An Analysis of California’s Common and Statutory Law Dealing with Unsolicited Commercial Electronic Mail: An Argument for Revision*

TABLE OF CONTENTS

I. INTRODUCTION ..................................................................................................................1202
II. THE GROWTH OF THE INTERNET AND UNSOLICITED COMMERCIAL E-MAIL ..................................................................................................................1204
III. USING CALIFORNIA COMMON LAW OF TRESPASS TO CHATTELS ...............................................................................................................................1208
IV. UNSOLICITED COMMERCIAL ELECTRONIC MAIL LEGISLATION IN CALIFORNIA .................................................................................................................................1215
   A. Electronic Mail and the Telephone Consumer Protection Act.................................................................................................................................1215
   B. California’s Statutes on Unsolicited Commercial Electronic Mail ...........................................................................................................................1217
V. ANALYSIS OF CALIFORNIA’S STATUTES ON UNSOLICITED COMMERCIAL ELECTRONIC MAIL ...........................................................................................................1219
   A. Where Sender Does Not Have a Contractual Relationship with the Internet Service Provider .........................................................................................1219
   B. Where Sender Does Have a Contractual Relationship with the Internet Service Provider ...........................................................................................1222
VI. PROPOSED REVISION OF THE CALIFORNIA STATUTES ...................................................................................................................................................1228

* J.D. candidate 2001, University of San Diego School of Law; B.A., University of California, Irvine. The author would like to thank Instructor Roberta Robinson, University of San Diego School of Law, for her editing, insight, and valuable guidance. The author would also like to thank the Law Review Board for making the review process as painless as possible. Finally, the author would like to thank his wife, Grace, for everything that is important. The author will be joining the Los Angeles office of Musick, Peeler & Garrett as an associate in the fall of 2001.
I. INTRODUCTION

Unsolicited commercial electronic mail, or spam,\(^1\) has been at the center of controversy.\(^2\) If you use the Internet, you have almost certainly received spam; chances are good that you are being bombarded with unsolicited commercial electronic mail.\(^3\) If you are one of the lucky few that have not received unsolicited commercial electronic mail, it is likely that you will receive spam as you continue to use the Internet.\(^4\) The magnitude and scale of the unsolicited commercial electronic mail problem are so great that they stretch the imagination. At any given time, up to thirty percent of all electronic mails sent in cyberspace is spam.\(^5\) Even a conservative estimate, pegging spam electronic mail at

---

1. See Send Your Junk E-Mail to New Web Site, STAR TRIB., June 3, 1999, at 13E. According to Net lore, a sketch from the British comedy troupe Monty Python’s Flying Circus was the inspiration for the spam nickname. In a diner, a frustrated couple tries in vain to order a dish that doesn’t include Hormel’s canned, chopped, jellied pork shoulder. As the waitress rattles off the day’s menu, “Spam, egg, Spam and sausage,” a group of Vikings at the next table sings, “Spam, Spam, Spam, lovely Spam!” eventually drowning out everyone else. Id.

2. There is even a controversy over the name spam. Hormel Foods Corporation, the maker of the canned food “SPAM” has threatened Cyber Promotion, Inc., an unsolicited electronic mail provider, with a lawsuit if it does not stop using the term “spam” in referring to its bulk electronic mail business. See Hormel Objects to Cyber Promotions’ Use of ‘SPAM’ Mark, ANDREWS COMPUTER & ONLINE INDUS. LITIG. REP. 24432, July 15, 1997, at 1, available in 1997 WL Database Allnewsplus; see also David Bloom, Digital L.A. 2 Faces of Spam: For Some, It’s Lunch Meat in a Can; Others Only See Junk E-mail Pain, L.A. DAILY NEWS, Sept. 12, 1998, available in 1998 WL 3869261.

   The SPAM folks also take time to explain their position on SPAM vs. spam, also known as unsolicited commercial e-mail or UCE. “We do not object to use of this slang term to describe UCE, although we do object to the use of our product image in association with that term. Also, if the term is to be used, it should be used in all lower-case letters to distinguish it from our trademark SPAM, which should be used with all upper-case letters.” Id.

3. See GartnerGroup Benchmarks the State of Spam in Largest Ever Survey of Internet Email Users; Reveals that Email Users Expect Greater Spam Protection from ISPs, BUS. WIRE, June 14, 1999, available in 1999 WL Database Allnewsplus [hereinafter GartnerGroup Benchmarks the State of Spam] (“Among the survey’s finding was that over 90 percent of [Internet] users receive spam at least once a week and almost 50 percent get spammed six or more times per week.”).

4. See Elizabeth Weise, Feeling Spammed? Internet Users Get Deluged by More Junk E-Mail, DETROIT NEWS, Aug. 5, 1999, at C3 (“And the longer you have your e-mail address, the higher the probability you will get spammed—from 63 percent at two months to 96 percent for those online four years or more.”).

5. See Court Ruling on Junk E-Mail is Good News for Computer Users, BUFF. NEWS, Jan. 10, 1999, at H2 (“By some estimates, as much as 30% of all e-mail is spam,
only ten percent of total electronic mail sent daily, translates to 220 million unsolicited commercial electronic mails a day. Even assuming that Internet use will not increase in the future, such an estimate translates to 80.3 trillion unsolicited commercial electronic mails sent each year.

Although we are used to receiving traditional paper “junk” mail, unsolicited commercial electronic mail seems to strike an especially negative chord with the American people. This is reasonable given that spam is different from traditional junk mail in at least three ways. First, the content of the vast majority of spam is in poor taste or outright fraudulent. Second, the monetary cost of receiving unsolicited commercial electronic mails is generally borne by the recipient. Third,

and the spammers are getting more sophisticated.”); see also Margie Wylie, Get Even With Spammers: Trade Your Junk E-Mail for Discount at Online Store, GRAND RAPIDS PRESS, May 26, 1999 (“‘You’ve got mail!’ should be ‘You’ve got spam!’ The world’s largest Internet service provider, AOL reports that unsolicited commercial pitches account for up to 30 percent of its total e-mail load.”).

6. Of the 2.2 billion electronic messages sent daily, some analysts think that 10% or 220 million messages are spam. See Michael Stroh, Spam is Still the Biggest Irritant of E-Mail, BUFFALO NEWS, Mar. 30, 1999, at E8.

