Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

ASPEN PUBLISHERS VOLUME 21 • NUMBER 1 • JANUARY 2009

The Digital Pendulum: Conforming (or Mutating) the Parameters of Trespass Theory to Address the Act of Wrongfully Accessing a Computer System

By Gary L. Urwin and Jennifer L. Wagman

Beginning in the late 1990s, case law began to see a reemergence of an old and largely dormant tort theory—trespass to chattels—being applied to the digital-age act of wrongfully accessing computer systems. The tort of trespass to chattels under California law, traditionally viewed as the "little brother of conversion,"[1] encompasses "intermeddling with or use of or damages to" personal property that does not amount to an interference with the possessory right sufficient to constitute a conversion.[2] The defendant is therefore liable for damages measured by the impairment or loss of use of the property, not its full value.[3] Prior to 2003, the California Supreme Court had not addressed the tort of trespass to chattels in any depth since 1946.[4]

In dusting off this cause of action and realizing its potentially expanded application from cows to computers, federal and state courts in California have defined the parameters of high-tech applications of the theory—or left them undefined—in cases involving a colorful variety of acts designed to access computers. These fact patterns involve conduct ranging from the use of Internet robots, crawlers, and spiders to "recursively crawl" popular sites, to the sending of unwelcome emails, to the use of software to alter and circumvent restrictions in other software, to the transmission of commands to remotely disable installed software, to online monitoring of a PC's activity to identify piracy in the copying and distributing of copyright-protected material.

This article provides an updated look at the original expansion and later contraction of the trespass to chattels doctrine in California as applied to computer systems, and the ease or unease of the equilibrium in California law that has, in theory at least, subsequently been achieved in its application.

eBay v. Bidder's Edge, Inc.

In *eBay v. Bidder's Edge, Inc.*,[5] Bidder's Edge, Inc. (BE) operated an auction-aggregation Web site that gave users the ability to search for items across numerous online auction sites without having to search each host site individually. By repeatedly accessing various auction Web sites, BE compiled information pertaining to those sites in an easy-to-use database. Thus, a user could conduct a single search on a desired item to obtain information about that item on every auction site tracked by BE. The most significant, but not the sole, site accessed by BE was eBay.

To assemble its information database, BE used a variant of the methodology used by search engines like

Gary L. Urwin, a partner in the Los Angeles office of Hogan & Hartson LLP, specializes in business litigation with particular emphasis on the areas of intellectual property, media and entertainment, technology and Internet/IT systems, and complex commercial litigation. **Jennifer L. Wagman** is an associate with Hogan & Hartson LLP and practices in the litigation group.

Google or Yahoo! to canvass and catalog Web sites for inclusion in a user's search results: automated, "recursive" crawling by computer programs known variously as robots, spiders, or web crawlers.[6] BE, initially on a limited basis with eBay's consent and subsequently on an expanded basis without eBay's consent, programmed its robots to access eBay's site; the robots eventually accessed eBay's site approximately 100,000 times per day. The parties differed in their estimates of the comparative proportion of eBay's traffic that this use represented, but it was clear that BE's activity alone, at certain periods, constituted between 1.11 percent and 1.53 percent of the number of requests received by eBay and between 0.70 percent and 1.10 percent of the total data transferred by eBay. These statistics are put in perspective by considering that eBay users performed an average of 10 million searches per day on eBay's database at the time and placed 600 bids every minute on almost 3 million items, some 400,000 of which were added as new items to eBay's site every day.[7]

eBay sued and moved for a preliminary injunction preventing BE from accessing the eBay computer system based on nine causes of action, including trespass to chattels. The court observed generally that the non-trespass claims would only support injunctive relief addressing BE's use of eBay's *marks* and use of the eBay auction listings, not an injunction prohibiting BE from accessing eBay's *computer systems*, which thereby placed the trespass claim at the center of the court's analysis.[8]

Building on then-recent case law that had resuscitated the hoary tort theory of trespass to chattels by applying the doctrine to the unauthorized use of long-distance phone lines,[9] the court granted eBay's preliminary injunction based on its trespass-to-chattels claim. Delineating the tort as one that "lies where an intentional interference with the possession of personal property has proximately cause(d) injury," Judge Whyte opined that, to prevail on a claim for trespass in the computer system context, the plaintiff must establish that: "(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."[10]

