*November 1, 2005*

Intellectual Property and Some Alternatives

- *DVD Copy Control Assoc. v. Bunner*, 116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185, (Cal. Ct. App. 2004)
- *eBay, Inc. v. Bidder's Edge, Inc.* 100 F. Supp. 2d 1058 (ND Cal. 2000)
- *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342; 71 P.3d 296; 1 Cal. Rptr. 3d 32 (Cal. 2003)

Additional reading

- Pamela Samuelson and Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L.J. 1575 (2002), <http://socrates.berkeley.edu/~scotch/re.pdf>
- Dan L. Burk, *The Trouble With Trespass*, 3 J. SMALL & EMERGING BUS. L. 1 (1998) <http://www.isc.umn.edu/research/papers/trespass-ed2.pdf>
- I. Trotter Hardy, *The Ancient Doctrine of Trespass to Websites*, 1996 J. Online L. art. 7 <http://www.wm.edu/law/publications/jol/95_96/hardy.html>

Online as off, there are many ways to skin a cat. Here, we look at some additional claims for protection of information and computer systems: trade secret and trespass to chattels.

The Uniform Trade Secrets Act, adopted as the basis of trade secret law in 41 states, provides for injunctive relief against misappropriation of trade secrets:

(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;

(2) "Misappropriation" means:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

(3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.

(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Does the Internet change the underlying rules of trade secret protection? Does Internet publication pose new challenges for trade secret law's rationales or its practical application?

The California courts in *DVD CCA v. Bunner* faced these questions, as well as examining the interactions between trade secret law and the First Amendment. The *Bunner* case involves the same DeCSS code the Second Circuit found to be an unlawful circumvention technology in *Universal v. Corley*. In *Bunner*, however, the DVD Copy Control Association, the licensing organization for the CSS code, sued a number of DeCSS posters in state court, alleging violations of their trade secrets. The Court of Appeal here heard the case after the California Supreme Court ruled that the First Amendment would not bar a trade secret injunction. At the end of both the *Bunner* and *Corley* lawsuits, is it lawful to post the DeCSS code?

Browse the EFF FAQ on *O'Grady, et al. v. Apple Computer, Inc.*, <http://www.eff.org/Censorship/Apple_v_Does/faq.php>, another case involving trade secret claims. There, Apple sued unidentified Doe defendants who allegedly gave confidential Apple information to online news sites Apple Insider and PowerPage. Then, Apple issued discovery subpoenas to the news sites' service providers, trying to obtain the identities of those it claimed had misappropriated Apple's trade secrets. The news sites moved for protective orders to protect their anonymous sources, arguing that Apple had not exhausted its internal investigation before seeking to breach journalistic confidentiality.

Trespass to chattels is an old cause of action seemingly reinvented for the online era. The tort claim for "interferences with possession of personal property" has been invoked against characters ranging from robotic website scrapers to alleged spammers. How do the elements of this hoary cause of action match the complaints of modern-day server operators in *eBay v. Bidder's Edge* and *Intel v. Hamidi*? Think about the values served by open access to information published on publicly accessible websites. Should aggregators like Expedia need permission from every airline to publish competitive airfare listings? Consider how useful it is that you don't need advance permission to send a long-lost friend an email when you find her address. Think also of the problems Internet users and server operators describe when they are flooded with too many web requests or email communications.

What law and policy arguments support tort claims against unwanted communications? What arguments oppose them?

States have considerable latitude to create rights different those of federal law, but they cannot *interfere with* federal law. Federal law not only creates the core intellectual property rights of patent and copyright, but it also crafts important public rights where those exclusive rights end. Thus in *Feist Pubs, Inc., v. Rural Telephone Serv. Co., Inc.*, 499 US 340, 349-50 (1991), the Supreme Court turned dismissed the claims of a phone book compiler to protection for the "sweat of the brow" labor of compiling a directory:

> It may seem unfair that much of the fruit of the compiler's labor may be used by others without compensation. As Justice Brennan has correctly observed, however, this is not "some unforeseen byproduct of a statutory scheme." *Harper & Row*, 471 U.S., at 589 (dissenting opinion). It is, rather, "the essence of copyright," *ibid*., and a constitutional requirement. The primary objective of copyright is not to reward the labor of authors, but "to promote the Progress of Science and useful Arts." Art. I, § 8, cl. 8. To this end, copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work. *Harper & Row*, *supra*, at 556-557. This principle, known as the idea-expression or fact-expression dichotomy, applies to all works of authorship. As applied to a factual compilation, assuming the absence of original written expression, only the compiler's selection and arrangement may be protected; the raw facts may be copied at will. This result is neither unfair nor unfortunate. It is the means by which copyright advances the progress of science and art.

Under the Constitution's Supremacy Clause, states may not create intellectual property-like rights inconsistent with federal law.

> States may not offer patent-like protection to intellectual creations which would otherwise remain unprotected as a matter of federal law. Both the novelty and the nonobviousness requirements of federal patent law are grounded in the notion that concepts within the public grasp, or those so obvious that they readily could be, are the tools of creation available to all. They provide the baseline of free competition upon which the patent system's incentive to creative effort depends. A state law that substantially interferes with the enjoyment of an unpatented utilitarian or design conception which has been freely disclosed by its author to the public at large impermissibly contravenes the ultimate goal of public disclosure and use which is the centerpiece of federal patent policy.

*Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 US 141, 157 (1989). The Court also remarked there on why trade secret law is not preempted:

> In *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974), the court held that state protection we held that state protection of trade secrets did not operate to frustrate

> the achievement of the congressional objectives served by the patent laws. Despite the fact that state law protection was available for ideas which clearly fell within the subject matter of patent, the Court concluded that the nature and degree of state protection did not conflict with the federal policies of encouragement of patentable invention and the prompt disclosure of such innovations. Several factors were critical to this conclusion. First, because the public awareness of a trade secret is by definition limited, the Court noted that "the policy that matter once in the public domain must remain in the public domain is not incompatible with the existence of trade secret protection." Second, the *Kewanee* Court emphasized that "[t]rade secret law provides far weaker protection in many respects than the patent law." This point was central to the Court's conclusion that trade secret protection did not conflict with either the encouragement or disclosure policies of the federal patent law. The public at large remained free to discover and exploit the trade secret through reverse engineering of products in the public domain or by independent creation. Thus, the possibility that trade secret protection would divert inventors from the creative effort necessary to satisfy the rigorous demands of patent protection was remote indeed. … We have since reaffirmed the pragmatic approach which *Kewanee* takes to the pre-emption of state laws dealing with the protection of intellectual property. At the same time, we have consistently reiterated the teaching of *Sears* and *Compco* that ideas once placed before the public without the protection of a valid patent are subject to appropriation without significant restraint.

*Id.* at 155-56.

***DVD Copy Control Assoc. v. Bunner***
116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185, (Cal. Ct. App. 2004)

**PREMO, Acting P. J.**--Plaintiff DVD Copy Control Association, Inc. (DVD CCA) sued defendant Andrew Bunner (Bunner) and others under California's Uniform Trade Secrets Act (UTSA) (Civ. Code, § 3426 et seq.), seeking an injunction to prevent defendants from using or publishing "DeCSS," a computer program allegedly containing DVD CCA's trade secrets.