7. This assumption is not accurate given the huge projected growth in Internet use. See North America is the Leading Region for Internet Users According to the Computer Industry Almanac, P.R. NEWSWIRE, Aug. 17, 1999, available in LEXIS, Wire Service Stories [hereinafter North America is the Leading Region].

8. The top three reasons that consumers cited for disliking spam are the waste of time, the invasion of privacy, and the offensive nature of the content. See Weise, supra note 4.


Much of the content of the “Spam Database Analysis” [of 200,000 randomly selected e-mails] was not fit for public publication, with many e-mails descriptive enough to make Monica Lewinsky blush and to make the Starr Report seem like a yawn.

That study found that more than 30% of the 200,000 unsolicited e-mails analyzed were pornographic, another 30% were “dubious money-making proposals.” Other direct marketed products made up another 24% of the total unsolicited e-mail the group collected.

Health cures, weight loss and Viagra sales or substitutes made up another 10% of the spam on the Internet.

Id.

10. Two dollars, or about 10%, of access fees charged by Internet service providers is used to mitigate the impact of spam, either through network expansion or with anti-spam software. See Wylie, supra note 5. Some consumers may have to pay more directly. For example, America Online customers on the $4.95 plan get three hours of monthly Internet access. Each additional hour costs an additional $2.50. See America Online, AOL Pricing Plans (visited Jan. 19, 2000) <http://www.aol.com/info/pricing>.
unsolicited commercial electronic mails have been known to carry dangerous viruses that can damage the recipient’s computer.\footnote{Unsolicited commercial e-mails may carry computer viruses. See Doug Bedell, \textit{Smashing Spam: Internet Coalition Pushing for Federal Law to Stop Electronic Quick-Buck Artists}, DALLAS MORNING NEWS, July 13, 1999, at 1F.}

The compounded economic loss of productivity in sorting, reading, and deleting spam is not trivial or lost on the general public.\footnote{See Jeanette Brown, \textit{The Mess Made for Business by Junk E-Mail}, BUS. WEEK, Apr. 19, 1999, at 146D.} It is no wonder that people and businesses have turned to self-help, the courts, and the legislature to combat the spread of spam.

This Comment will examine the law governing unsolicited commercial electronic mail in California. Part II details the growth of the Internet and unsolicited commercial electronic mail. Part III examines the law of trespass to chattel as applied to unsolicited commercial electronic mail in California. Part IV examines recent legislative efforts to regulate spam in California. Part V analyzes the implications of the new unsolicited electronic mail legislation in California. Finally, Part VI details some suggested revisions to the California statute dealing with unsolicited commercial electronic mail.

II. THE GROWTH OF THE INTERNET AND UNSOLICITED COMMERCIAL E-MAIL

The U.S. Defense Department created the Internet over two decades ago for academic and military use.\footnote{See Philip Elmer-Dewitt, \textit{Battle for the Sole of the Internet}, TIME, July 25, 1994, at 50, 52. Initially, only universities and the government had the ability to access the Internet. See \textit{id}.} Initially, very few people had access to the sophisticated computer equipment required to access the Internet. With relatively few users, there were few problems with unsolicited commercial electronic mail. However, as prices for equipment dropped significantly, more people began to access the Internet. Internet service providers emerged to provide easy access to millions of customers.\footnote{See \textit{id}. at 53.}

The growth of the Internet spurred the growth of unsolicited commercial electronic mails. In the beginning, self-governance was effective in deterring unsolicited commercial electronic mail.\footnote{See Joshua A. Marcus, Note, \textit{Commercial Speech on the Internet: Spam and}
and more people began logging onto the Internet, a series of norms and
rules called "Netiquette" emerged and was commonly followed. However, as technology improved and commercial entities started to
provide access to the general public, the sheer number of Internet users
made Netiquette impracticable since many newcomers did not know the
rules or ignored them. The commercialization of the Internet combined
with a cheap and easy form of advertising proved too tempting for
opportunist Internet users to ignore Netiquette. Currently, there are
over 83 million adults in North America alone that use the Internet on a
weekly basis, with the number expected to grow rapidly.

Consumers and the Internet service providers have not welcomed the
increase in unsolicited commercial electronic mail. Many consumers
believe that their Internet service providers are sending the junk
electronic mail directly or indirectly through the sale of their Internet
address. The customer satisfaction rates of Internet service providers
have gone down significantly as more and more customers are deluged
with unsolicited commercial electronic mails.

Consumers have also responded to unsolicited commercial electronic
mail by requesting that senders take their respective addresses off of the
particular mailing list. Such requests have generally been ineffective.
In fact, such replies to unsolicited commercial electronic mail businesses

16. These rules generally barred sending unsolicited commercial electronic mail.

See id.
17. See id. at 247.
18. See Kopec, supra note 9 (quoting Rep. Rush Holt, D-N.J., as stating that, "It
costs very little to send out millions of e-mails and whatever return you get is gravy.").
19. Number of adult Internet users, in thousands (add 15% to 30% to account for
occasional Internet users):

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Worldwide</td>
<td>39,479</td>
<td>150,887</td>
<td>318,650</td>
<td>717,083</td>
</tr>
<tr>
<td>North America</td>
<td>26,217</td>
<td>82,989</td>
<td>148,730</td>
<td>229,780</td>
</tr>
</tbody>
</table>

North America is the Leading Region, supra note 7.
20. Twenty-four percent of respondents in a survey thought that their ISPs
provided spammers with their electronic mail address. See GartnerGroup Benchmarks
the State of Spam, supra note 3.

See id.
21. See id.
22. There is even a service that will generate a "strongly worded reply" demanding
that the spammers "cease or pay the recipient $10 for each further mailing." Bedell,
supra note 11.
26, 1999, at L5.
will likely backfire and increase the total number of spam sent to one's email address. Even worse, the spammer may be counting on replies as part of a larger scam. In one case, the unsolicited commercial electronic mail came with a telephone number and instructions on how to be removed from the mailing list. Unfortunately, people who called to be removed from the list "ended up making an international call to the island of Grenada." Since the problem of unsolicited commercial electronic mail generally increases with time, consumers have resorted to canceling their old accounts and opening brand new accounts just to avoid receiving the increased volume of electronic mail. Even a new email address provides only a short-term solution since the new electronic mail address is still vulnerable to unsolicited commercial electronic mail.