Applying these criteria, the court first concluded that there was unauthorized interference. It was uncontested that BE's robots crawled eBay's Web site, and the court quickly dismissed BE's contention that the access was authorized because the eBay site was publicly accessible. To the contrary, the court noted, eBay's servers were private property to which eBay granted conditional access to the public; because eBay did not generally permit the type of automated access made by BE,[11] the access exceeded the scope of consent. On the non-traditional nature of the access, the court noted that "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 [as was the use of long distance telephone lines in *Thrifty-Tel*]."[12]

The court then went on to a trickier question in applying the second criterion of the required showing for trespass: whether BE's unauthorized use in this case "proximately resulted in damage to plaintiff." It is in this section of the opinion, and in the earlier balance-of-harm discussion addressing similar factors in the context of preliminary injunction law, that the court set forth the two most provocative points of its analysis, relating to type and extent of real harm.

First, the court defined the type of damage required in a computer-age trespass-to-chattels case. The court was not deterred by the fact that there was no claim of *physical damage* to eBay's computer system caused by the trespass nor any evidence to support a claim that eBay lost customers or revenues, candidly noting:

> 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").[13]

Nonetheless, the court stated:

> A trespasser is liable when the trespass diminishes the condition, quality or value of personal property. (Citation omitted). The *quality or value of personal property may be "diminished even though it is not physically damaged* by defendant's conduct." … 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* … send[ing] some 80,000 to 100,000 requests to plaintiff's computer systems per day.[14]

The court went on to state:

> [a]lthough eBay appears unlikely to be able to show a *substantial* interference at this time, such a showing is not required. … 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 . . . .[15]

Second, and perhaps even more noteworthy, in order to assess damage the court seized not only upon the pervasive number of BE's instances of access but also upon the cumulative effect to eBay *if* other aggregators similar to BE, emboldened by eBay's failure to obtain an injunction, potentially (here perhaps a polite synonym for hypothetically or speculatively) began to jump on the bandwagon and recursively crawl eBay's site in the same way that BE was doing:[16]

> 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. (Citation omitted). … *[T]he 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,* [such that] the plaintiff has at least *established a possibility of irreparable harm*."[17]

Thus, the court effectively found that this potential for aggregated harm, through access by other hypothetical parties' robots, contributed significantly to eBay's ability to satisfy the harm requirement:

> *If* preliminary injunction 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.[18]

Ticketmaster

In 2000, while *eBay* was being decided in the Northern District of California, the *Ticketmaster* litigation was pending in the Central District of California. In *Ticketmaster Corp. v. Tickets.com, Inc.*,[19] Ticketmaster sought to prevent Tickets.com from using robots or spiders to download material from Ticketmaster's Web site in order to extract factual information that Tickets.com then incorporated into its own Web site. In denying Ticketmaster's motion for preliminary injunction, Judge Hupp distinguished the facts of *eBay*, holding that there was insufficient injury to Ticketmaster's chattel as a result of Tickets.com's use of robots to constitute a trespass.[20]

The same court later granted summary judgment in favor of Tickets.com with respect to the trespass claim.[21] The court reasoned that:

> *unless there is actual dispossession* of the chattel for a substantial time (not present here), *the elements of the tort have not been made out.* Since the spider does not cause physical injury to the chattel, there *must be some evidence that the use or utility of the computer* (or computer network) being 'spiderized' *is adversely affected* by the use of the spider.[22]

Moreover, the fact that plaintiff expended time and money to thwart the spider was insufficient to establish damage to its computers or the manner in which they operate.[23]

Thus, during the same period as *eBay*, a different district court dealing with a large Internet site that could potentially have been harmed by hypothetical users as easily as eBay absent court protection found that the site owner had not provided adequate evidence of harm, whereas eBay's showing of comparatively minimal use by BE was sufficient indication of harm for a preliminary injunction to issue.

Oyster Software

In 2001, the District Court in the Northern District of California in *Oyster Software, Inc. v. Forms Processing, Inc.*,[24] addressed whether Oyster could survive a motion for summary judgment in regard to all of its claims, including its claim for trespass to chattels.