The trial court granted DVD CCA's request for a preliminary injunction and entered an order prohibiting defendants from posting, disclosing, or distributing DeCSS or related proprietary material. Bunner appealed. His primary argument on appeal was that the injunction infringed his free speech rights under the state and federal constitutions. This court concluded that the injunction was an unconstitutional prior restraint and reversed.

The California Supreme Court granted review and held that the preliminary injunction did not violate the free speech clauses of the United States and California Constitutions "assuming the trial court properly issued the injunction under California's trade secret law." (*DVD Copy Control Assn., Inc. v. Bunner* (2003) 31 Cal.4th 864, 889 [4 Cal. Rptr. 3d 69, 75 P.3d 1] (*DVD*).) The Supreme Court remanded the matter to this court to determine whether the evidence in the record supports the factual findings necessary to establish that the preliminary injunction was warranted under the UTSA. (*Id.* at p. 890.) We now conclude that it was not.

## I. Factual and Procedural Background

### *A. Introduction*

Digital versatile disks (DVD's) are five-inch disks used to store large amounts of data in digital form. A single DVD may contain a full-length motion picture. Unlike motion pictures on videocassettes, motion pictures contained on DVD's may be copied without perceptible loss of video or audio quality. This aspect of the DVD format makes it particularly susceptible to piracy. For this reason, motion pictures stored on DVDs have been protected from unauthorized use by a content scrambling system referred to as CSS. Simply put, CSS scrambles the data on the disk and then unscrambles it when the disk is played on a compliant DVD player or computer. CSS does not allow the content on the DVD to be copied. (*DVD, supra*, 31 Cal.4th at p. 871.)

For obvious reasons, the motion picture industry desired to keep the CSS technology a secret. But to make DVD players and computer DVD drives that can unscramble and play a CSS-protected DVD, the manufacturers had to have the CSS "master keys" and an understanding of how the technology works. In an attempt to keep CSS from becoming generally known, the industries agreed upon a restrictive licensing scheme and formed DVD CCA to be the sole licensing entity for CSS. Under the CSS licensing scheme, each licensee receives a different master key to incorporate into its equipment and sufficient technical know how to permit the manufacture of a DVD-compliant device. All licensees

must agree to maintain the confidentiality of CSS.

In spite of these efforts to maintain the secrecy of CSS, DeCSS appeared on the Internet sometime in October 1999 and rapidly spread to other Web sites, including those of the defendants. According to DVD CCA, DeCSS incorporates trade secret information that was obtained by reverse engineering [FN] CSS in breach of a license agreement. DVD CCA alleges that DeCSS allows users to illegally pirate the copyrighted motion pictures contained on DVDs, "activity which is fatal to the DVD video format and the hundreds of computer and consumer electronics companies whose businesses rely on the viability of this digital format."

- - - - - - - - - - - - - - Footnotes - - - - - - - - - - - - - -
Reverse engineering is the process by which one starts with a known product and works backward to determine how it was developed or manufactured. (*Kewanee Oil Co. v. Bicron Corp.* (1974) 416 U.S. 470, 476 [40 L. Ed. 2d 315, 94 S. Ct. 1879].) The concept is not limited to computer software but applies to any product or process.
- - - - - - - - - - - - - End Footnotes- - - - - - - - - - - - -

DVD CCA filed the instant complaint for injunctive relief on December 27, 1999, alleging that Bunner and the other defendants had misappropriated trade secrets by posting DeCSS or links to DeCSS on their Web sites, knowing that DeCSS had been created by improper means. The requested injunctive relief sought to prevent defendants from using DeCSS, from disclosing DeCSS or other proprietary CSS technology on their Web sites or elsewhere, and from linking their Web sites to other Web sites that disclosed DeCSS or other CSS technology.

After first denying DVD CCA's request for a temporary restraining order, the trial court issued a preliminary injunction on January 21, 2000, enjoining defendants from "[p]osting or otherwise disclosing or distributing, on their websites or elsewhere, the DeCSS program, the master keys or algorithms of [CSS], or any other information derived from this proprietary information." The injunction does not prohibit linking to other Web sites and it does not expressly prohibit defendants from "using" DeCSS.

*B. The Factual Record*

The evidence before the trial court was submitted in the form of written declarations. John Hoy, president of DVD CCA explained that DeCSS first appeared on the Internet on October 6, 1999. That first posting was in machine-readable form referred to as object code. The DeCSS source code was posted about three weeks later, on or around October 25, 1999. Hoy declared that both postings contain CSS technology and the master key that had been assigned to DVD CCA's licensee, Xing Technology Corporation (Xing), a manufacturer of computer DVD drives. The intended inference is that DeCSS was created, at least in part, by reverse engineering the Xing software. Since Xing licensed its software pursuant to an agreement that prohibits reverse engineering, Hoy concludes that the CSS technology contained in DeCSS was "obtained in violation of the specific provision in the Xing end-user license 'click wrap' agreement which prohibits reverse

engineering." Hoy stated on information and belief that Jon Johansen, a resident of Norway, was the author of the program.

Well before DeCSS was released on the Internet, a number of people had become interested in unraveling the CSS security system. Users of the Linux computer operating system had organized a forum dedicated to finding a way to override CSS. Apparently DVD CCA had not licensed CSS to anyone making DVD drives for the Linux system, so that computers using Linux were incapable of playing DVD's. CSS was widely analyzed and discussed in the academic cryptography community. Another exchange of information took place on www.slashdot.org (Slashdot), a news Web site popular with computer programmers. As early as July 1999 comments on Slashdot revealed a worldwide interest in cracking CSS. The gist of these communications is contained in the following excerpts of a discussion that took place on July 15, 1999:

> "Yes, it is true, we have now all needed parts for software decoding of DVDs, but any software doing so will be illegal and/or non-free. ... The information about CSS was obtained by reverse engineering some DVD software decoder."
>
> "This code was released before anyone checked into the legal end of things. ... Best idea now is to download the code. Get it spread around as widely as possible. It may not be able to be used legally when all is said and done, but at least it will be out there for others to work with."
>
> "Well, it might not be the most ethical thing on earth, but if the appropriate algorithms were to be found just lying on the web, once the coders have seen them, they don't have a 'forget' button for their brains. ..."

Bunner first became aware of DeCSS on or about October 26, 1999, as a result of reading and participating in discussions on Slashdot. Bunner explained that he is a part-time user of Linux and supports its acceptance as a viable alternative to established computer operating systems such as Microsoft Windows. Bunner thought DeCSS would be useful to other Linux users. He claimed that at the time he posted the information on his Web site he had no information to suggest that the program contained any trade secrets or that it involved the misappropriation of trade secrets. There is no evidence as to the date Bunner first posted the program on his Web site.

Counsel representing the motion picture industry had become aware of the DeCSS posting on October 25, 1999. Beginning November 4, 1999, counsel sent letters to Web site operators and Internet service providers hosting Web pages that contained DeCSS or links to DeCSS and demanded the information be taken down. Sixty-six such letters were sent between November 4 and November 23, 1999. None of the letters listed in counsel's declaration were addressed to Bunner or to his Web site address. About 25 of the 66 sites were taken down. DeCSS was also removed from Johansen's Web site on or around November 8, 1999, but a link to DeCSS reappeared on the same site on or around December 11, 1999.

