined depending on the outcome of a case now pending before the California Supreme Court. The precedent set in this case could, in turn, influence courts in other jurisdictions. A key issue in the case—one that legal scholars and intellectual property lawyers have debated for many years—is whether an anti-reverse-engineering clause in a mass-market license should be enforceable.

The California case, *DVD CCA v. Bunner*, presents this issue squarely, although the litigants have thus far primarily focused on whether Bunner had a free speech right (or not) to post a computer program on the Internet developed, in part, with aid of information derived from reverse engineering allegedly in violation of such a mass-market license.

This column will explain why the California court should reaffirm the longstanding rule that reverse engineering is a lawful way to acquire trade secrets and should reject the premise that breach of a mass-market license forbidding reverse engineering is an improper means to obtain a trade secret. The litigants' emphasis on free speech issues has obscured the considerable weaknesses in the trade-secret theory in this case.

In January 2000 the DVD Copy Control Association (DVD CCA) charged Andrew Bunner (and others, including Andrew McLaughlin) with trade-secret misappropriation for posting on the Internet a computer program known as DeCSS, which allegedly contained or was substantially derived from trade secrets embodied in an encryption program, the Content Scramble System (CSS), widely used in DVD players and DVD discs under license from DVD CCA or its predecessors in interest. DVD CCA claimed that a Norwegian teenager, Jon Johansen, misappropriated CSS trade secrets when he reverse-engineered CSS in breach of a mass-market license provision forbidding such activities, and that Bunner knew or should have known that DeCSS embodied or was derived from stolen trade secrets when he posted this program on his Web site.

Bunner argued he was exercising his free speech rights under the First Amendment to the U.S. Constitution when he posted DeCSS on his Web site. Bunner relied in part on cases holding that the First Amendment protects computer programs as expressions of programming ideas. The trial judge rejected this defense, and after concluding that DVD CCA was likely to prevail on its trade-secret

JASON SCHNEIDER

claim against Bunner, the judge issued a preliminary injunction, ordering Bunner to take DeCSS down from his Web site pending trial on the merits [5]. Bunner appealed this ruling to the California Court of Appeals. The appellate court found merit in Bunner's First Amendment defense and hence reversed the trial judge's ruling without addressing the trade-secret claims in the case [4]. DVD CCA then asked the California Supreme Court to review this ruling, claiming it would have a ruinous effect on California's high-tech sector and other industries. The California Supreme Court agreed to hear the appeal. Its decision can be expected by the end of the year.

The California Supreme Court has several options for resolving this case. DVD CCA hopes the court will reinstate the preliminary injunction and rule that enjoining disclosure of stolen trade secrets is categorically immune from First Amendment challenge. This would have significant negative implications for industries that rely on reverse engineering. Bunner hopes the court will rule that the First Amendment protects his posting of DeCSS on the Internet even if it was derived from stolen trade secrets.

A broad affirmance could have deleterious impacts on industries relying on trade-secret protection. A better outcome would be for the California Supreme Court to realize the trade-secret claims in this case are weak and to affirm the Court of Appeals decision in favor of Bunner on trade-secret grounds, as a law professor brief amicus curiae (that is, a friend of the court brief) argues to the California Supreme Court [2].

## Reverse Engineering and Trade-Secret Law

California trade-secrecy law explicitly provides that reverse engineering is a lawful way to acquire a trade secret, as do the laws of other jurisdictions. Several reasons support reverse engineering as a sound principle of trade-secret law [8]. Purchase of a product in the open market generally confers personal property rights in the product, including the right to take the product apart, measure it, subject it to testing, and the like. The time, money, and energy reverse engineers invest in analyzing products may also be a way of "earning" rights to the information they learn thereby. The law also regards the sale of a product in the open market as a kind of publication of innovations it embodies and a dedication of them to the public domain unless the creator has obtained patent protection for them. Trade-secret misappropriation arises only if a person or firm misuses or discloses the secret in breach of an agreement or confidential relationship, engages in other wrongful conduct (bribery, coercion, trespass) to obtain the secret, or acquires the secret from a misappropriator knowing or having reason to know that the information was a misappropriated trade secret.