Internet service providers have responded to unsolicited commercial electronic mail with self-help. Internet service providers and spammers are constantly playing a game of cyber "cat and mouse" to defend or penetrate the network of Internet service providers. One tactic of Internet service providers is to collect all the junk electronic mails from a spammer and send them back to the spammer as an electronic "email bomb." The purpose of these electronic mail bombs is to overwhelm and thus disable the spamming party's own network. Internet service providers have also responded to spamming by transmitting harmful signals back to the spammer. Ordinarily, network computers send occasional "ping" signals to check the connection. However, Internet service providers have used mass quantities of signals, or "ping attacks,"

24. See Bedell, supra note 11 ("Replying to spammers is often counterproductive, Mr. Oxman of Choose Your Mail warns. Asking to be removed from a spam list may only exacerbate the problem by confirming that yours is a 'live' address."); Campbell, supra note 23 ("Don't respond [to spam]! Don't ask them to 'take you off a list.' People who respond—even negatively—are viewed as Grade A targets. You will probably get more junk than ever.").
25. See Campbell, supra note 23.
26. Id.
27. See GartnerGroup Benchmarks the State of Spam, supra note 3 ("The poll [of Internet users] shows that email users are not only annoyed by spam, but that many have and will do something about it by changing their ISP [Internet Service Provider] in order to reduce or eliminate it.").
28. Even if Internet users do all they can to protect their electronic mail addresses, they may still receive spam. Spammers use computer programs that randomly generate e-mail addresses. Therefore, never disclosing one's electronic mail address does not mean that one will never get spam. See Bedell, supra note 11.
30. See id.
31. See id.
32. See id.
to overwhelm and disable the network of the offending party.\textsuperscript{33} In order to avoid such attacks, spammers have employed "spoofing" techniques to camouflage their origin or to make it appear as if their true origin is elsewhere.\textsuperscript{34}

Internet service providers are also employing new and sophisticated computer software to prevent outbreaks of unsolicited commercial electronic mail.\textsuperscript{35} There is also software available to the general public to screen out unsolicited commercial electronic mail.\textsuperscript{36} Such software also reduces the enormous economic harm that spamming can cause to a computer system.\textsuperscript{37} There is evidence that these new software programs have had some success in reducing spam.\textsuperscript{38} However, some commentators have raised concerns regarding the right of privacy with these new software programs designed to detect spam activity.\textsuperscript{39} In some situations, Internet service providers have resorted to reading an individual's mail in order to determine if such mail is unsolicited commercial electronic mail.\textsuperscript{40}

Unsolicited commercial electronic mail has had a negative impact on both the users and Internet service providers. Consumers subsidize the cost of receiving unwanted electronic mail.\textsuperscript{41} For the Internet service provider, the cost can be measured in the dollars and resources spent to deal with unsolicited commercial electronic mail.\textsuperscript{42} Aside from the

\begin{itemize}
\item \textsuperscript{33} See id.
\item \textsuperscript{34} See id.
\item \textsuperscript{35} See Jeff Partyka, \textit{AT&T WorldNet to Use Brightmail Anti-Spam}, INFOWORLD DAILY NEWS, Aug. 26, 1999, available in 1999 WL 10504704 (quoting Jeff Magill, Vice President of Marketing at Brightmail, "As soon as one of those e-mail accounts receives a piece of [spam] e-mail, it's transmitted to the BLOC, which is staffed 24 hours a day, seven days a week by spam masters . . . . Once it finds a piece of suspected spam, the BLOC staff updates each user's 'spam wall' to keep out the latest outbreaks.").
\item \textsuperscript{36} For example, Microsoft Explorer 4 and 5 are set up to use a program called Outlook 97. Outlook 97 has a built in filter that can screen out potential spam by looking at key words. See Bedell, supra note 11.
\item The cost of receiving spam can be 10% of the access fee. See Wylie, supra note 5.
\item See Bedell, supra note 11 (quoting Ian Oxman, President of Choose Your Mail, as saying, "We'll be bringing 200,000 [unsolicited e-mail] messages sent from all over . . . . And we're finding over half of the stuff is unique, which is really kind of frightening.").
\item See generally Steven Miller, Comment, \textit{Washington's "Spam Killing" Statute: Does It Slaughter Privacy in the Process?}, 74 WASH. L. REV. 453 (1999) (arguing that "existing privacy laws fail to provide meaningful protection to e-mail subscribers").
\item See id. at 453.
\item See Campbell, supra note 23; see also America Online, supra note 10.
\item About 10% of revenues are used to combat spam. See Wylie, supra note 5.
\end{itemize}
dollars spent, unsolicited commercial electronic mail has been highly disruptive to Internet service providers. Networks have experienced delays or have entirely shut down because they have been overwhelmed with unsolicited commercial electronic mail.43

III. USING CALIFORNIA COMMON LAW OF TRESPASS TO CHATTELS

The explosive growth of unsolicited commercial electronic mail and the lack of legislation concerning spam have forced the Internet service providers to turn to the courts for relief. Internet service providers have relied on a cause of action based on trespass to chattel to stop spammers, and at least a few courts have been receptive to the arguments asserted by the Internet service providers.44

The cause of action for trespass to chattels is based on common law.45 California courts adopted the theory of trespass to chattel by citing the works of Professor Prosser and the Restatement of Torts.46 In Zaslow v. Kroenert,47 the California Supreme Court found that intentionally placing another person’s personal property in storage without asserting ownership did not amount to substantial interference to the extent necessary to amount to a conversion.48 However, in finding for the plaintiff, the court cited Professor Prosser and ruled that “[w]here the conduct complained of does not amount to a substantial interference with possession or the right thereto, but consists of intermeddling with or use of or damages to the personal property, the owner has a cause of

43. See David A. Price, Net Heads Are Fed Up with ‘Spam’, INV. BUS. DAILY, Aug. 1, 1997, available in 1997 WL 10709799. “For 18 hours, Internet service provider Concentric Network Corp. couldn’t deliver e-mail to its members. Five CompuServe Corp. mail servers were knocked out of commission, delaying e-mail delivery for two hours. A university mail server was shut down in May...[due to] millions of [unsolicited commercial] e-mail...messages.” Id.
45. See Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996). Trespass to chattel, although seldom employed as a tort theory in California (indeed, there is nary a mention of the tort in Witkin’s Summary of California Law), lies where an intentional interference with the possession of personal property has proximately caused injury. Prosser notes trespass to chattel has evolved considerably from its original common law application...[A]ccording to Prosser, “...there may be recovery...for interferences with the possession of chattels which are 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. Trespass to chattels survives today, in other words, largely as a little brother of conversion.” Id. (citation omitted).
46. See id.
47. 176 P.2d 1 (Cal. 1946).
48. See id. at 7.
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.\textsuperscript{49} Because the California Supreme Court relied on the Restatement of Torts to form the common law cause of action for trespass to chattels, the Restatement should be persuasive authority in analyzing trespass to chattels in California.