Meanwhile, the news that the CSS encryption system had been penetrated made headlines in Internet news magazines. Wired News ran several articles in the first days of November 1999 announcing the development of DeCSS. An article on November 4, 1999, said: "It shouldn't be surprising that an awful lot of people are upset at this week's Wired News reports about a utility to remove DVD security. But it's out there and people are using it." An article on eMedia around the same time explained that DeCSS was "available for free download from several sites on the World Wide Web."

DVD CCA filed suit on December 27, 1999, naming as defendants the operators of every infringing Web site it could identify. A hearing for a temporary restraining order was to be held the following day. In support of that application, DVD CCA informed the court that since October 25, 1999, DeCSS had been displayed on or linked to at least 118 Web pages in 11 states and 11 countries throughout the world and that approximately 93 Web pages continued to publish infringing information.

The lawsuit outraged many people in the computer programming community. A campaign of civil disobedience arose by which its proponents tried to spread the DeCSS code as widely as possible before trial. Some of the defendants simply refused to take their postings down. Some people appeared at the courthouse on December 28, 1999, to pass out diskettes and written fliers that supposedly contained the DeCSS code. They made and distributed T-shirts with parts of the code printed on the back. There were even contests encouraging people to submit ideas about how to disseminate the information as widely as possible. …

**II. Discussion**

*B. The Existence of a Trade Secret*

In order to obtain an injunction prohibiting disclosure of an alleged trade secret, the plaintiff's first hurdle is to show that the information it seeks to protect is indeed a trade secret. The UTSA defines a trade secret as "information ... that: (1) Derives independent economic value, actual or potential, from not being generally known ... ; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." In short, the test for a trade secret is whether the matter sought to be protected is information (1) that is valuable because it is unknown to others and (2) that the owner has attempted to keep secret. The first element is the crucial one here: in order to qualify as a trade secret, the information "must be secret, and must not be of public knowledge or of a general knowledge in the trade or business." (*Kewanee Oil Co. v. Bicron Corp., supra,* 416 U.S. at p. 475.)

The secrecy requirement is generally treated as a relative concept and requires a fact-intensive analysis. (1 Milgrim on Trade Secrets (2003) § 1.07[2], pp. 1-343, 1-352.) Widespread, anonymous publication of the information over the Internet may destroy its status as a trade secret. (*Religious Technology Center v. Netcom On-Line Com.* (N.D.Cal. 1995) 923 F. Supp. 1231, 1256; see also *Religious Tech. Center v. NetCom On-Line Comm.* (N.D.Cal. 1995) 907 F. Supp. 1361.) The concern is whether the information has

retained its value to the creator in spite of the publication. Publication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value.

In the instant matter, the secrecy element becomes important at two points. First, if the allegedly proprietary information contained in DeCSS was already public knowledge when Bunner posted the program to his Web site, Bunner could not be liable for misappropriation by republishing it because he would not have been disclosing a trade secret. Second, even if the information was not generally known when Bunner posted it, if it had become public knowledge by the time the trial court granted the preliminary injunction, the injunction (which only prohibits *disclosure*) would have been improper because DVD CCA could not have demonstrated interim harm.

1. The Likelihood of Prevailing on the Merits

The trial court did not make an express finding that the proprietary information contained in DeCSS was not generally known at the time Bunner posted it. Indeed, there is no evidence to support such a finding. Bunner first became aware of DeCSS on or around October 26, 1999. But there is no evidence as to when he actually posted it. Indeed, neither Bunner's name nor his Web site address appears among the 66 cease and desist letters counsel sent in November. We do know, however, that by the first week in November Internet news magazines were publicizing the creation of DeCSS and informing readers that the program was available to be downloaded for free on the Internet. As early as July 1999 people in the computer programming community were openly discussing the fact that the CSS code had been reverse engineered and were brainstorming ways to be able to use it legally. That means that when DeCSS appeared in October 1999 there was a worldwide audience ready and waiting to download and repost it.

DVD CCA urges us, in effect, to ignore the fact that the allegedly proprietary information may have been distributed to a worldwide audience of millions prior to Bunner's first posting. According to DVD CCA, so long as Bunner knew or should have known that the information he was republishing was obtained by improper means, he cannot rely upon the general availability of the information to the rest of the world to avoid application of the injunction to him. In support of this position, DVD CCA contends that the denial of an injunction would offend the public policies underlying trade secret law, which are to enforce a standard of commercial ethics, to encourage research and invention, and to protect the owner's moral entitlement to the fruits of his or her labors. DVD CCA points out that these policies are advanced by making sure that those who misappropriate trade secrets do not avoid "judicial sanction" by making the secret widely available.

The first problem with this argument is that by denying a preliminary injunction the court does not per se protect a wrongdoer from judicial sanction, which in most cases would come following trial on the merits.

Second, the evidence in this case is very sparse with respect to whether the offending program was actually created by improper means. Reverse engineering alone is not improper means. Here the creator is believed to be a Norwegian resident who probably had to breach a Xing license in order to access the information he needed. We have only very thin circumstantial evidence of when, where, or how this actually happened or whether an enforceable contract prohibiting reverse engineering was ever formed.

Finally, assuming the information was originally acquired by improper means, it does not necessarily follow that once the information became *publicly* available that everyone else would be liable under the trade secret laws for republishing it simply because they knew about its unethical origins. In a case that receives widespread publicity, just about anyone who becomes aware of the contested information would also know that it was allegedly created by improper means. Under DVD CCA's construction of the law, in such a case the general public could theoretically be liable for misappropriation simply by disclosing it to someone else. This is not what trade secret law is designed to do.

It is important to point out that we do not assume that the alleged trade secrets contained in DeCSS became part of the public domain simply by having been published on the Internet. Rather, the evidence demonstrates that in this case, the initial publication was quickly and widely republished to an eager audience so that DeCSS and the trade secrets it contained rapidly became available to anyone interested in obtaining them. Further, the record contains no evidence as to when in the course of the initial distribution of the offending program Bunner posted it. Thus, DVD CCA has not shown a likelihood that it will prevail on the merits of its claim of misappropriation against Bunner.

2. Interim Harm

The element of secrecy also bears upon the question of interim harm. The Restatement explains the relationship this way: "Injunctive relief is often appropriate in trade secret cases to insure against additional harm from further unauthorized use of the trade secret and to deprive the defendant of additional benefits from the appropriation. If the information has not become generally known, an injunction may also be appropriate to preserve the plaintiff's rights in the trade secret by preventing a public disclosure. If the trade secret has already entered the public domain, an injunction may be appropriate to remedy any head start or other unfair advantage acquired by the defendant as a result of the appropriation. However, if the defendant retains no unfair advantage from the appropriation, an injunction against the use of information that is no longer secret can be justified only on a rationale of punishment and deterrence. Because of the public interest in promoting competition, such punitive injunctions are ordinarily inappropriate in trade secret actions." (Rest.3d Unfair Competition, § 44, com. c, p. 500.)