Courts in the U.S. have also treated reverse engineering as an important factor in maintaining balance in intellectual property law. Patent law allows qualifying innovators up to 20 years of exclusive rights to make, use, and sell the invention, but only in exchange for disclosure of significant details about their inventions to the public. This deal is attractive in part because if an innovator chooses to protect the invention as a trade secret, this protection may be short-lived if the innovation can be reverse-engineered. If state legislatures or courts tried to make trade secrets immune from reverse engineering, this would undermine patent policy because it would, in the words of a federal appellate court in *Chicago Lock v. Fanberg*, "convert the company's trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords" [3].

The U.S. Supreme Court in *Bonito Boats v. Thunder Craft Boats* [1] struck down a Florida law that forbade manufacturers of boats from using existing boat parts as "plugs" for a direct molding process that yielded competing products. This law "prohibit[ed] the entire public from engaging in a form of reverse engineering of a product in the public domain." The Court said it was "difficult to conceive of a more effective method of creating substantial property rights in an intellectual creation than to eliminate the most efficient method for its exploitation." The Court said its prior rulings protected "more than the right of the public to contemplate the abstract beauty of an otherwise unprotected intellectual

creation—they assure its efficient reduction to practice and sale in the marketplace." The Court went on to say "[w]here an item in general circulation is unprotected by a patent, '[r]eproduction of a functional attribute is legitimate competitive activity.'"

The Court in *Bonito Boats* regarded reverse engineering as "an essential part of innovation," likely to yield variations on the product that "could lead to significant advances in technology." The Court added that "the competitive reality of reverse engineering may act as a spur to the inventor" to develop additional patentable ideas. Even when reverse engineering does not lead to additional innovation, the *Bonito Boats* decision suggests it may still promote consumer welfare by providing consumers with competing products offered at a lower price.

It is difficult to explain why the judges in *Bunner* have failed to consider the public policy reasons why trade-secret law permits reverse engineering and why enforcement of anti-reverse engineering clauses might frustrate these policies. Hopefully, the California Supreme Court will rectify this.

## Anti-Reverse-Engineering Clauses

The very reasons reverse-engineering is socially beneficial—for example, in eroding a first-comer's market power and enabling follow-on innovation—help to explain why some firms want to thwart it, as by requiring customers to agree not to reverse-engineer the product. From the early days of the computer software industry, anti-reverse-engineering clauses have been common in software licenses (even though software engineers routinely engage in reverse engineering). Even as a mass market for software evolved, firms continued to include anti-reverse-engineering clauses in so-called shrinkwrap or click-through licenses. Although a few cases have enforced anti-reverse-engineering clauses in negotiated licenses between sophisticated parties, no court has yet enforced a mass-market license restriction on reverse engineering and at least two courts have refused to do so.

The trial court ruling in *Bunner* is the only case in which a court has premised a finding of trade-secret misappropriation on breach of an anti-reverse-engineering clause of a mass-market license, and that decision was reversed on appeal, albeit on free speech grounds.

*Vault v. Quaid* [10] is a federal appellate case that refused to enforce a mass-market license restriction on reverse engineering and rejected a claim of trade-secret misappropriation based on reverse engineering in breach of such a license term. Vault sued Quaid because Quaid reverse-engineered Vault's Prolok program and developed a program (Ramkey) capable of bypassing the copy-protection feature of the Prolok program. Vault charged Quaid with copyright infringement (because of the intermediate copying of the Prolok program undertaken in the reverse-engineering process) and contributory copyright infringement (because users of Quaid's Ramkey program could make copies of programs protected by the Prolok copy-protection system). But it also complained that Quaid had breached a shrinkwrap license forbidding reverse engineering and that Quaid had thereby misappropriated trade secrets embedded in Prolok. The Fifth Circuit Court of Appeals decided the copyright claims were without merit and that enforcement of the shrinkwrap license's anti-reverse-engineering clause would conflict with federal copyright policy. The trial court ruled that Quaid's reverse engineering activities did not violate state trade secrecy law, and the claim was apparently so weak that Vault did not even appeal this ruling.

While the case law on anti-reverse-engineering clauses of mass-market licenses is relatively sparse, a substantial number of legal commentators have recommended courts not enforce such clauses. David McGowan, a professor at the University of Minnesota Law School, for example, has expressed concern that enforcement of such clauses would lead to "lethargic transition among standard products [in the software industry] and diminished production of works building upon ideas embedded in object code" [6]. Commentators agree that the availability of future competitive products represents a

public interest that would be thwarted if anti-reverse-engineering clauses were enforced. McGowan points out that if "reverse engineering furthers copyright's goal of promoting the dissemination and improvement of intellectual property [and] reverse engineering does not deprive authors of returns necessary to induce investment … then competition policy would favor reverse engineering as a device to lower the cost of transition among standard products (thereby increasing allocative efficiency) without infringing on copyright goals or methodology"[6].