"Chattel" is defined as "[a]n article of personal property, as distinguished from real property" and "may refer to animate as well as inanimate property."\textsuperscript{50} The Restatement of Torts states that trespass to a chattel can occur by either "(a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another."\textsuperscript{51} These two types of trespass to chattel place different burdens on the plaintiff to recover damages. If the trespass to the chattel is a dispossession, an "action will lie although there has been no impairment of the condition, quality, or value of the chattel, and no other harm to any interest of the possessor."\textsuperscript{52} However, in an action for intermeddling with the chattel of another without the other’s consent, the intermeddling "must be for a time so substantial that it is possible to estimate the loss caused thereby."\textsuperscript{53}

Of these two types of trespass to chattel, the former does not apply to spamming. Dispossession is defined as an "ouster" or "[a]n act whereby the wrongdoer gets the actual occupation of the land or hereditament."\textsuperscript{54} In a typical spamming incident, the offending party does not actually dispossess the Internet service providers of their network.\textsuperscript{55} However, the act of spamming does intermeddle with the possessory interest in a

\begin{itemize}
  \item \textsuperscript{49} Id.
  \item \textsuperscript{50} BLACK’S LAW DICTIONARY 236 (6th ed. 1990).
  \item \textsuperscript{51} RESTATEMENT (SECOND) OF TORTS § 217 (1965).
  \item \textsuperscript{52} Id. § 218 cmt. d.
  \item \textsuperscript{53} Id. cmt. i.
  \item \textsuperscript{54} BLACK’S LAW DICTIONARY 471 (6th ed. 1990); see also RESTATEMENT (SECOND) OF TORTS § 221 (1965). The Restatement states that:
    \begin{itemize}
      \item \textsuperscript{a} taking a chattel from the possession of another without the other’s consent, or
      \item \textsuperscript{b} obtaining possession of a chattel from another by fraud or duress, or
      \item \textsuperscript{c} barring the possessor’s access to a chattel, or
      \item \textsuperscript{d} destroying a chattel while it is in another’s possession, or
      \item \textsuperscript{e} taking the chattel into the custody of the law.
    \end{itemize}
  \item Id.\textsuperscript{55} Although the spammer may cause Internet service providers considerable damage and delay, the spammer never assumes actual control of the provider’s facilities or network. See generally Price, supra note 43.
\end{itemize}
chattel of the Internet service providers through the unauthorized use of the possessor's network.

In *Thrifty-Tel, Inc. v. Bezenek*, the California Court of Appeal held that the defendant's intermeddling with the plaintiff's computer network by unauthorized electronic signals was sufficient to maintain an action for trespass to chattels. In *Thrifty-Tel*, hackers used computers to get the unauthorized access codes of a telephone company to make free long distance telephone calls. The defendants argued that trespass required a physical touching of another's chattel or entry onto another's land. Although the court recognized that the early common law rule required physical touching, the court stated that "the electronic signals generated by the Bezenek boys' activities were sufficiently tangible to support a trespass cause of action." Therefore, in California, unauthorized intermeddling with a computer network by electronic signals can result in liability based on a cause of action for trespass to chattel.

In determining damages for trespass to chattel by electronic signals, the *Thrifty-Tel* court held that the plaintiff must produce reasonably certain evidence of actual damages caused by the specific intermeddling incident. In that case, the plaintiff did not produce any specific evidence of actual damages caused by the defendants' intermeddling. The plaintiff only produced evidence of hours expended in tracking down the defendants and a statistical average of the cost to fight off hackers per incident. The court ruled that the plaintiff did not meet its burden of proving damages. In California, the plaintiff has the burden of showing that the particular defendant caused particular damage with reasonable certainty in order to recover damages for trespass to chattel.

56. 54 Cal. Rptr. 2d 468 (Ct. App. 1996).
57. Id. at 472-73.
58. Id. at 471.
59. See id. at 473.
60. Id. at 473 n.6.
61. See id. at 475.
62. See id.
63. See id.
64. See id.
65. See id. The court stated:

We know of no authority—and Thrifty-Tel cites none—suggesting a plaintiff may satisfy this burden [of proving damages] merely by producing a formula or figure that in the abstract purports to represent the average damages suffered as a consequence of similar torts. Indeed, to assess damages based on a statistical average might be unfair. For example, the facts here indicate the actual damages resulting from hacking may vary dramatically depending upon the hacker's method. . . . Nor can Thrifty-Tel claim actual damages were not readily calculable: If it is able to determine an average loss for computer trespass, then surely it is able to produce evidence showing with reasonable certainty any damages caused by Ryan and Gerry in November 1991.

Id.
The holding in *CompuServe v. Cyber Promotions, Inc.* is also relevant to the analysis regarding an action for trespass to chattel in California. In *CompuServe*, a federal district court held that an online service provider had established a cause of action for trespass to chattels against a company that had repeatedly sent unsolicited commercial electronic mail to its subscribers even after several requests to stop were made. Cyber Promotions sent millions of unsolicited electronic mail messages to customers of CompuServe, an Internet service provider. CompuServe received numerous complaints from its subscribers about unsolicited commercial electronic mail sent from the defendant. CompuServe instructed Cyber Promotions on several occasions to stop sending spam to its customers, but Cyber Promotions refused to honor this request.

The defendants argued that since CompuServe was not physically dispossessed of its computer system, there was no trespass to chattels. The court rejected the defendants’ argument and followed the *Thrifty-Tel* decision. The court held that intermeddling with electronic signals via computer was a “tangible” trespass by Cyber Promotions and thus interfered with CompuServe’s possessory interest in its computer systems. The court further held that a plaintiff could sustain an action for trespass to chattels without showing that the defendants took physical custody of the network if the plaintiff could show that the defendants intentionally interfered with the plaintiff’s right to possess that chattel. In that case, Cyber Promotions’ refusal to honor the repeated requests by CompuServe was evidence of its intent to trespass.