As the trial court clearly explained, the preliminary injunction prohibiting disclosure was intended to protect the trade secret. Therefore, even if Bunner was liable for misappropriation, if the information had since become generally known, a preliminary injunction prohibiting disclosure would have done nothing to protect the secret because

the secret would have ceased to exist. Further, assuming that an injunction against the *use* of information could be justified, we can conceive of no possible justification for an injunction against the *disclosure* of information if the information were already public knowledge. …

We concur with the concerns expressed by Judge Whyte in his opinion in *Religious Technology Center v. Netcom On-Line Com., supra,* 923 F. Supp. at page 1256: "The court is troubled by the notion that any Internet user, ... can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. Nonetheless, one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers, [citation], can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation."

There is little question that such behavior is unethical and that it probably violates other laws. But that which is in the public domain cannot be removed by action of the states under the guise of trade secret protection. (*Kewanee Oil Co. v. Bicron Corp., supra,* 416 U.S. at p. 481.)

The evidence in the present case is undisputed that by the time this lawsuit was filed hundreds of Web sites had posted the program, enabling untold numbers of persons to download it and to use it. The only inference that can be drawn from this evidence is that by December 27, 1999, when DVD CCA first took legal action to stop publication of DeCSS, the technology had become available to those persons most interested in obtaining it. DVD CCA presented no evidence that the disclosure it sought to prohibit would cause more or different harm than that it claims it would have suffered by the general disclosure of the program. Accordingly, the record does not support the trial court's finding that the balance of harms favored DVD CCA.

**III. Conclusion**

We conclude that evidence in the limited record before us does not justify the issuance of an injunction under the UTSA. DVD CCA presented no evidence as to when Bunner first posted DeCSS and no evidence to support the inference that the CSS technology was still a secret when he did so. Further, there is a great deal of evidence to show that by the time DVD CCA sought the preliminary injunction prohibiting disclosure of the DeCSS program, DeCSS had been so widely distributed that the CSS technology may have lost its trade secret status. There is no evidence at all to the contrary. Thus, DVD CCA has not shown a likelihood of success on the merits; nor has it demonstrated that it would suffer further harm if the preliminary injunction did not issue. The preliminary injunction, therefore, burdens more speech than necessary to protect DVD CCA's property interest and was an unlawful prior restraint upon Bunner's right to free speech. (*DVD, supra,* 31 Cal.4th at p. 881; and see *Madsen v. Women's Health Center, Inc.* (1994) 512 U.S. 753, 765 [129 L. Ed. 2d 593, 114 S. Ct. 2516].) It follows that issuance of the injunction was an abuse of the trial court's discretion.

It is important to stress that our conclusion is based upon the appellate record filed in this court. It is *not* a final adjudication on the merits. The ultimate determination of trade secret status and misappropriation would be subject to proof to be presented at trial. (*Whyte v. Schlage Lock Co., supra*, 101 Cal.App.4th at p. 1453.)

**IV. Disposition**

The order granting a preliminary injunction is reversed. Defendant Andrew Bunner shall recover his appellate costs.

***eBay, Inc. v. Bidder's Edge, Inc.***
100 F. Supp. 2d 1058 (N.D. Cal. 2000)

RONALD M. WHYTE

… eBay is an Internet-based, person-to-person trading site. eBay offers sellers the ability to list items for sale and prospective buyers the ability to search those listings and bid on items. The seller can set the terms and conditions of the auction. The item is sold to the highest bidder. The transaction is consummated directly between the buyer and seller without eBay's involvement. A potential purchaser looking for a particular item can access the eBay site and perform a key word search for relevant auctions and bidding status. eBay has also created category listings which identify items in over 2500 categories, such as antiques, computers, and dolls. Users may browse these category listing pages to identify items of interest.

Users of the eBay site must register and agree to the eBay User Agreement. Users agree to the seven page User Agreement by clicking on an "I Accept" button located at the end of the User Agreement. The current version of the User Agreement prohibits the use of "any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior expressed written permission." It is not clear that the version of the User Agreement in effect at the time BE began searching the eBay site prohibited such activity, or that BE ever agreed to comply with the User Agreement.

…A software robot is a computer program which operates across the Internet to perform searching, copying and retrieving functions on the web sites of others. A software robot is capable of executing thousands of instructions per minute, far in excess of what a human can accomplish. Robots consume the processing and storage resources of a system, making that portion of the system's capacity unavailable to the system owner or other users. Consumption of sufficient system resources will slow the processing of the overall system and can overload the system such that it will malfunction or "crash." A severe malfunction can cause a loss of data and an interruption in services.

The eBay site employs "robot exclusion headers." A robot exclusion header is a message, sent to computers programmed to detect and respond to such headers, that eBay does not permit unauthorized robotic activity. Programmers who wish to comply with the Robot Exclusion Standard design their robots to read a particular data file, "robots.txt," and to comply with the control directives it contains…

BE is a company with 22 employees that was founded in 1997. … BE does not host auctions. BE is an auction aggregation site designed to offer on-line auction buyers the ability to search for items across numerous on-line auctions without having to search each host site individually. As of March 2000, the BE web site contained information on more that five million items being auctioned on more than one hundred auction sites. BE also provides its users with additional auction-related services and information. (Id. P 2.)

The information available on the BE site is contained in a database of information that BE compiles through access to various auction sites such as eBay. When a user enters a search for a particular item at BE, BE searches its database and generates a list of every item in the database responsive to the search, organized by auction closing date and time. Rather than going to each host auction site one at a time, a user who goes to BE may conduct a single search to obtain information about that item on every auction site tracked by BE. It is important to include information regarding eBay auctions on the BE site because eBay is by far the biggest consumer to consumer on-line auction site. …

In early 1998, eBay gave BE permission to include information regarding eBay-hosted auctions for Beanie Babies and Furbies in the BE database…. On April 24, 1999, eBay verbally approved BE crawling the eBay web site for a period of 90 days. The parties contemplated that during this period they would reach a formal licensing agreement. They were unable to do so….

In late August or early September 1999, eBay requested by telephone that BE cease posting eBay auction listings on its site. BE agreed to do so. In October 1999, BE learned that other auction aggregations sites were including information regarding eBay auctions. On November 2, 1999, BE issued a press release indicating that it had resumed including eBay auction listings on its site. On November 9, 1999, eBay sent BE a letter reasserting that BE's activities were unauthorized, insisting that BE cease accessing the eBay site, alleging that BE's activities constituted a civil trespass and offering to license BE's activities. eBay and BE were again unable to agree on licensing terms. As a result, eBay attempted to block BE from accessing the eBay site; by the end of November, 1999, eBay had blocked a total of 169 IP addresses it believed BE was using to query eBay's system. BE elected to continue crawling eBay's site by using proxy servers to evade eBay's IP blocks.

Approximately 69% of the auction items contained in the BE database are from auctions hosted on eBay. BE estimates that it would lose one-third of its users if it ceased to cover the eBay auctions.

The parties agree that BE accessed the eBay site approximate 100,000 times a day. eBay alleges that BE activity constituted up to 1.53% of the number of requests received by eBay, and up to 1.10% of the total data transferred by eBay during certain periods in October and November of 1999. … eBay has not alleged any specific incremental damages due to BE activity. …

eBay now moves for preliminary injunctive relief preventing BE from accessing the eBay computer system based on nine causes of action: trespass, false advertising, federal and state trademark dilution, computer fraud and abuse, unfair competition, misappropriation, interference with prospective economic advantage and unjust enrichment. However, eBay does not move, either independently or alternatively, for injunctive relief that is limited to restricting how BE can use data taken from the eBay site.