The California Supreme Court should heed these concerns and rule that reverse engineering cannot constitute trade-secret misappropriation claims, even when done in breach of a mass-market license. The continued competitiveness and innovation of the California computer industry—and indeed, of all industries that could impose mass-market license restrictions on reverse engineering—depends on nonenforcement of such clauses.

## Secrets Leak on the Internet

A second major weakness of the trade-secret misappropriation claim in *DVD CCA v. Bunner* is that the secret was no longer a secret by the time Bunner posted DeCSS on the Internet. It had already been widely posted on the Internet, both in source and object code forms, before Bunner ever got a copy. By the time Bunner posted DeCSS on his Web site, any trade secrets of CSS revealed by DeCSS were already leaked. It was too late to put the genie back in the bottle.

Among the failed trade-secret cases that resemble *Bunner* is *Religious Technology Center v. Lerma* [7]. RTC claimed copyright and trade-secret interests in certain texts the Church of Scientology uses in its religious practices. RTC sued the *Washington Post* for copyright infringement and trade-secret misappropriation based on the *Post*'s duplication of documents containing the alleged trade secrets and publication of portions of the RTC texts. The information had been available in publicly accessible court records as an appendix to an affidavit in a California courthouse for more than two years, notwithstanding RTC's efforts to maintain its trade-secret status by sending its agents to the courthouse to block others from having access to the documents. Documents containing this information had also been posted on the Internet for 10 days. The *Post* knew RTC claimed this information as a trade secret and, in fact, returned to RTC's lawyers one document RTC alleged had been stolen. However, the *Post* was able to obtain another copy of the same document from the clerk of the court in California.

By the time the *Post* received the document, the trade-secret status of the information had been lost. "Once a trade secret is posted on the Internet," said the court, "it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade-secret misappropriation, the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct in interacting with the Internet."

Given the specific facts of the *Lerma* case, the judge was correct in ruling that the public availability of information had destroyed RTC's trade-secret claim. However, posting information on the Internet may not automatically cause it to cease to be a trade secret. If information is posted on an obscure site and its owner quickly detects its presence on the Internet, a firm may be able to obtain a court order to remove the information from the Internet and enjoin its reposting.

However, the longer information is available on the Internet, the more sites where it is available, the larger the number of people who have accessed the information, and the more word has spread about the availability of the information (through newsgroups or in chatrooms), the greater the likelihood that trade-secret status will be lost. This is unfortunate, of course, but there is always an inherent risk in relying upon trade-secrecy law that the information will leak out, particularly where the information is susceptible to being reverse-engineered.

*Lerma* and similar cases do not invoke the First Amendment to vindicate the publication of previously secret information by someone who was not a party to the misappropriation. First Amendment defenses are rare in trade-secret cases because trade-secret law contains limiting principles that make recourse to the First Amendment unnecessary. Trade-secret

**First Amendment defenses are rare in trade-secret cases because trade-secret law contains limiting principles that make recourse to the First Amendment unnecessary.**

laws do not confer exclusive property rights in the secrets that are good against the whole world. Trade-secret laws only protect against certain kinds of unfair conduct, such as uses or disclosure of the secret in breach of confidential relationships and the use of wrongful means to obtain the secret.

## DeCSS and the DMCA

Winning before the California Supreme Court does not necessarily mean that Bunner can repost DeCSS without worrying about legal consequences. Attentive readers will be aware that Eric Corley (aka Emmanuel Goldstein) has been enjoined from posting DeCSS on the Web site of *2600* magazine [9]. Corley posted DeCSS on the *2600* site as part of the magazine's coverage of a controversy about the DeCSS program and the movie industry's interest in suppressing its dissemination. Corley also linked to sites where DeCSS could be found.

Universal City Studios sued Corley under the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) the U.S. Congress passed in 1998. Corley argued the First Amendment protected his posting of DeCSS in the course of news coverage as well as his linking to sites where DeCSS had been posted. Neither the trial judge nor the appellate judges found merit in these arguments [9]. They ordered Corley not to post or link to DeCSS because this provided others with a technology primarily designed to circumvent a technical measure (namely, CSS) movie companies were using to protect access to their works in violation of the DMCA rules.