The cause of action for intermeddling with a chattel in the possession

---

67. See id. CompuServe is one of the leading Internet access providers in the country. Cyber Promotions is one of the leading bulk electronic mail marketing firms. The president of Cyber Promotions, Sanford Wallace, has adopted the name “Spamford” Wallace to the protest of the Hormel Corporation. See *Hormel Objects to Cyber Promotions’ Use of ‘SPAM’ Mark*, supra note 2.
69. See id. at 1018.
70. See id. at 1019.
71. See id. at 1024.
72. See id. at 1020, 1022.
73. See id. at 1021.
74. See id.
75. See id. at 1022.
76. See id. at 1024.

1211
of another requires evidence of actual damages. The defendants in *CompuServe* argued that, even if they did use CompuServe’s network, their use did not result in physical damage or loss of measurable economic harm. The Restatement requires harm to the possessor’s materially valuable interest in the physical condition, quality, or value of the chattel, unless the possessor is deprived of the use for a substantial period of time. The court held that the burden on CompuServe’s computer system to process additional unwanted mail, the cost of trying to return or stop future mail, and the loss of customer goodwill represented sufficient tangible damage. In California, the *Thrifty-Tel* decision is still good law and may require more certainty in proving quantifiable damages.

The *CompuServe* court also rejected the argument made by Cyber Promotions that CompuServe had consented to the trespass by the very act of connecting its network to the Internet. If the possessor has consented to the use of the network, the user has a license to use the chattel within the scope of the consent without liability to the possessor. Cyber Promotions argued that since CompuServe “made the business decision to connect to the Internet,” the connection in effect conferred consent of Cyber Promotions to send information to members connected via the Internet. The analogy used to make the argument was that of a business establishment inviting the public to enter its property for business purposes. Although the court conceded that “there [was] at least a tacit invitation for anyone on the Internet to utilize plaintiff’s computer equipment to send e-mail to its subscribers,” the court emphasized the fact that CompuServe had expressly revoked any implied consent. The withdrawal of consent can make the original lawful use into unlawful intermeddling if the party continues to persist in the use after the termination of the privilege.

---

77. *See id.* at 1022; *see also* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 475 (Ct. App. 1996).
79. *See RESTATEMENT (SECOND) OF TORTS § 218 cmt. d (1965).*
81. *See Thrifty-Tel, Inc.*, 54 Cal. Rptr. 2d at 475.
83. *See RESTATEMENT (SECOND) OF TORTS § 218 cmt. b (1965).*
85. *Id.* at 1023-24. There was a factual dispute as to when notice was given. However, the court pointed to “clear” records that the defendant was eventually notified to not send e-mails to CompuServe subscribers. *See id.* at 1024.
86. *See RESTATEMENT (SECOND) OF TORTS § 217 cmt. f (1965).* “The actor may commit a new trespass by continuing an intermeddling which he has already begun, with or without the consent of the person in possession. Such intermeddling may persist after the other’s consent, originally given, has been terminated.” *Id.*
concluded that Cyber Promotions had exceeded any privilege it might have enjoyed at the onset of the spamming campaign. The court, in dicta, also noted that a published policy statement that limits unauthorized sending of unsolicited commercial electronic mail may not be sufficient to serve as notice.

Finally, the CompuServe court declared that spammers do not have a constitutional right to send spam to subscribers of Internet service providers. The court based its logic on the decision in Cyber Promotions, Inc. v. America Online, Inc. The court in America Online concluded that Cyber Promotions did not have an "unfettered [constitutional] right to send unsolicited e-mail advertisements to subscribers of another private online company over the Internet." Cyber Promotions had argued in that case that they had a constitutional right to send spam to America Online subscribers because America Online essentially assumed the role of the state by being the "postmaster" of the Internet. The court in CompuServe declared, "[T]he constitutional guarantee of free speech is a guarantee only against abridgment by government . . . ." The constitutional protection does not extend to private conduct. In following America Online, the court in CompuServe rejected the argument that the Internet service provider was acting as a quasi-government entity by virtue of the control of the new medium.

First, the court in CompuServe stated that the holding in America Online was that Internet service providers like America Online were "not exercising powers that are traditionally the exclusive prerogative of the state, such as where a private company exercises municipal powers

88. See id. CompuServe had a published policy statement that did not permit sending unsolicited e-mails to its subscribers. See id. The court stated that this notice "may be insufficiently communicated to potential third-party users when it is merely posted at some location on the network. However, in the present case the record indicates that defendants were actually notified that they were using CompuServe's equipment in an unacceptable manner." Id.
89. See id. at 1025-26.
91. Id. at 437.
92. See id. at 442.
94. See id.
95. See id. at 1025-26.
by running a company town." The lack of control was evident in the finding that consumers had many choices among Internet service providers.

Second, the CompuServe court rejected the argument that Cyber Promotions did not have "adequate alternative means of communication available to them." The court noted that Cyber Promotions could "send e-mail advertisements to those on the Internet who do not use CompuServe accounts" and communicate with CompuServe subscribers "through online bulletin boards, web page advertisements, or facsimile transmissions, as well as through more conventional means such as the U.S. mail or telemarketing." The fact that Cyber Promotions may have to bear a prohibitively high cost for sending spam was deemed irrelevant by the court. The court stated that "[t]here is no constitutional requirement that the incremental cost of sending massive quantities of unsolicited advertisements must be borne by the recipients."

The legal victories against the largest and most visible bulk e-mail provider, Cyber Promotions, Inc., have yielded some protection for the Internet service providers against unsolicited commercial e-mail. It has effectively put Cyber Promotions out of business. A recent article declared that, "the Titanic of the junk e-mail business [Cyber Promotions] has just met its iceberg." However, the "cat and mouse" game continues because it is difficult for the Internet service providers to track down the source of unsolicited commercial electronic mail. Also, the sheer number of different spammers has made the task nearly impossible. Finally, even if the Internet service providers could establish a claim based on trespass to chattels, it is difficult to prove

---

96. Id. at 1025.
97. See id.
98. Id. at 1026.
99. Id.
100. Id.
101. Id. at 1026.
102. Id.
103. Spammers often engage in "spoofing" techniques to hide their origin. Therefore, it is difficult if not impossible for Internet service providers to track down the spamming party. See Robins, supra note 29.
104. There are literally millions of spams being sent. See generally Wylie, supra note 5. In fact, AOL says that spam accounts for 30% of their total e-mail activity. See id.
actual damages since the plaintiff must show that a particular defendant caused specific damages.\textsuperscript{105}