**II. LEGAL STANDARD**

To obtain preliminary injunctive relief, a movant must demonstrate "either a likelihood of success on the merits and the possibility of irreparable injury, or that serious questions going to the merits were raised and the balance of hardships tips sharply in its favor." …

**III. ANALYSIS**

**A. Balance of Harm**

eBay asserts that it will suffer four types of irreparable harm if preliminary injunctive relief is not granted: (1) lost capacity of its computer systems resulting from to BE's use of automated agents; (2) damage to eBay's reputation and goodwill caused by BE's misleading postings; (3) dilution of the eBay mark; and (4) BE's unjust enrichment. The harm eBay alleges it will suffer can be divided into two categories. The first type of harm is harm that eBay alleges it will suffer as a result of BE's automated query programs burdening eBay's computer system ("system harm"). The second type of harm is harm that eBay alleges it will suffer as a result of BE's misrepresentations regarding the information that BE obtains through the use of these automated query programs ("reputational harm")….

eBay's allegations of harm are based, in part, on the argument that BE's activities should be thought of as equivalent to sending in an army of 100,000 robots a day to check the prices in a competitor's store. This analogy, while graphic, appears inappropriate. Although an admittedly formalistic distinction, unauthorized robot intruders into a "brick and mortar" store would be committing a trespass to real property. There does not appear to be any doubt that the appropriate remedy for an ongoing trespass to business premises would be a preliminary injunction. More importantly, for the analogy to be accurate, the robots would have to make up less than two out of every one-hundred customers in the store, the robots would not interfere with the customers' shopping experience, nor would the robots even be seen by the customers. Under such circumstances, there is a legitimate claim that the robots would not pose any threat of irreparable harm. However, eBay's right to injunctive relief is also based upon a much stronger argument.

If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses. BE does not appear to seriously contest that reduced system performance, system unavailability or data loss would inflict irreparable harm on eBay consisting of lost profits and lost customer goodwill. Harm resulting from lost profits and lost customer goodwill is irreparable because it is neither easily calculable, nor easily compensable and is therefore an appropriate basis for injunctive relief. Where, as here, the denial of preliminary injunctive relief would encourage an increase in the complained of activity, and such an increase would present a strong likelihood of irreparable harm, the plaintiff has at least established a possibility of irreparable harm

In the patent infringement context, the Federal Circuit has held that a preliminary

injunction may be based, at least in part, on the harm that would occur if a preliminary injunction were denied and infringers were thereby encouraged to infringe a patent during the course of the litigation. In the absence of preliminary injunctive relief, "infringers could become compulsory licensees for as long as the litigation lasts."… Similarly fundamental to the concept of ownership of personal property is the right to exclude others. If preliminary injunctive relief against an ongoing trespass to chattels were unavailable, a trespasser could take a compulsory license to use another's personal property for as long as the trespasser could perpetuate the litigation.

BE correctly observes that there is a dearth of authority supporting a preliminary injunction based on an ongoing to trespass to chattels. In contrast, it is black letter law in California that an injunction is an appropriate remedy for a continuing trespass to real property. If eBay were a brick and mortar auction house with limited seating capacity, eBay would appear to be entitled to reserve those seats for potential bidders, to refuse entrance to individuals (or robots) with no intention of bidding on any of the items, and to seek preliminary injunctive relief against non-customer trespassers eBay was physically unable to exclude. The analytic difficulty is that a wrongdoer can commit an ongoing trespass of a computer system that is more akin to the traditional notion of a trespass to real property, than the traditional notion of a trespass to chattels, because even though it is ongoing, it will probably never amount to a conversion. The court concludes that under the circumstances present here, BE's ongoing violation of eBay's fundamental property right to exclude others from its computer system potentially causes sufficient irreparable harm to support a preliminary injunction.

BE argues that even if eBay is entitled to a presumption of irreparable harm, the presumption may be rebutted. … If eBay's irreparable harm claim were premised solely on the potential harm caused by BE's current crawling activities, evidence that eBay had licensed others to crawl the eBay site would suggest that BE's activity would not result in irreparable harm to eBay. However, the gravamen of the alleged irreparable harm is that if eBay is allowed to continue to crawl the eBay site, it may encourage frequent and unregulated crawling to the point that eBay's system will be irreparably harmed. There is no evidence that eBay has indiscriminately licensed all comers. Rather, it appears that eBay has carefully chosen to permit crawling by a limited number of aggregation sites that agree to abide by the terms of eBay's licensing agreement. "The existence of such a [limited] license, unlike a general license offered to all comers, does not demonstrate a decision to relinquish all control over the distribution of the product in exchange for a readily computable fee."…

BE argues that even if eBay will be irreparably harmed if a preliminary injunction is not granted, BE will suffer greater irreparable harm if an injunction is granted. According to BE, lack of access to eBay's database will result in a two-thirds decrease in the items listed on BE, and a one-eighth reduction in the value of BE, from $ 80 million to $ 70 million. Although the potential harm to BE does not appear insignificant, BE does not appear to have suffered any irreparable harm during the period it voluntarily ceased crawling the eBay site. Barring BE from automatically querying eBay's site does not prevents BE from maintaining an aggregation site including information from eBay's site.

Any potential economic harm is appropriately addressed through the posting of an adequate bond.

Moreover, it appears that any harm alleged to result from being forced to cease an ongoing trespass may not be legally cognizable. In the copyright infringement context, once a plaintiff has established a strong likelihood of success on the merits, any harm to the defendant that results from the defendant being preliminarily enjoined from continuing to infringe is legally irrelevant. See Triad Sys. Corp. v. Southeastern Exp. Co., 64 F.3d 1330, 1338 (9th Cir. 1995) (defendant "cannot complain of the harm that will befall it when properly forced to desist from its infringing activities.")…. The reasoning in these cases appears to be that a defendant who builds a business model based upon a clear violation of the property rights of the plaintiff cannot defeat a preliminary injunction by claiming the business will be harmed if the defendant is forced to respect those property rights. … Accordingly, the court concludes that eBay has demonstrated at least a possibility of suffering irreparable system harm and that BE has not established a balance of hardships weighing in its favor.

**B. Likelihood of Success**

…I. Trespass

Trespass to chattels "lies where an intentional interference with the possession of personal property has proximately cause injury." Thrifty-Tel v. Bezenek, 46 Cal. App. 4th 1559, 1566 (1996). Trespass to chattels "although seldom employed as a tort theory in California" was recently applied to cover the unauthorized use of long distance telephone lines. Id. Specifically, the court noted "the electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action." Thus, it appears likely that the electronic signals sent by BE to retrieve information from eBay's computer system are also sufficiently tangible to support a trespass cause of action.

In order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff. See Thrifty-Tel, 46 Cal. App. 4th at 1566. Here, eBay has presented evidence sufficient to establish a strong likelihood of proving both prongs and ultimately prevailing on the merits of its trespass claim.

a. BE's Unauthorized Interference

eBay argues that BE's use was unauthorized and intentional. eBay is correct. BE does not dispute that it employed an automated computer program to connect with and search eBay's electronic database. BE admits that, because other auction aggregators were including eBay's auctions in their listing, it continued to "crawl" eBay's web site even after eBay demanded BE terminate such activity.

