Trade Secrets vs. Free Speech

How to balance the benefits of free speech and the need for secrecy.

Andrew Bunner was one of several hundred persons who posted a computer program known as DeCSS on the Internet in the fall of 1999. DeCSS enables users to bypass the Content Scramble System (CSS) used to protect DVD movies. Two months later, DVD Copy Control Association (DVD CCA) charged Bunner and 520 others (including 500 "John Does") with trade secret misappropriation, claiming the defendants posted DeCSS on the Internet, knowing or having reason to know that it embodied or was substantially derived from trade secrets stolen by Jon Johansen, a Norwegian teenager, who, they claimed, reverse engineered CSS secrets in violation of an anti-reverse engineering clause of a DVD player shrinkwrap license. Bunner's main defense was that DeCSS was First Amendment-protected "speech" that he and others were entitled to republish.

In January 2000, a California judge issued a preliminary injunction forbidding Bunner from posting DeCSS on the Internet or otherwise disclosing CSS secrets. The California Court of Appeal, assumed (without deciding) that DVD CCA had shown a reasonable likelihood of success on the merits of the trade secret claim (a necessary finding for a preliminary injunction to issue), but agreed with Bunner that DeCSS in source code form was First Amendment-protected speech and that the preliminary injunction was an unconstitutional prior restraint on speech. The California Supreme Court agreed to hear DVD CCA's appeal almost a year ago, but has yet to schedule argument in the case.

A previous column ("Reverse Engineering Under Siege," Oct. 2002) explained why Bunner should have won this case on trade secret grounds: first, because reverse engineering of a mass-marketed product is a proper way to acquire a trade secret, notwithstanding a shrinkwrap license provision prohibiting it, and second, because DeCSS has been so widely published on the Internet that any CSS secrets it might have contained have dissipated. In this column, I will consider the merits of Bunner's free speech defense.

Defending Free Speech

In response to DVD CCA's motion for a preliminary injunction, Bunner filed a document with the court (known as a declaration) stating he had learned about DeCSS from reading postings on the slashdot.org Web site and decided to post DeCSS in source code form on his Web site in order to aid those who, like

ROBERT NEUBECKER

In rare instances, however, the First Amendment may trump trade secret rights, and *Bunner* may be such a case.

himself, wanted to play DVDs on computers running the GNU/Linux operating system and to aid open source development of a Linux-based DVD player. Publishing a text on the Internet in order to communicate the ideas and information it contains seems to be the kind of activity the First Amendment is meant to protect.

The trial judge, however, thought so little of Bunner's First Amendment defense that his opinion did not even mention such a defense had been raised. The California Court of Appeal, in contrast, found the First Amendment defense quite compelling. The court agreed with Bunner that the DeCSS program in source code form was First Amendment-protected expression, which he had a First Amendment right to republish. "Regardless of who authored the program," the court said, "DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS." (The court hinted, without deciding, that object code would be treated differently.)

The Court of Appeal characterized the preliminary injunction against publication of DeCSS source code as a regulation of "pure speech" and a classic prior restraint that "bears a heavy presumption against its constitutional validity." The court invoked *New York Times v. United States*, the Supreme Court's famous decision refusing to enjoin publication of the Pentagon Papers by the *New York Times* and *Washington Post*. The Court of Appeal opined that "DVD CCA's statutory right to protect its economically valuable trade secret is not an interest that is 'more fundamental' than the First Amendment right of free speech or even on an equal footing with the national security interests and other vital interests that have previously been found insufficient to justify a prior restraint." Hence, it concluded that Bunner's First Amendment defense was sound. The court did not rule out the possibility of permanent injunctive relief if DVD CCA won on the merits (not seeming to realize that allowing CSS secrets to be published on the Internet prior to trial would dispel the secrets and render the claim moot).

The concept of prior restraint may not be familiar to many *Communications* readers; here's the basic idea. The First Amendment was added to the U.S. Constitution because the founders wanted to ensure the new government they were establishing would not be able to prevent critical commentary about the government from being spoken or published, as the British had done prior to the American Revolution. Protecting free speech and a free press was deemed essential to maintaining a free and democratic society. Let people say what they have to say, and if they have violated the law in so saying, punish them afterward. In the famous Pentagon Papers case, for example, the *New York Times* and *Washington Post* knew Daniel Ellsberg had purloined the Pentagon Papers they were publishing, and the newspapers risked civil and criminal liability for publishing excerpts from them. However, the Supreme Court decided that even a serious risk of damage to U.S. national security interests did not justify a prior restraint on publication of these documents.