IV. UNSOLICITED COMMERCIAL ELECTRONIC MAIL
LEGISLATION IN CALIFORNIA

The frustration felt by Internet users has not been lost on the legislature.\textsuperscript{106} Several states have passed or are considering passing legislation to regulate or ban unsolicited commercial electronic mail.\textsuperscript{107} The Congress of the United States is also considering different variations of anti-spam legislation.\textsuperscript{108}

A. Electronic Mail and the Telephone Consumer Protection Act

The notion of regulating unsolicited commercial advertisements is not entirely new. Congress enacted the Telephone Consumer Protection Act in 1991\textsuperscript{109} in response to "abuses by the telemarketing industry."\textsuperscript{110} This legislation banned the use of any telephone facsimile machine, computer, or other device to send an unsolicited advertisement via a telephone facsimile machine.\textsuperscript{111} Unsolicited fax advertisements are

\textsuperscript{105} California requires particular damages. \textit{See} Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 475 (Ct. App. 1996).

\textsuperscript{106} Interestingly, although most people detest spam and feel that it should be regulated, 74\% of surveyed Internet users felt that the Internet service providers should regulate spam, while only 15\% believed that federal, state, or local government should get involved. \textit{See} GartnerGroup Benchmarks the State of Spam, supra note 3.

\textsuperscript{107} \textit{See} \textit{CAL. BUS. \\& PROF. CODE} § 17538.45 (West 1998 & Supp. 2000). Authors of the bill A.B. No. 1629 were Miller (R) and Cunneen (R); this Bill was read a third time and passed in the State Assembly with 38 Ayes and 0 Noes on August 26, 1998. \textit{See AB 1629 Assembly Bill: History} (visited July 11, 2000) \texttt{<http://www.leginfo.ca.gov/pub/97-98/bill/asm/ab_1601-1650/ab_1629_bill_history.html>}. The bill was approved and signed by Governor Wilson on September 26, 1998. \textit{See id.} Delaware is considering making unsolicited commercial e-mail unlawful unless it has been requested by the recipient. \textit{See} S.B. 138, 140th Gen. Assembly (Del. 1999). Illinois is considering making unsolicited commercial e-mails a Class C misdemeanor. \textit{See} H.B. 2718, 91st Gen. Assembly (Ill. 1999).


\textsuperscript{111} \textit{See} 47 U.S.C. § 227(b)(1)(C) ("It shall be unlawful for any person within the United States . . . to use any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine . . . ").
strikingly similar to spam. Both unsolicited faxes and electronic mails are inconveniences, and both impose a monetary burden on the recipient. One difference is that unsolicited fax advertising ties up the recipient’s fax machine, making it impossible to receive other faxes, while electronic mail does not.

The Telephone Consumer Protection Act of 1991 was most likely not intended to regulate unsolicited commercial e-mail. In defining the term “telephone facsimile machine” to mean “equipment which has the capacity (A) to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or (B) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper,” Congress may have inadvertently included spam in the Telephone Consumer Protection Act. In an ironic twist, an individual sued CompuServe (the Internet service provider that sued Cyber Promotions in CompuServe v. Cyber Promotions, the leading case against unsolicited commercial electronic mail) under the Telephone Consumer Protection Act for two unsolicited electronic mails CompuServe sent to him.

112. See Sorkin, supra note 110, at 1008. The sender of a fax usually pays “for the telephone call to the recipient’s fax machine.” Id. The recipient of a fax generally has to pay for the cost to transfer the digital data into a hard copy. See id. Typically, the costs associated with the transfer include paper, ink or toner, and maintenance of the machines, as well as the cost of maintaining a dedicated telephone line to receive faxes. See id. at 1009. It costs the recipient between 4 and 12 cents to receive one page of fax. See id. at 1010. However, it is much easier to send much larger quantities of unsolicited advertisements by electronic mail than by fax. See id. It is, therefore, much easier to send larger quantities of advertisement at a lower price. Unsolicited commercial electronic mail may place a much greater burden upon recipients than unsolicited fax transmissions because the recipient will get many more electronic mail advertisements. See id. at 1012.

113. See id. at 1011. Unsolicited commercial electronic mails do not have the same problem. Multiple electronic mails can be received simultaneously. See id. However, the recipient’s telephone line may be tied up extensively when one is forced to download unsolicited commercial electronic mails. See id. Further, unlike fax transmissions, spam is typically stored in the disk space of the recipient’s provider of Internet service. Unlike telephone companies, which are directly compensated by the advertiser to carry their advertisement, the Internet service providers are not paid for the use of their network by spammers. See id.

114. See id. at 1012-20.

115. 47 U.S.C. § 227(a)(2) (1994). A personal computer with a standard modem and printer would qualify under the plain meaning of the statute. As a result, some commentators have argued that unsolicited commercial electronic mail is illegal under the Telephone Consumer Protection Act. See Sorkin, supra note 110, at 1013.


117. See Sorkin, supra note 110, at 1002 n.12. Section 227(b)(3)(B) of the TCPA provides for statutory damages of $500 for each violation. Robert Arkow of California filed a small claims action against CompuServe in February 1995 based upon this provision, seeking $1,000 in
A detailed statutory construction of the language and history of the Act, however, suggests that unsolicited electronic mails are not included in the act.118

The Telephone Consumer Protection Act may still be significant in one respect: Congress is now considering various modifications to the act to explicitly include unsolicited commercial electronic mails.

B. California's Statutes on Unsolicited Commercial Electronic Mail

State legislatures have responded to the problem of unsolicited commercial electronic mail with a vengeance; California has adopted two statutes specifically aimed at curbing unsolicited commercial electronic mail.119 Section 17538.4 of the California Business and Professions Code deals with all unsolicited commercial electronic mail,120 and section 17538.45 specifically addresses instances where the registered user of an Internet service provider sends unsolicited commercial electronic mail.121 To understand the law in California regarding unsolicited e-mail, both statutes must be examined.

Section 17538.4 of the California Business and Professions Code regulates the sending of all unsolicited electronic mail.122 The statute defines unsolicited electronic mail as a “document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit”123 where the “initiator does not have an existing business or personal relationship”124 and the “documents are not sent at the request of, or with the express consent of, the recipient.”125 It also requires that all unsolicited advertising material must “include ‘ADV:’ as the first four

---

statutory damages for two unsolicited e-mail advertisements he received from CompuServe, and an additional $1,000 in punitive damages based upon his claim that he had previously notified CompuServe of his desire not to receive such messages. The parties settled under undisclosed terms.