In *Oyster*, the plaintiff operated a Web site through which it offered software to customers that processed electronic or paper documents.[25] Contained in this Web site were metatags or "Hypertext Markup Language (HTML) code that describe[s] the contents of the Internet web site to a search engine."[26] Oyster discovered that Forms Processing, Inc., (FPI) was sending robots to Oyster's site and copying its metatags to use on FPI's own site. Based on FPI's copying of the metatags, Oyster brought a claim against various defendants, including FPI, claiming trademark infringement, conspiracy, and trespass to chattels. In response to Oyster's complaint, FPI brought a motion for summary judgment, claiming (among other things) that Oyster

did not produce any evidence "of obstruction of the basic function of Oyster's computer system by FPI" and thus that Oyster's trespass claim should fail.[27]

In addressing the summary judgment motion, the *Oyster* court followed its interpretation of the *eBay* rule and stated that, in order to prevail on a trespass claim, a plaintiff must show that "an intentional interference with the possession of personal property has proximately caused injury."[28] The *Oyster* court interpreted *eBay*'s rule to state that a plaintiff does not have to prove "substantial interference" with possession, but rather must show only that the defendant's conduct constituted "'intermeddling with or use of another's personal property.'"[29]

In applying this comparatively lenient rule, the court first stated that Oyster had presented no evidence that the use of the robots interfered with the basic function of its computers. Further, Oyster conceded that the robots placed only a "negligible" load on Oyster's computer system.[30] Nonetheless, the court agreed that FPI's simple copying of Oyster's metatags was sufficient for Oyster to survive summary judgment on its trespass claim because, as the *Oyster* court interpreted, *eBay* required only "use" of plaintiff's computer, whether or not the interference was more than negligible.[31] Thus, because Oyster presented evidence of use by FPI, the claim was not dismissed on the ground that Oyster had showed only "minimal interference."[32]

What then is the quantum of harm to a computer system's resources necessary to sustain (or in the case of *eBay*, establish the probable validity of) a claim of trespass to a computer system? In *Ticketmaster*, a very small but measurable amount was not enough; in *eBay*, a more substantial (though not overwhelming) amount (with the specter of repetition by others not before the court) *was* enough, at least for injunctive purposes. The *Oyster* court took *eBay* a step beyond its original application by requiring only a minimal showing of harm, not involving the potential for other hypothetical parties' use of robots on plaintiff's site, to survive a motion for summary judgment on a trespass claim.

Intel v. Hamidi

The California Supreme Court dealt with some of these issues in the 2003 case *Intel Corp. v. Hamidi*.[33] The court in *Intel* addressed the viability of a trespass to chattels claim in the context of electronic activity.

In this case, Intel brought a trespass-to-chattels claim against a former employee, Hamidi, based on Hamidi's use of Intel's electronic mail system to send emails to numerous employees strongly criticizing Intel's employment practices.[34] The court initially observed that, under established trespass law, "the defendant's interference must, to be actionable, have caused some *injury to the chattel or to the plaintiff's rights in it*."[35] The "dispositive issue," according to the court, was "whether the undisputed facts demonstrate[d] [that defendant's] actions caused or threatened to cause damage to [plaintiff's] computer system, or injury to its rights in that personal property."[36]

The evidence in *Intel* indicated that, despite defendant's sending his email message six times to as many as 35,000 addressees each time, plaintiff was not precluded from using its computers, nor did the defendant's actions "interfere[] with [the system's] ordinary and intended operation."[37] Moreover, Intel did not present evidence to show that the system "was slowed or otherwise impaired" by Hamidi's activity.[38] Further, the time and effort that Intel's staff spent attempting to block Hamidi's messages did not constitute "an injury to the [plaintiff's] interest in its computers … . [T]he fact [that plaintiff's] staff spent time attempting to block [defendant's] messages [could not] be bootstrapped into an injury to [plaintiff's] possessory interest in its computers."[39] Thus, while Intel may have shown that it had suffered injury in terms of employee time lost, which Justice Brown in dissent characterized as "time required to review and delete Hamidi's messages[,] divert[ing] employees from productive tasks and undermin[ing] the utility of the computer system," Intel ultimately could not show any real injury to the chattel itself or any possessory interest therein.[40]

Ultimately, the *Intel* court, favoring more of the *Ticketmaster* reasoning and less of the reasoning used in *eBay*, held that a trespass-to-chattels claim is not available under California state law absent a showing of *tangible interference to or impairment of* the use or operation of a computer.