BE argues that it cannot trespass eBay's web site because the site is publicly accessible. BE's argument is unconvincing. eBay's servers are private property, conditional access to which eBay grants the public. eBay does not generally permit the type of automated access made by BE. In fact, eBay explicitly notifies automated visitors that their access is not permitted. "HN9 In general, California does recognize a trespass claim where the defendant exceeds the scope of the consent." Baugh v. CBS, Inc., 828 F. Supp. 745, 756 (N.D. Cal. 1993).

Even if BE's web crawlers were authorized to make individual queries of eBay's system, BE's web crawlers exceeded the scope of any such consent when they began acting like robots by making repeated queries…. Moreover, eBay repeatedly and explicitly notified BE that its use of eBay's computer system was unauthorized. The entire reason BE directed its queries through proxy servers was to evade eBay's attempts to stop this unauthorized access. The court concludes that BE's activity is sufficiently outside of the scope of the use permitted by eBay that it is unauthorized for the purposes of establishing a trespass.

eBay argues that BE interfered with eBay's possessory interest in its computer system. Although eBay appears unlikely to be able to show a substantial interference at this time, such a showing is not required. Conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel. See Thrifty-Tel, 46 Cal. App. 4th at 1567 (distinguishing the tort from conversion). Although the court admits some uncertainty as to the precise level of possessory interference required to constitute an intermeddling, there does not appear to be any dispute that eBay can show that BE's conduct amounts to use of eBay's computer systems. Accordingly, eBay has made a strong showing that it is likely to prevail on the merits of its assertion that BE's use of eBay's computer system was an unauthorized and intentional interference with eBay's possessory interest.

b. Damage to eBay's Computer System

A trespasser is liable when the trespass diminishes the condition, quality or value of personal property. See Compuserve, Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997). The quality or value of personal property may be "diminished even though it is not physically damaged by defendant's conduct." Id. at 1022. The Restatement offers the following explanation for the harm requirement:

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected

> interest of the possessor is affected ... Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

Restatement (Second) of Torts § 218 cmt. e (1977).

eBay is likely to be able to demonstrate that BE's activities have diminished the quality or value of eBay's computer systems. BE's activities consume at least a portion of plaintiff's bandwidth and server capacity. Although there is some dispute as to the percentage of queries on eBay's site for which BE is responsible, BE admits that it sends some 80,000 to 100,000 requests to plaintiff's computer systems per day. Although eBay does not claim that this consumption has led to any physical damage to eBay's computer system, nor does eBay provide any evidence to support the claim that it may have lost revenues or customers based on this use, eBay's claim is that BE's use is appropriating eBay's personal property by using valuable bandwidth and capacity, and necessarily compromising eBay's ability to use that capacity for its own purposes. See CompuServe, 962 F. Supp. at 1022 ("any value [plaintiff] realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base.").

BE argues that its searches represent a negligible load on plaintiff's computer systems, and do not rise to the level of impairment to the condition or value of eBay's computer system required to constitute a trespass. However, it is undisputed that eBay's server and its capacity are personal property, and that BE's searches use a portion of this property. Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property. Accordingly, BE's actions appear to have caused injury to eBay and appear likely to continue to cause injury to eBay. If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value. California law does not require eBay to wait for such a disaster before applying to this court for relief The court concludes that eBay has made a strong showing that it is likely to prevail on the merits of its trespass claim, and that there is at least a possibility that it will suffer irreparable harm if preliminary injunctive relief is not granted. eBay is therefore entitled to preliminary injunctive relief.

2. Copyright Preemption

BE argues that the trespass claim, along with eBay's other state law causes of action, "is similar to eBay's originally filed but now dismissed copyright infringement claim, and each is based on eBay's assertion that Bidder's Edge copies eBay's auction listings, a right within federal copyright law." BE is factually incorrect to the extent it argues that the trespass claim arises out of what BE does with the information it gathers by accessing

eBay's computer system, rather than the mere fact that BE accesses and uses that system without authorization.

A state law cause of action is preempted by the Copyright Act if, (1) the rights asserted under state law are "equivalent" to those protected by the Copyright Act, and (2) the work involved falls within the "subject matter" of the Copyright Act as set forth in 17 U.S.C. §§ 102 and 103. Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212 (9th Cir. 1998). "In order not to be equivalent, the right under state law must have an extra element that changes the nature of the action so that it is qualitatively different from a copyright infringement claim." Xerox Corp. v. Apple Computer, Inc., 734 F. Supp. 1542, 1550 (N.D. Cal. 1990). Here, eBay asserts a right not to have BE use its computer systems without authorization. The right to exclude others from using physical personal property is not equivalent to any rights protected by copyright and therefore constitutes an extra element that makes trespass qualitatively different from a copyright infringement claim. But see, Ticketmaster Corp. v. Tickets.com, Inc., 2000 U.S. Dist. LEXIS 4553, No. CV-99-7654 (C.D. Cal. minute order filed Mar. 27, 2000) (dismissing trespass claim based on unauthorized Internet information aggregation as preempted by copyright law).

3. Public Interest

The traditional equitable criteria for determining whether an injunction should issue include whether the public interest favors granting the injunction. American Motorcyclist Ass'n v. Watt, 714 F.2d 962, 965 (9th Cir. 1983). The parties submit a variety of declarations asserting that the Internet will cease to function if, according to eBay, personal and intellectual property rights are not respected, or, according to BE, if information published on the Internet cannot be universally accessed and used. Although the court suspects that the Internet will not only survive, but continue to grow and develop regardless of the outcome of this litigation, the court also recognizes that it is poorly suited to determine what balance between encouraging the exchange of information, and preserving economic incentives to create, will maximize the public good. Particularly on the limited record available at the preliminary injunction stage, the court is unable to determine whether the general public interest factors in favor of or against a preliminary injunction….

**IV. ORDER**

Bidder's Edge, its officers, agents, servants, employees, attorneys and those in active concert or participation with them who receive actual notice of this order by personal service or otherwise, are hereby enjoined pending the trial of this matter, from using any automated query program, robot, web crawler or other similar device, without written authorization, to access eBay's computer systems or networks, for the purpose of copying any part of eBay's auction database. As a condition of the preliminary injunction, eBay is ordered to post a bond in the amount of $ 2,000,000 to secure payment of any damages sustained by defendant if it is later found to have been wrongfully enjoined. This order shall take effect 10 days from the date on which it is filed.

Nothing in this order precludes BE from utilizing information obtained from eBay's site other than by automated query program, robot, web crawler or similar device. The court denies eBay's request for a preliminary injunction barring access to its site based upon BE's alleged trademark infringement, trademark dilution and other claims. This denial is without prejudice to an application for an injunction limiting or conditioning the use of any information obtained on the theory that BE's use violates some protected right of eBay.