The injunction against Corley is not necessarily the end of the debate about the First Amendment and the DMCA, even as to DeCSS and other CSS descramblers. Consider the Gallery of CSS Descramblers research scientist David Touretsky has maintained on his Web site at Carnegie Mellon University (www-2.cs.cmu.edu/~dst/DeCSS/Gallery/) Representatives of the movie industry have asked Touretsky to remove this gallery from his Web site, alleging that it violates the DMCA anticircumvention rules. As yet, they have not brought a lawsuit against him. Perhaps this is because the movie industry cannot be sure other courts will follow the *Corley* analysis of the DMCA and the First Amendment or extend it further to Touretsky and CMU. Touretsky's Web site, after all, is academically rigorous and explains CSS and the principles of descrambling it in considerable detail. It looks very much like the kind of expression of ideas that the First Amendment was meant to protect.

If the California Supreme Court affirms the California Court of Appeal First Amendment ruling in *Bunner*, DVD CCA would almost certainly seek U.S. Supreme Court review on the ground it conflicted with the First Amendment ruling in the *Corley* case. The U.S. Supreme Court accepts a small number of cases for review, but it is more likely to hear an appeal when a conflict exists between appellate courts decisions on the same legal issue, such as whether the First Amendment protects a particular activity on the Internet. The Electronic Frontier Foundation, which has represented both Corley and Bunner in the lawsuits, would welcome the chance to persuade the Supreme Court that DeCSS is expression protected by the First Amendment.

## Conclusion

*DVD CCA v. Bunner* is one of the most important cases the California Supreme Court will decide in the next year. Thus far, virtually all of the analysis in the case has focused on Bunner's First Amendment defense. Free speech rights may be a more exciting basis for a legal defense than the trade-secret issues discussed here. However, these legal defenses should not be neglected.

In this column, I have explained why the California Supreme Court should reject DVD CCA's theory that breach of a mass-market license clause forbidding reverse engineering is an improper means to obtain a trade secret. Even if the Court decides the breaching reverse engineer could be held for trade-secret misappropriation, this does not mean a person so remote from the misappropriation as Bunner should be held liable for the misappropriation given the infor-

mation was widely available on the Internet at the time he posted it.

The future of reverse engineering and other limiting principles of trade-secret law will be affected by the California Supreme Court's ruling. Hopefully, the California Supreme Court will affirm the Court of Appeals' ruling in favor of Bunner on trade-secret grounds. This seems more likely than a ruling that upholds the right to post misappropriated trade secrets as a matter of free speech law. C


## References

1. *Bonito Boats, Inc. v. Thunder Craft Boats*, Inc., 489 U.S. 141(1989)
2. Brief Amicus Curiae of Law Professors In Support of Affirmance to the California Supreme Court in *DVD CCA v. Bunner*; available at www.sims.berkeley.edu/~pam/papers/bunneramicus.
3. *Chicago Lock Co. v. Fanberg*, 676 F.2d 400 (9th Cir. 1982).
4. *DVD CCA v. Bunner*, 93 Cal. App.4th 648, 113 Cal. Rptr. 338 (2001)
5. *DVD CCA v. McLaughlin*, 2000 WL 48512 (Calif. Super. 2000); www.eff.org/pub/Intellectual_property/Video/DVDCCA_case/20000120-pi-order.html.
6. McGowan, D. Free contracting, fair competition, and article 2B: Some reflections on federal competition policy, information transactions, and aggressive neutrality. *Berkeley Tech. L.J. 13*, 1173, 1998.
7. *Religious Technology Center, Ltd. v. Lerma*, 908 F. Supp. 1362 (E.D. Va. 1995).
8. Samuelson, P. and Scotchmer, S. The law and economics of reverse engineering. *Yale L. J. 111*:1575 (2002).
9. *Universal City Studios, Inc. v. Corley*. 273 F.3d 429 (2d Cir. 2001).
10. *Vault Corp. v. Quaid Software Ltd*. 847 F.2d 255 (5th Cir. 1988).


**Pamela Samuelson** (pam@sims.berkeley.edu) is a Chancellor's Professor of Information Management and Law at the University of California, Berkeley.

Research support for this work comes from NSF Grant. No. SES 9979852.