> [U]nder California law the [trespass to chattels] 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….[41]

The court further reasoned that:

> it is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. *Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury* and prevent the tort; otherwise, we can create injury for every supposed tort.[42]

Acknowledging the then-recent case law exploring this area, the court noted that "decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning."[43] In those decisions, "the defendant's use of the plaintiff's computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power."[44] The court recognized that the "undisputed evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation." [45] Therefore, this case presented a fundamentally different fact pattern from *eBay* since no actual or potential injury to the chattel itself was claimed.

Finally, the court in *Intel* took pains to curtail any expansive reading of the rationale used in *eBay.* The *Intel* court twice stated that a showing of actual, not potential or hypothetical, harm is required, notwithstanding anything said in *eBay*: "we do not read *eBay* (citation omitted) as holding that the actual injury requirement may be dispensed with [as was argued by Intel], and such a suggestion would, in any event, *be erroneous as a statement of California law*."[46] Therefore, while the court in *eBay* allowed plaintiff to show harm through the threat of copycat robotic searchers, the California Supreme Court in *Intel* determined that California law allows a finding of harm only when actual, not potential, injury has been established.

Subsequent Applications

In analyzing subsequent cases that apply the uneasy equilibrium created by *eBay, Intel*, and the other cases cited in this article and in assessing the facts of pending or potential new cases confronting practitioners, significant consideration should be paid to the procedural time at which, and the procedural vehicle by which, the trespass issue is to be examined. These factors have a demonstrable tendency to play a role in the relative strictness or leniency of a court's application of the factors needed to sustain a trespass claim. The following cases are illustrative.

Miller v. IBM

Miller v. International Business Machines Corp.[47] arose out of a failed dotcom-era project by Best-of-China.com (BCC) to establish a Web portal and e-commerce site for Internet users in China that would provide news, information, products, and services. BCC contracted with various IBM subsidiaries (hereinafter IBM) to provide consulting services, software development services, and computer hardware to establish the Web portal.[48]

After BCC encountered funding difficulties and the parties attempted to resolve their disputes on various issues, IBM terminated its services and removed its software from BCC's server.[49] Various claims ensued.

Among BCC's claims was one for trespass to chattels. BCC alleged that IBM had impermissibly accessed BCC's server and disabled or removed some of the software that had been developed pursuant to the parties' agreements. BCC contended that IBM was authorized to access BCC's server only for purposes of building and maintaining the system, not for purposes of disabling it. In accessing the system, BCC contended, IBM had caused physical damage to certain parts of the system's hardware, rendering the system wholly inoperable. BCC alleged that the acts interfered with BCC's rights to derive income and value and caused BCC to incur expenses for transporting, storing, and insuring a valueless server system. IBM, by contrast, contended that it removed only applications for which BCC failed to pay.

On IBM's summary judgment motion, the district court adopted a two-step analysis for a trespass claim. Citing *eBay,* the court recited that a trespass claim requires a showing of (1) access without authorization and (2) damage. The court then concluded (without citing *Intel* or specifying a particular state's trespass law) that a triable issue existed as to prong one, the access-without-authorization prong, because "this issue [*i.e.,* whether extraction of the components was justified by BCC's failure to keep payments current] is in dispute."[50] (The court presumably meant that a question of fact existed as to the scope of the applicable rights.) On the second prong, the requirement-of-damage prong, however, the court agreed with IBM's argument that BCC had not shown damage from the trespass, and it granted IBM's motion for summary judgment on this basis.

Noting that BCC had *alleged* damage from the trespass, the court nonetheless found that BCC had not made a sufficient showing on summary judgment to back up this claim:

> *The only evidence [BCC] has cited in support of [its] claim are a series of email messages* exchanged between [Mr. Miller] and Mr. Hui, wherein they *discuss the removal of the software that ETC developed. [Citations omitted]. …[BCC] contends that the removal of this software disabled the system, rendered it valueless, interfered with [Mr. Miller's] and BCC's right to derive income and value from the Server System,* and caused BCC to expend

> unnecessary expenses in transporting, storing and insuring the Server system. Aside from these allegations, however, Mr. Miller has proferred no evidentiary support for his claim that he and/or BCC incurred damages as a result of IBM China and ETC's alleged trespass.[51]

Thus, in opposing the motion for summary judgment, BCC failed to make a sufficient showing of harm, given that it only alleged damage to its system without providing any evidentiary support for that contention. Unlike *Oyster,* where plaintiff essentially had to show only the use by defendant of plaintiff's computer system in order to survive summary judgment, the court in *Miller* required a higher threshold of harm to survive at the summary judgment stage.