Id. at 1012-16.

118. See id. at 1012-16.


120. Id. § 17538.4.

121. Id. § 17538.45.

122. Id. § 17538.4.

123. Id. § 17538.4(e).

124. Id. § 17538.4(e)(1).

125. Id. § 17538.4(e)(2).
characters” in the subject heading of the electronic mail. In addition, the statute prohibits a person or entity from sending unsolicited electronic mail unless the sender “establishes a toll free telephone number or valid sender operated” electronic mail address so “that the recipient ... may call or [write an electronic mail] notifying the sender not to e-mail any further unsolicited documents.” Notice of the toll number must be the first text attached in the body of the message. Finally, “upon notification by a recipient of his or her request not to receive any further unsolicited” electronic mail, the sender must not cause to be sent any unsolicited electronic mail to that recipient. Violation of this section is a misdemeanor.

Section 17538.45 of the California Business and Professions Code regulates the sending of all unsolicited electronic mail. Electronic mail advertisement is defined as “any electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient.” It prohibits registered users from sending unsolicited commercial electronic mail to a recipient with whom he does not have an existing business or personal relationship and when it is not sent at the request of or with the express consent of the recipient. The new law also allows Internet service providers to recover the greater of the actual monetary loss suffered by the violation of the statute or $50 in “liquidated damages” for each mail message initiated, with a maximum of $25,000, so long as the defendant had notice of the Internet service provider’s policy barring electronic mail advertising. Also, the spam must have actually used the electronic mail service provider’s equipment located in California.

126. Id. § 17538.4(g).
127. Id. § 17538.4(a)(2).
128. See id. § 17538.4(b).
129. Id. § 17538.4(c).
130. See id. § 17538(f); see also CAL. PENAL CODE § 19 (West 1999) (stating that the punishment for a misdemeanor is six months in county jail, $1000, or both).
131. CAL. BUS. & PROF. CODE § 17538.45.
132. Id. § 17538.45(a)(1).
133. The statute makes a distinction between registered and non-registered users. See id. § 17538.45(a)(5). Registered users are defined as “any individual, corporation, or other entity that maintains [an account] with an electronic mail service provider.” Id.
134. See id. § 17538.45.
135. See id. § 17538.9(f)(1).
136. See id. § 17538.9(f)(3)(A).
137. See id. § 17538.45(f).
V. ANALYSIS OF CALIFORNIA'S STATUTES ON UNSOLICITED COMMERCIAL ELECTRONIC MAIL

Sections 17538.4 and 17538.45 of the California Business and Professions Code clearly affect the sending of unsolicited commercial electronic mail.\textsuperscript{138} Depending upon whether one is a recipient or an Internet service provider and whether there is a contractual relationship between the parties, the remedies and causes of action can be significantly different. The statutes also significantly change the consequences of sending unsolicited commercial electronic mail.

A. Where Sender Does Not Have a Contractual Relationship with the Internet Service Provider

One significant aspect of section 17538.4 of the California Business and Professions Code is that it imposes several duties on the sender of unsolicited commercial electronic mail, such as requiring the sender to identify the nature of the mail in the subject heading and to clearly identify the sender with a toll free number or return address.\textsuperscript{139} One impact of compliance with the subject heading requirement will be to alert the recipient that they are receiving unsolicited commercial electronic mail.\textsuperscript{140} A direct consequence of requiring the sender to clearly identify a return address is that it prohibits employing “spoofing” techniques to hide one’s address.\textsuperscript{141}

However, section 17538.4 fails to resolve many of the problems associated with unsolicited commercial electronic mail. First, it does not prevent the initial harm suffered by the recipient and requires active effort by the recipient to be taken off the list.\textsuperscript{142} Second, even if the

\textsuperscript{138} Id. §§ 17538.4, 17538.45.
\textsuperscript{139} See id. § 17538.4(b).
\textsuperscript{140} Of course, this assumes that people will eventually learn of its significance.
\textsuperscript{141} Currently, these spoofing techniques can prohibit the recipient from knowing the origin of the electronic mail. See Robins, supra note 29.
\textsuperscript{142} Many of the new electronic mail retrieval programs come with built-in screening software to block unsolicited electronic mail. For example, Microsoft Outlook Express 4 and 5 have features that allow the user to block the receipt of mail from a particular sender or with a particular subject. See Bedell, supra note 11. However, it is unclear that a typical Internet user knows of the availability of this feature. Further, it is likely that non-savvy computer users may require technical assistance to program the software to effectively block out unsolicited electronic mail. For those that are using older versions of electronic mail retrieval software, they may be required to purchase or download a free version of the latest software with spam blocking features. Even the
recipient notifies the sender, it does not guarantee that the recipient will no longer receive unsolicited commercial electronic mail. This section also does not protect the rights of Internet service providers who suffer damages and may actually be in the best position to stop unsolicited commercial electronic mail. Finally, the statute fails to supply a strong civil remedy for Internet users.

Section 17538.4 has a limited impact because it does not prevent the initial harm suffered by the recipient and requires an active effort by the recipient to be taken off the list. The economic cost of sorting through and deleting unsolicited commercial electronic mail is significant. Although requiring the use of “ADV:” in the subject heading may reduce the time it takes to identify the spam, the recipient will still be forced to download the mail before he or she can delete the file. Further, placing the burden on the recipient to identify the spam and to call a toll free number or write a reply letter to the sender could add to the loss in productivity when dealing with unsolicited commercial electronic mail.

Notification by the sender does not guarantee that the recipient will no longer receive unsolicited commercial electronic mail. Even if all spammers comply with section 17538.4, it would mean that the notification would only remove the recipient from the mailing list of a particular sender. There are literally tens of thousands of different mailers selling tens of thousands of products employing spam. It is therefore possible to reply to hundreds of items of unsolicited commercial electronic mail and still get more spam. Further, many spammers currently exploit the recipient’s request to be taken off a mailing list by sending more unsolicited commercial electronic mail to the recipient. Therefore, many recipients receiving unwanted electronic mail may follow the advice of spam experts and not reply at

wide availability and use of screening software by users do not shift the cost of spam from the recipient to the sender. The time and cost of learning of the availability of the software, using the software, and possibly purchasing and downloading new software are all borne by Internet users rather than the spamming party.