The default principle of First Amendment law, then, is to place responsibility on a speaker or publisher to weigh the consequences of possible civil or criminal liability for wrongful speech or publication and to trust that rational assessments of risk will generally deter illegal speech and publication. For the most part, this system works quite well. Before charging a public official with corruption, for example, newspapers tend to double-check

their facts. This makes news reports more reliable than they might otherwise be, and it also reduces the risk the papers will be sued for millions of dollars in damages for libel. It seems fair to assume the risk of civil and criminal liability substantially deters wrongful disclosures of trade secrets as well as other wrongful speech acts.

Spectrum of Theories

The trial court decision in *Bunner* is consistent with the theory that trade secret lawsuits are categorically immune from First Amendment/free speech scrutiny. The judge did not expressly endorse this view, but did so implicitly by ignoring that a First Amendment defense had even been raised. The Court of Appeal decision embraced a polar opposite theory under which preliminary injunctions against disclosure of trade secrets are constitutionally suspect on First Amendment grounds. Briefs submitted by DVD CCA to the California Supreme Court argue that the Court of Appeal's decision will eviscerate trade secrecy law in the state of California.

Neither extreme theory is tenable, in my view. Preliminary and permanent injunctions are routinely granted in trade secret cases without offending the First Amendment, and this is as it should be. In the ordinary trade secret case, the misappropriator of trade secrets is an errant licensee, a faithless employee or former employee, an abuser of confidences, a trickster who uses deceit or other wrongful means to obtain the secrets, or a knowing recipient of misappropriated information trying to free-ride on the trade secret developer's investment. In such cases, injunctions merely require persons to abide by express or implicit agreements they have made, respect the confidences under which they acquired secrets, and refrain from wrongful acts vis-à-vis the secrets. The First Amendment does not give anyone the right to engage in unfair competitive activity of the sort that trade secrecy law typically regulates.

In rare instances, however, the First Amendment may trump trade secret rights, and *Bunner* may be such a case. In the small number of trade secret cases in which free speech defenses have succeeded, the alleged misappropriator had neither a contractual nor confidential relationship with the trade secret claimant, and had neither engaged in any wrongful acts in acquiring information, nor aided or abetted the misappropriation, but was merely a recipient of allegedly misappropriated information.

In an Oregon case, *Sports Management News, Inc. v. Nachtigal*, for instance, Adidas charged SMNI with trade secret misappropriation for publishing information about future sneaker designs. Adidas asserted these designs were its trade secrets, that its employees were under obligations not to disclose this information, and SMNI either knew or should have known it was publishing misappropriated trade secrets. A trial judge issued a preliminary injunction against publication of any further information about Adidas designs and ordered SMNI to submit information it planned to publish about Adidas designs to the court for its approval prior to publication. The Oregon Supreme Court agreed with SMNI that this was an unconstitutional prior restraint on speech and lifted the trial court's injunction.

Unfortunately, the U.S. Supreme Court has provided little or no guidance about how to resolve conflicts between trade secrets and the First Amendment. Trying to predict how the Supreme Court would rule in *Bunner* is difficult given that First Amendment law is not entirely consistent. Various theories exist about how much speech the First Amendment protects and why. Some scholars take a narrow view and believe the First Amendment only protects against prior restraints of political speech. However, the Supreme Court has protected many other kinds of speech, including commercial speech (for example, advertisements), art, and entertainment. At least two appellate courts have decided that computer programs, at least in source code form, are First Amendment-protected speech (and the Court of Appeal in *Bunner* relied on these cases).

Code As Speech

Universal City Studios v. Corley was one of the decisions that

From the standpoint of computer technologists, it may seem strange, or even perverse, for courts to consider making a distinction between source and object code.

ruled computer programs can be First Amendment-protected speech. As some readers may know, *Corley* also involved an injunction against the posting of DeCSS on the Internet (although *Corley* involved a permanent injunction after trial on the merits, not a preliminary injunction, as in *Bunner*). Although Corley was also a defendant in *Bunner*, he didn't appeal that trial court decision, perhaps because he was so intensely engaged in the parallel lawsuit brought by seven major motion picture firms that charged him with violating the Digital Millennium Copyright Act (DMCA) anti-circumvention rules. The Second Circuit Court of Appeals rejected Corley's First Amendment defense and expressly took issue with the Court of Appeal's First Amendment analysis in *Bunner*.