Therapeutic Research Facility

At the other end of the spectrum is the court's treatment of a pleaded trespass claim in *Therapeutic Research Faculty v. NBTY, Inc.*[52] *Therapeutic Research* arose on a motion to dismiss, as distinguished from *Miller*, which arose in the context of a motion for summary judgment.

In *Therapeutic Research*, the owner of copyrights in a work available both in a print edition and in an online version brought a claim against a user of the plaintiff's Web site. The online version of the copyrighted work was available in a password-protected area of plaintiff's Web site for plaintiff's paid subscribers only. The defendant purchased a single-user subscription to the online version of the work, the terms of which limited access to the work to "one and only one person."[53] Plaintiff claimed that the defendant shared the confidential user name and pass code among its employees and that the defendant had allowed a third party to use the confidential name and password from the defendant's single-user subscription to gain access to protected areas of the site.

In addition to copyright infringement claims and claims arising under various statutes including the Computer Fraud and Abuse Act,[54] plaintiff pleaded a trespass claim. On defendant's motion to dismiss, the court's treatment of the trespass claim was succinct and lenient, largely due to the pleading-stage status of the case:

> Plaintiff alleges in its Complaint that it has suffered "irreparable damages" because "Defendants, without permission … or exceeding the scope of such permission, willfully and maliciously entered upon [its] passcode-protected web site." (Citation omitted). Since Defendants fail to show Plaintiff's allegations are insufficient to state a trespass claim, this portion of their motion is denied.[55]

Thus, without citation to *Intel, eBay*, or the other authorities discussed in this article, the *Therapeutic Research* court upheld as adequate, for purposes of surviving a motion to dismiss, allegations that the defendant lacked or exceeded permission to access the site. Further, the plaintiff survived the motion to dismiss despite the lack of any allegation of damage or impairment to the plaintiff's computer system.

Vertkin v. Vertkin

Vertkin v. Vertkin[56] was a civil action brought between a divorcing couple. In a decision issued the same year as *Therapeutic Research*, the *Vertkin* court decisively granted the defendant's motion to dismiss because the plaintiff had failed to "state a colorable trespass to chattels claim."[57]

In *Vertkin*, the husband allegedly "installed various types of tracking software on Plaintiff [wife]'s computers" to obtain her personal information, despite a recently issued restraining order forbidding him from "remov[ing], transfer[ring], or otherwise alter[ing] any financial accounts held between him and Plaintiff."[58] Among other claims, the plaintiff wife alleged that she had a viable trespass-to-chattels claim based on the defendant's removing information from her computer (as opposed to the previous cases that involved burdens or harmful processes placed *on* the plaintiff's computer, not material taken *from* the computer).

Directly citing and following *Intel* for the proposition that a plaintiff has a trespass claim only if the intermeddling impaired the chattel as to its "'condition, quality, or value, or if the possessor [was] deprived of the use of the chattel for a substantial time,'" the court held that the plaintiff's trespass claim must be dismissed.[59] Because the only harm that the plaintiff alleged was a result of the defendant's taking of information and not harm to the quality or condition of her computer, her cause of action was dismissed. Though arising in an atypical context, this case illustrates a consistent application of the principles to reject a trespass claim (even at the early pleading stage) when the pleaded harm relates only to the content of the information accessed/taken and not to any damage or impairment to the system itself.

Atlantic Recording

In a fourth post-*Intel* case, *Atlantic Recording Corp. v. Serrano,*[60] the court addressed a counterclaim by Serrano, alleging trespass to chattels in the context of a motion to dismiss.

In *Atlantic Recording*, a group of music and recording companies that owned exclusive rights to reproduce and distribute certain copyrighted music collectively brought suit against Serrano. Serrano allegedly used a peer-to-peer (P2P) network to search for files stored on other users' computers and subsequently distributed 224 audio files, including files containing plaintiffs' copyrighted audio, over the Internet without plaintiffs' permission.