***Intel Corp. v. Hamidi*,**
30 Cal. 4th 1342; 71 P.3d 296; 1 Cal. Rptr. 3d 32 (Cal. 2003)

**WERDEGAR, J.**

Intel Corporation (Intel) maintains an electronic mail system, connected to the Internet, through which messages between employees and those outside the company can be sent and received, and permits its employees to make reasonable nonbusiness use of this system. On six occasions over almost two years, Kourosh Kenneth Hamidi, a former Intel employee, sent e-mails criticizing Intel's employment practices to numerous current employees on Intel's electronic mail system. Hamidi breached no computer security barriers in order to communicate with Intel employees. He offered to, and did, remove from his mailing list any recipient who so wished. Hamidi's communications to individual Intel employees caused neither physical damage nor functional disruption to the company's computers, nor did they at any time deprive Intel of the use of its computers. The contents of the messages, however, caused discussion among employees and managers.

On these facts, Intel brought suit, claiming that by communicating with its employees over the company's e-mail system Hamidi committed the tort of trespass to chattels. The trial court granted Intel's motion for summary judgment and enjoined Hamidi from any further mailings. A divided Court of Appeal affirmed. …

After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself. The consequential economic damage Intel claims to have suffered, i.e., loss of productivity caused by employees reading and reacting to Hamidi's messages and company efforts to block the messages, is not an injury to the company's interest in its computers--which worked as intended and were unharmed by the communications--any more than the personal distress caused by reading an unpleasant letter would be an injury to the recipient's mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient's telephone equipment.

Our conclusion does not rest on any special immunity for communications by electronic mail; we do not hold that messages transmitted through the Internet are exempt from the ordinary rules of tort liability. To the contrary, e-mail, like other forms of communication, may in some circumstances cause legally cognizable injury to the recipient or to third parties and may be actionable under various common law or statutory theories. Indeed, on facts somewhat similar to those here, a company or its employees might be able to plead causes of action for interference with prospective economic relations, interference with contract, or intentional infliction of emotional distress. And, of course, as with any other means of publication, third party subjects of e-mail communications may under appropriate facts make claims for defamation, publication of private facts, or other speech-based torts. Intel's claim fails not because e-mail transmitted through the Internet enjoys unique immunity, but because the trespass to chattels tort--unlike the causes of action just mentioned--may not, in California, be proved without evidence of an injury to the plaintiff's personal property or legal interest therein.

Nor does our holding affect the legal remedies of Internet service providers (ISP's) against senders of unsolicited commercial bulk e-mail (UCE), also known as "spam." A series of federal district court decisions, beginning with *CompuServe, Inc. v. Cyber Promotions, Inc.* (S.D.Ohio 1997) 962 F. Supp. 1015, has approved the use of trespass to chattels as a theory of spammers' liability to ISP's, based upon evidence that the vast quantities of mail sent by spammers both overburdened the ISP's own computers and made the entire computer system harder to use for recipients, the ISP's customers. In those cases, discussed in greater detail below, the underlying complaint was that the extraordinary *quantity* of UCE impaired the computer system's functioning. In the present case, the claimed injury is located in the disruption or distraction caused to recipients by the *contents* of the e-mail messages, an injury entirely separate from, and not directly affecting, the possession or value of personal property.…

Hamidi, a former Intel engineer, together with others, formed an organization named Former and Current Employees of Intel (FACE-Intel) to disseminate information and views critical of Intel's employment and personnel policies and practices. FACE-Intel maintained a Web site (which identified Hamidi as Webmaster and as the organization's spokesperson) containing such material. In addition, over a 21-month period Hamidi, on behalf of FACE-Intel, sent six mass e-mails to employee addresses on Intel's electronic mail system. The messages criticized Intel's employment practices, warned employees of the dangers those practices posed to their careers, suggested employees consider moving to other companies, solicited employees' participation in FACE-Intel, and urged employees to inform themselves further by visiting FACE-Intel's Web site. The messages stated that recipients could, by notifying the sender of their wishes, be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.…

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; indeed, internal Intel memoranda show the company's management concluded no security breach had

occurred. Hamidi stated he created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff time was consumed in attempts to block further messages from FACE-Intel. According to the FACE-Intel Web site, moreover, the messages had prompted discussions between "[e]xcited and nervous managers" and the company's human resources department.

DISCUSSION

I. *Current California Tort Law*

Dubbed by Prosser the "little brother of conversion," the tort of trespass to chattels allows recovery for interferences with possession of personal property "not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered." (Prosser & Keeton, Torts (5th ed. 1984) § 14, pp. 85-86.)

Though not amounting to conversion, the defendant's interference must, to be actionable, have caused some injury to the chattel or to the plaintiff's rights in it. Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property *has proximately caused injury*." (*Thrifty-Tel, Inc. v. Bezenek* (1996) 46 Cal.App.4th 1559, 1566 [54 Cal. Rptr. 2d 468], italics added.) In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case, *and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use.*" (*Zaslow v. Kroenert, supra,* 29 Cal.2d at p. 551) …

The Restatement, too, makes clear that some actual injury must have occurred in order for a trespass to chattels to be actionable…. "The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. *Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c).* Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference." (Rest.2d Torts, § 218)

…The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. …[N]o evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. …

[T]he decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning. … [Thus] a series of federal district court decisions held that sending [unsolicited commercial email] through an ISP's equipment may constitute trespass to the ISP's computer system. The lead case, *CompuServe, Inc. v. Cyber Promotions, Inc., supra*, 962 F. Supp. 1015, 1021-1023 (*CompuServe*), was followed by *Hotmail Corp. v. Van$ Money Pie, Inc.* (N.D.Cal., Apr. 16, 1998, No. C 98-20064 JW) 1998 U.S. Dist. LEXIS 10729, page *7, *America Online, Inc. v. IMS* (E.D.Va. 1998) 24 F. Supp. 2d 548, 550-551, and *America Online, Inc. v. LCGM, Inc.* (E.D.Va. 1998) 46 F. Supp. 2d 444, 451-452.

In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In *CompuServe*, the plaintiff ISP's mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed "a tremendous burden" on the ISP's equipment, using "disk space and drain[ing] the processing power," making those resources unavailable to serve subscribers. (*CompuServe, supra*, 962 F. Supp. at p. 1022.) Similarly, in *Hotmail Corp. v. Van$ Money Pie, Inc., supra*, 1998 U.S. Dist. LEXIS 10729 at page *7, the court found the evidence supported a finding that the defendant's mailings "fill[ed] up Hotmail's computer storage space and threaten[ed] to damage Hotmail's ability to service its legitimate customers."…

…These decisions do not persuade us to Intel's position here, for Intel has demonstrated neither any appreciable effect on the operation of its computer system from Hamidi's messages, nor any likelihood that Hamidi's actions will be replicated by others if found not to constitute a trespass.

That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi's activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. The individual advertisers sued in *America Online, Inc. v. IMS, supra*, 24 F. Supp. 2d at page 549, and *America Online, Inc. v. LCGM, Inc., supra*, 46 F. Supp. 2d at page 448, were alleged to have sent more than 60 million messages over 10 months and more than 92 million messages over seven months, respectively. Collectively, UCE has reportedly come to constitute about 45 percent of all

e-mail. (Hansell, *Internet Is Losing Ground in Battle Against Spam*, N.Y. Times (Apr. 22, 2003) p. A1, col. 3.) The functional burden on Intel's computers, or the cost in time to individual recipients, of receiving Hamidi's occasional advocacy messages cannot be compared to the burdens and costs caused ISP's and their customers by the ever-rising deluge of commercial e-mail.