The Second Circuit decided that the functionality of computer program code limited the extent of First Amendment protection courts should accord to code. Corley posted DeCSS in object code form. In that form, DeCSS can fairly be described as a technology primarily designed to bypass a technical measure (CSS) that copyright owners were using to control access to their works (that is, DVD movies), which is what the DMCA anti-circumvention rules prohibit from being distributed. Although the Second Circuit enjoined Corley from posting either source or object code forms of DeCSS, it did not discuss the source vs. object code distinction, and its rationale for the broad injunction is more persuasive as to object code than as to source code.

From the standpoint of computer technologists, it may seem strange, or even perverse, for courts to consider making a distinction between source and object code. In most respects, these forms of programs are equivalent, and there is, of course, no firm way of distinguishing between them, given it is possible for source code to be directly executed and that some humans can read object code. From the standpoint of First Amendment law, however, it matters whether a person who posts code on the Internet is trying to communicate ideas and information in the program with others in his field or community, or whether the code is being disseminated to enable execution of its functionality. If some defendants in *Bunner* posted DeCSS as part of a protest against the motion picture industry's aggressive assertions of intellectual property rights or in order to educate people about how CSS works, courts might view these postings differently than postings for purposes of encouraging people to use DeCSS to infringe copyrights in DVD movies.

From a First Amendment standpoint, it may make a difference whether someone has posted source or object code, as well as whether he or she posted the program in order to communicate with others about its contents or for other purposes. It is, of course, possible for object code to be disseminated for expressive purposes (for example, as a proof of an algorithmic concept), but object code may more commonly be distributed for non-expressive purposes. But expressiveness and communicative intent are key determinants in First Amendment cases. Ironically, lawyers for DVD CCA and for Bunner are both disinclined to distinguish between source and object code. DVD CCA wants an injunction against both forms of DeCSS, and Bunner's lawyers want the First Amendment to protect object as well as source code.

The Right Outcome in *Bunner*

Trade secret law has internal limiting principles that generally suffice to avert conflicts between trade secrets and the First Amendment. Trade secrecy is inherently "leaky" because secrets are susceptible to reverse engineering, independent discovery, or accidental disclosure, all of

which trade secrecy law considers as fair means of acquiring secrets. For example, in *Chicago Lock v. Fanberg*, a court refused to enjoin publication of a compilation of key code information that Chicago Lock considered to be its trade secrets because its authors, the Fanbergs, had acquired the key code information by reverse engineering Chicago locks for their customers and from fellow reverse-engineering locksmiths. Publishing this book was lawful as a matter of trade secret law because reverse engineering is a lawful means of acquiring trade secrets. There was no need to invoke the First Amendment because limiting doctrines of trade secrecy law resolved the dispute.

Similarly, the *Washington Post* was able to persuade a court to dismiss a trade secret misappropriation claim brought by the Religious Technology Center based on the *Post*'s publication of excerpts of Scientology texts in its newspaper, even though the *Post* knew that RTC claimed proprietary rights in these texts. Documents embodying RTC's secrets had been posted on the Internet for 10 days as well as available in unsealed court records in California. Because of this, the judge dismissed the claim, saying that information in the documents was no longer secret. Again, it was unnecessary to invoke the First Amendment because limiting doctrines of trade secrecy law protected the *Post*'s publication of this information.

The same limiting principles should have been applied in *Bunner*, making resort to the First Amendment unnecessary. Bunner republished information obtained from reverse engineering of a mass marketed product by a person remote in time and place from him. In addition, many people had published this information on the Internet before he did, and as a consequence, the secrets leaked out.

If the California Supreme Court decides Bunner violated that state's trade secrecy law, the First Amendment defense should be taken seriously. Unlike the usual defendant in a trade secret case, Bunner did not have a contractual or confidential relationship with DVD CCA, and he engaged in no unlawful conduct in obtaining access to DeCSS. Hence, the usual rationale for enjoining disclosure of trade secrets does not apply. Bunner published source, not object, code and he did so for a communicative purpose. While the contents of DeCSS are obviously of far less public importance than the contents of the Pentagon Papers, the First Amendment protects many communications of similar or lesser importance. On balance, Bunner does have a solid First Amendment defense. Let's hope the California Supreme Court recognizes it. C

Pamela Samuelson (pam@sims.berkeley.edu) is a Chancellor's Professor of Law and Information Management at UC Berkeley.