Adhering to the theory of "the best defense," Serrano brought a counterclaim alleging, *inter alia,* trespass to chattels. The basis for the alleged trespass claim arose from the actions of plaintiffs' online investigation company, Media Sentry, Inc. Media Sentry was hired to investigate and collect electronic evidence of copyright infringement. Media Sentry allegedly identified Serrano as using a P2P network at a particular IP address,[61] leading to a subpoena of Serrano's Internet service provider to ascertain his identity and ultimately to a copyright infringement suit. In response, Serrano alleged that Media Sentry's accessing his computer to ascertain whether he was using a P2P network constituted a trespass. The court, somewhat colloquially, characterized Serrano's claim as one that Media Sentry "committed trespass by searching Defendant's computer without permission."[62]

The court agreed with plaintiffs' challenge to this claim by granting plaintiffs' motion to dismiss. However, the court granted the motion *without* prejudice, leaving the door open to future pleading of additional facts. In granting the motion, the court applied two case-based trespass principles. First, the court cited *Intel* for the proposition that the trespass-to-chattels tort does not encompass a communication that neither damages the recipient computer system nor impairs its functioning. Because Serrano had not alleged any damage to his computer or any interference with his right to possess the machine, his counterclaim failed in this respect. Second, the court cited *eBay* for the proposition that, when the specter of many electronic communications seriously threatens a computer system's integrity, a trespass-to-chattels action may lie. However, because Serrano, unlike eBay, did not "operate[ ] a high profile commercial web site subject to attack by spammers or information-collecting robots," he could not base his trespass claim on the potential that "other operators of parasitic websites [would] widely replicate[ ] the [plaintiffs'] conduct [such that] the [defendant's] business and computer operations would surely suffer."[63]

Thus, the court found insufficient the defendant/counterclaimant's allegations that he (not his computer) suffered "embarrassment, anxiety, mental distress, emotional pain and suffering, inconvenience and financial distress" due to the plaintiffs' alleged trespass.[64] Without an allegation that defendant suffered damage to his computer or that plaintiffs interfered with his right to possess, and without any potential that "automated data collection services threaten to overwhelm his personal computer," defendant failed to plead his trespass claim adequately.[65] The court stated that "[i]n short, Defendant ha[s] merely alleged an electronic communication that neither damaged the recipient computer system nor impaired its functioning. [Citing *Intel*.] The California Supreme Court has clearly held that such conduct is not actionable under trespass to chattels."[66]

Coupons, Inc.

Finally, in *Coupons, Inc. v. Stottlemire,*[67] trespass again arose in the context of a motion to dismiss and again survived at an early pleading stage. In this case, the plaintiff developed coupon software that enabled a consumer to obtain online, printable consumer coupons. The coupons were offered to the public by the plaintiff's clients, consumer products companies that from time to time offered sales promotions. In the normal use of the plaintiff's software by consumers, a numerical limit applied to the number of times that a user could print each coupon.

Plaintiff alleged that defendant, an individual, discovered how to remove the counter that limited the amount of times that a consumer could print a coupon and then created a computer program that automated the removal of the counter. Defendant allegedly provided his removal, or circumvention, software to others, allowing users to print and use coupons with no numerical limit (other than the overall campaign limit established by the consumer product company from which the sales campaign originated). Amidst a variety of other claims, plaintiff alleged that the defendant committed trespass to chattels by wrongfully "meddl[ing]" with plaintiff's server, causing it to send more than the authorized number of coupons to users.[68]

On a motion to dismiss, a Magistrate Judge allowed the trespass claim to survive. Citing *Intel* and holding that the complaint sufficiently alleged the existence of damage by "causing [the server] to send more than the authorized number of coupons to Stottlemire's computer," the court determined that it would be "premature to dismiss the trespass to chattels claim at this time."[69] Further, the court saved for a later date defendant's argument that any interference with the server must be non-trivial to be actionable, with language perhaps signifying that the claim is unlikely to survive summary judgment: "[a]lthough this may be an appropriate argument once more facts have been established," dismissal was not appropriate at the pleading stage.[70]

Conclusion

Although there has not always been consistency on the conceptual nature of "damage" or "impairment" to a computer, a pattern emerges from the courts' dealings with these moving-pendulum issues.