Intel relies on language in the *eBay* decision suggesting that unauthorized use of another's chattel is actionable even without any showing of injury: … But as the *eBay* court went on immediately to find that the defendant's conduct, if widely replicated, *would* likely impair the functioning of the plaintiff's system (*id.* at pp. 1071-1072), we do not read the quoted remarks as expressing the court's complete view of the issue. In isolation, moreover, they would not be a correct statement of California or general American law on this point. While one may have no *right* temporarily to use another's personal property, such use is actionable as a trespass only if it "has proximately caused injury." (*Thrifty-Tel, supra*, 46 Cal.App.4th at p. 1566.) "[I]n the absence of any actual damage the action will not lie." (Prosser & Keeton, Torts, *supra*, § 14, p. 87.) ….

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose--to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. *Proposed Extension of California Tort Law*

We next consider whether California common law should be *extended* to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi's messages, but rather the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an electronic message would be strictly liable to the owner of equipment through which the communication passes--here, Intel--for any consequential injury flowing from the *contents* of the communication. The arguments of amici curiae and academic writers on this topic, discussed below, leave us highly doubtful whether creation of such a rigid property rule would be wise.

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein of the University of Chicago urges us to excuse the required showing of injury

to personal property in cases of unauthorized electronic contact between computers, "extending the rules of trespass to real property to all interactive Web sites and servers." The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass….

[T]he metaphorical application of real property rules would not, by itself, transform a physically harmless electronic intrusion on a computer server into a trespass. That is because, under California law, intangible intrusions on land, including electromagnetic transmissions, are not actionable as trespasses (though they may be as nuisances) unless they cause physical damage to the real property….

More substantively, Professor Epstein argues that a rule of computer server inviolability will, through the formation or extension of a market in computer-to-computer access, create "the right social result." In most circumstances, he predicts, companies with computers on the Internet will continue to authorize transmission of information through e-mail, Web site searching, and page linking because they benefit by that open access. When a Web site owner does deny access to a particular sending, searching, or linking computer, a system of "simple one-on-one negotiations" will arise to provide the necessary individual licenses.

Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley of the University of California, Berkeley, writing on behalf of an amici curiae group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel." The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. As Professor Dan Hunter of the University of Pennsylvania asks rhetorically: "Does this mean that one must read the 'Terms of Acceptable Email Usage' of every email system that one emails in the course of an ordinary day? If the University of Pennsylvania had a policy that sending a joke by email would be an unauthorized use of its system, then under the logic of [the lower court decision in this case], you would commit 'trespass' if you emailed me a . . . cartoon." (Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons* (2003) 91 Cal. L.Rev. 439, 508-509.)

Web site linking, Professor Lemley further observes, "would exist at the sufferance of the linked-to party, because a Web user who followed a 'disapproved' link would be trespassing on the plaintiff's server, just as sending an e-mail is trespass under the [lower] court's theory." Another writer warns that "[c]yber-trespass theory will curtail the free flow of price and product information on the Internet by allowing website owners to tightly control who and what may enter and make use of the information housed on its Internet site." (Chang, *Bidding on Trespass: eBay, Inc. v. Bidder's Edge, Inc. and the*

*Abuse of Trespass Theory in Cyberspace Law* (2001) 29 AIPLA Q.J. 445, 459.) A leading scholar of Internet law and policy, Professor Lawrence Lessig of Stanford University, has criticized Professor Epstein's theory of the computer server as quasi-real property, previously put forward in the *eBay* case ( *eBay, supra,* 100 F. Supp. 2d 1058), on the ground that it ignores the costs to society in the loss of network benefits: "eBay benefits greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb." (Lessig, The Future of Ideas: The Fate of the Commons in a Connected World (2001) p. 171; see also Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, *supra,* 91 Cal. L.Rev. at p. 512 ["If we continue to mark out anticommons claims in cyberspace, not only will we preclude better, more innovative uses of cyberspace resources, but we will lose sight of what might be possible"].)

We discuss this debate among the amici curiae and academic writers only to note its existence and contours, not to attempt its resolution. Creating an absolute property right to exclude undesired communications from one's e-mail and Web servers might help force spammers to internalize the costs they impose on ISP's and their customers. But such a property rule might also create substantial new costs, to e-mail and e-commerce users and to society generally, in lost ease and openness of communication and in lost network benefits. In light of the unresolved controversy, we would be acting rashly to adopt a rule treating computer servers as real property for purposes of trespass law.
…
The judgment of the Court of Appeal is reversed.

**DISSENT: BROWN, J.**, Dissenting.

Candidate A finds the vehicles that candidate B has provided for his campaign workers, and A spray paints the water soluble message, "Fight corruption, vote for A" on the bumpers. The majority's reasoning would find that notwithstanding the time it takes the workers to remove the paint and the expense they incur in altering the bumpers to prevent further unwanted messages, candidate B does not deserve an injunction unless the paint is so heavy that it reduces the cars' gas mileage or otherwise depreciates the cars' market value. Furthermore, candidate B has an obligation to permit the paint's display, because the cars are driven by workers and not B personally, because B allows his workers to use the cars to pick up their lunch or retrieve their children from school, or because the bumpers display B's own slogans. I disagree.

Intel Corporation has invested millions of dollars to develop and maintain a computer system. It did this not to act as a public forum but to enhance the productivity of its employees. Kourosh Kenneth Hamidi sent as many as 200,000 e-mail messages to Intel employees. The time required to review and delete Hamidi's messages diverted employees from productive tasks and undermined the utility of the computer system. "There may . . . be situations in which the value to the owner of a particular type of

chattel may be impaired by dealing with it in a manner that does not affect its physical condition." (Rest.2d Torts, § 218, com. h, p. 422.) This is such a case.

The majority repeatedly asserts that Intel objected to the hundreds of thousands of messages solely due to their content, and proposes that Intel seek relief by pleading content-based speech torts. This proposal misses the point that Intel's objection is directed not toward Hamidi's message but his use of Intel's property to display his message. Intel has not sought to prevent Hamidi from expressing his ideas on his Web site, through private mail (paper or electronic) to employees' homes, or through any other means like picketing or billboards. But as counsel for Intel explained during oral argument, the company objects to Hamidi's using Intel's property to advance his message.

Of course, Intel deserves an injunction even if its objections are based entirely on the e-mail's content. Intel is entitled, for example, to allow employees use of the Internet to check stock market tables or weather forecasts without incurring any concomitant obligation to allow access to pornographic Web sites. ( *Loving v. Boren* (W.D.Okla. 1997) 956 F. Supp. 953, 955.) A private property owner may choose to exclude unwanted mail for any reason, including its content. ( *Rowan v. U.S. Post Office Dept.* (1970) 397 U.S. 728, 738 [25 L. Ed. 2d 736, 90 S. Ct. 1484] (*Rowan*); *Tillman v. Distribution Systems of America Inc.* (App. Div. 1996) 224 A.D.2d 79 [648 N.Y.S.2d 630, 635] (*Tillman*).)

…