First, practitioners can expect, under most conventional fact patterns (and without actual evidence of impairment or slowing of the accessed computer's resources), that courts will effectuate the balance between these principles by approaching pleading stage motions somewhat leniently in considering allegations seeking to elevate computer *use* to computer *damage* or *impairment*. In other words, despite court decisions on either end of the spectrum in the trespass cases discussed in this article, an important consideration in determining the outcome of a case appears to be the stage at which the issue presents itself for decision. On a motion to dismiss, a court may be surprisingly likely to find that trespass survives, as in *Therapeutic Research* in which the plaintiff essentially failed to plead any damage, or in *Coupons, Inc.* in which the plaintiff pleaded only access to the system and not harm. Occasionally, however, a sufficiently clear fact pattern emerges to support a successful motion to dismiss, as in *Vertkin*, where plaintiff's trespass claim was based only on the information taken and not on any harm to plaintiff's tangible property.

On the other hand, when a trespass claim is being decided at trial or on a motion for summary judgment and a higher evidentiary burden is applied, claims lacking a significant showing of the *Intel* factors will face a tough road, as was the case in *Miller* (plaintiff's trespass claim did not survive summary judgment because a mere allegation of harm without proof of harm was insufficient). Thus, at the final disposition stage requiring an evidentiary showing, courts can be expected to be significantly more rigorous about scrutinizing claims of damage or impairment and in need of a concrete showing of harm to a computer, not merely the unwelcome use of an insignificant amount of its resources.

Second, the *eBay* principle of hypothetical damage by repeated use is fact-specific and has been applied in a restricted fashion, modern courts declining to accept its pre-*Intel* invitation to make non-impairing use actionable beyond a relatively narrow set of facts akin to *eBay.* (Indeed, a large part of the *eBay* rationale depends on the injunction context and a site such as eBay's that is susceptible to robotic searching by multiple accessing parties.) However, in an appropriate case, the *eBay* doctrine is available, perhaps with some tarnish, and subject to a likely pleading battle given the Supreme Court's rigor in requiring real *damage* before one can recover *damages.*

Notes

1. William Lloyd Prosser & W. Page Keeton, The Law of Torts § 14 at p.86 (5th ed. 1984); *see generally* 7 Stuart M. Speiser, Charles F. Krause & Alfred W. Gans, The American Law of Torts § 23:23 at pp.678-679 (1990).
2. Zaslow v. Kroenert, 29 Cal. 2d 541, 551 (1946).
3. *Id.*
4. *Id. Cf.* Jordan v. Talbot, 55 Cal. 2d 597, 610 (1961) (dealing incidentally with the parameters of the cause of action).
5. eBay v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000).
6. *Id.* at 1061 n.2.
7. *Id.* at 1064.
8. *Id.* at 1063.
9. Thrifty-Tel v. Bezenek, 46 Cal. App. 4th 1559, 1566 (1996).
10. *eBay*, 100 F. Supp. 2d at 1069-1070.
11. eBay excluded robots by means of an automated "robot exclusion header" contained in a robots.txt data file. The header was readable by robots, and programmers of robots could voluntarily design their robots to comply with the directive they would receive on the site that eBay did not permit unauthorized robotic activity. In other words, robots accessing the message in the robots.txt file received electronic direction that they should not further access the site. While major search engines, including Yahoo! and Google, respected the industry's so-called "Robots Exclusion Standard" that underlay this practice, BE did not afford the same courtesy. *Id.* at 1061, 1063.
12. *Id.* at 1069. A similar though less detailed analysis had also been applied, and a similar injunctive remedy obtained, in the same district two years earlier in Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389 * 7 (N.D. Cal. Apr. 16, 1998).
13. *Id.* at 1071 (emphasis added). *See also eBay*, 100 F. Supp. 2d at 1065 ("In alleging economic harm, eBay's argument is that eBay has expended considerable time, effort and money to create its computer system, and that BE should have to pay for the portion of eBay's system BE uses. eBay attributes a pro rata portion of the costs of maintaining its entire system to the BE activity. However, *eBay does not indicate that these expenses are incrementally incurred because of BE's activities, nor that any particular service disruption can be attributed to BE's activities.*" *eBay*, 100 F. Supp. 2d at 1065 (emphasis added).
14. *Id.* at 1071 (emphasis added).
15. *Id.* at 1071 (emphasis added).
16. *Id.* at 1071-1072.
17. *Id.* at 1066 (emphasis added) (footnotes omitted).
18. *Id.* at 1071-1072 (emphasis added).
19. Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000).
20. *Id.* at *4. ("A basic element of trespass to chattels must be physical harm to the chattel (not present here) or some obstruction of its basic function (in the court's opinion not sufficiently shown here). … The comparative use [by defendant] appears

very small and there is no showing that the use interferes to any extent with the regular business of [the plaintiff].").
21. Ticketmaster Corp. v. Tickets.com, No. CV99-7654-HLH(VBKX), 2003 WL 21397701 (C.D. Cal. Mar. 7, 2003).
22. *Id.* at *3 (emphasis added).
23. *Id.*
24. Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001).
25. *Id.* at *1.
26. *Id.* at *1 n.3.
27. *Id.* at *3.
28. *Id.* at *12, citing *eBay*, 100 F. Supp. 2d at 1069.
29. Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 2001, at *12, citing *eBay*, 100 F. Supp. 2d at 1069-1070.
30. Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 2001, at *13.
31. *Id.*
32. *Id.*
33. Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003).
34. *Id.*
35. *Id.* at 1350 (emphasis added).
36. *Id.* at 1352.
37. *Id.* at 1349, 1353.
38. *Id.* at 1352.
39. *Id.* at 1359.
40. *Id.* at 1367 (Brown, J. dissenting).
41. *Id.* at 1347 (emphasis added).
42. *Id.* at 1359 (emphasis added).
43. *Id.* at 1353, later citing Register.com v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000)*; cf. Oyster,* 2001 WL 1736382 2001 at*12, *13.
44. *Intel*, 30 Cal. 4th at 1356.
45. *Id.* at 1352.The court also articulated the difference between trespass to a computer system caused by injury to the operation of the system and the "fictional recharacterizing" of a trespass based on "the allegedly injurious effect of a communication's *contents* on recipients as an impairment to the device which transmitted the message." *Intel*, 30 Cal. 4th at 1358. The court rejected a so-called "harm by content" theory as it determined that Intel's claim failed because its "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." *Id.* at 1348.
46. *Id.* at 1357 n.5 (emphasis added). *See also id.* at 1357 (noting that this reading of *eBay* "would *not be a correct statement of California or general American law* on this point") (emphasis added).
47. Miller v. International Business Machines Corp., No. C02-2118 MJJ, 2006 WL 2792416 (N.D. Cal. Sept. 26, 2006).
48. *Id.* at *2.
49. *Id.*
50. *Id.*
51. *Id.* (emphasis added).
52. Therapeutic Research Faculty v. NBTY, Inc., 488 F. Supp. 2d 991 (E.D. Cal. 2007).
53. *Id.*
54. Companion claims for violations of the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030), along with fact-specific intellectual property claims, are commonly asserted together with trespass claims in the situations described in this article.
55. *Id.* at 999.
56. Vertkin v.Vertkin, No. 07-4471 SC, 2007 WL 4287512 (N.D. Cal. Dec. 6, 2007).
57. *Id.* at *3.
58. *Id.* at *1.
59. *Id.* at *3, citing *Intel*, 30 Cal. 4th at 1357.
60. Atlantic Recording Corp. v. Serrano, No. 07-CV-1824 W(JMA), 2007 WL 4612921 (S.D. Cal. Dec. 28, 2007).
61. IP addresses, or Internet protocol addresses, "enable computers to communicate with each other over the Internet … . (Citation omitted). When a computer requests information from another computer over the Internet, the requesting computer must offer its IP address to the responding computer in order to allow a response to be sent. (Citation omitted). These IP addresses allow the identification of the source of incoming requests." *eBay*, 100 F. Supp. 2d at 1061.
62. *Id.* at *4.
63. *Id.* at *5.
64. *Id.*
65. *Id.*
66. *Id.*
67. Coupons, Inc. v. Stottlemire, No. CV 07-03457 HRL, 2008 WL 3245006 (N.D. Cal. July 2, 2008).
68. *Id.* at *6.
69. *Id.*
70. *Id.*

Reprinted from *Intellectual Property & Technology Law Journal* January 2009,Volume 21, Number 1, pages 1-9, with permission from Aspen Publishers, Inc., Wolters Kluwer Law & Business, New York, NY, 1-800-638-8437, www.aspenpublishers.com