143. See Brown, supra note 12.
144. CAL. BUS. & PROF. CODE § 17538.4(g).
145. This assumes that the recipient is not using screening software to block out unsolicited commercial electronic mail.
146. See generally Brown, supra note 12 (discussing economic consequences of spam).
147. See generally Bedell, supra note 11 (discussing some negative ramifications of battering spammers). There are several organizations, such as www.spamfree.org, www.junkbusters.com, and www.cauce.org that will assist consumers in getting their name removed from mass mailing lists. While these organizations can assist consumers, compliance with those requests is only voluntary. See Stanley A. Miller II, Taking Aim at Spam, MILWAUKEE J. SENTINEL, May 11, 1999, at 1M.
148. See Bedell, supra note 11.
Additionally, section 17538.4 does not protect the rights of Internet service providers who also suffer damages and who may actually be in the best position to stop unsolicited commercial electronic mail. The Internet service providers have a right to prevent unauthorized access to their network by spammers. Also, section 17528.4 creates no additional remedies for Internet service providers. The legislation explicitly imposes an affirmative duty on the recipient to notify the sender to be taken off the mailing list. While it can be argued that the Internet service providers are also “recipients” or agents of the recipients and, therefore, have the power to give notice to the spamming party, the construction of the statute strongly suggests that the legislature only intended to grant individual recipients a remedy.

First, the statute identifies the recipient’s notice as “his or her request” suggesting that the request be made by an individual rather than an entity. Second, the statute specifically refers to the role of the Internet service provider as “merely carry[ying the] transmission over its network” suggesting that the Internet service provider is not the recipient of the mail. Third, the right of Internet service providers to limit spamming activity by registered users is expressly listed in section 17538.45 but is not mentioned in section 17538.4 for non-registered users. Finally, section 17538.5 specifically allows employers to notify the sender of unsolicited commercial electronic mail on behalf of all its employees but does not mention similar rights for Internet service providers.

The Internet service provider is in the best position to stop unsolicited commercial electronic mail. As a carrier of electronic data, the Internet service provider would have access to the unsolicited electronic mail before the individual recipient, thus giving it an ability to delete the file first. It also has greater capability and resources to detect unsolicited electronic mail. The addition of “ADV:” in the subject heading would make it easier for the Internet service providers to screen out unsolicited junk mail, but an unwary individual recipient may not be informed of the

149. See id.
152. See CAL. BUS. & PROF. CODE § 17538.4(b).
153. Id. § 17538.4(c).
154. Id. § 17538.4(f).
155. Id. § 17538.4(h).
significance of the "ADV:" heading. Also, giving Internet service providers the ability to notify the sender on behalf of individual recipients would be a more efficient means of stopping unsolicited electronic mail. For example, if one spammer sends one million unsolicited commercial electronic mails to individual recipients, the statute would require that one million people respond and give notice to the spammer to take them off the particular mailing list. If the Internet service provider had the power to give notice, it could send one reply on behalf of the million subscribers. Finally, the Internet service providers have more financial resources than the typical subscriber to seek legal recourse for any violation of the statute.\[156\]

Finally, the statute fails to supply strong penalties for violations of section 17538.4. Violation of any provision of section 17538.4 is a misdemeanor punishable by imprisonment in the county jail not exceeding six months, by a fine not exceeding $1000, or by both imprisonment and fine.\[157\] Making the violation a misdemeanor does not preclude civil remedies.\[158\]

The penalty for the violation seems to have been "watered down." Historical notes indicate that the original statute would have made the act of continuing to send unsolicited electronic mail after notification "punishable by a fine of $500 for each and every transmission."\[159\] The original statute would have had a stronger deterrent effect in that each and every transmission would have multiplied the penalty, thus giving the spammer a stronger economic incentive not to violate the law. The legislation also does not give individual recipients or the Internet service providers a statutory basis for recovering punitive damages from spammers for violations.

### B. Where Sender Does Have a Contractual Relationship with the Internet Service Provider

Section 17538.45 of the California Business and Professions Code deals with Internet service providers' rights and remedies against "unsolicited electronic mail advertisements [sent] by registered user[s]."\[160\] Registered users are those that maintain a contractual

---

156. This is assuming that, since Internet service providers are businesses, they generally have greater resources than the typical individual subscriber.

157. See CAL. BUS. & PROF. CODE § 17538(f); see also CAL. PENAL CODE § 19 (West 1999) (describing the punishment for a misdemeanor).

158. See CAL. BUS. & PROF. CODE § 17534.5.

159. Id. § 17538.4, Historical and Statutory Notes, 1998 Legislation, 17538.4(d) (West Supp. 2000); see also CAL. PENAL CODE § 19 (West 1999) (describing the punishment for a misdemeanor).

relationship with the Internet service provider. Registered users sending unsolicited commercial electronic mail must, therefore, comply with both section 17538.4 and section 17835.45.

Internet service providers are granted several rights under section 17835.45. The most significant of these rights is the ability to seek civil "liquidated damages" from the registered users. The liquidated damages provision is significant because it changes the common law as well as the statutory law governing contracts.

Legislative history indicates that the liquidated damages clause was intended to make it easier to satisfy the particular damage requirement of the common law. The author of the California spam legislation claims, "that courts around the country have recognized that ISP's [Internet service providers] have a cognizable property interest in their equipment and service" but that "existing legal remedies for ISP's to control the use of their network are inadequate because it is virtually impossible for them to calculate their actual losses or damages from mass-distributed unsolicited e-mail ads."

California courts have consistently limited plaintiffs' recovery on a cause of action based on trespass to chattel to the specific and particular harm caused by the defendant. Unlike other torts, such as conversion, which require substantial deprivation of the possessory interest in the chattel, an action for trespass to chattel can be maintained for intentional intermeddling of the chattel. For example, if a person steals an owner's car, the owner can sue on conversion because the owner is substantially deprived of the use of his possessory interest in the car. However, if a person intentionally brushes a car, the owner may not have a claim based on conversion because the person did not substantially deprive the owner of his possession or use of the car.

The owner may have a remedy for trespass to chattel, however, because the person intentionally interfered with his chattel. Unlike conversion, measuring damages for trespass to chattel is more uncertain and can result in a windfall for the plaintiff. California courts are, therefore, reluctant to grant damages for trespass to chattel absent proof that the defendant caused specific and particular harm to the plaintiff.

161. See id. § 17538.45(5).
162. See id. § 17538.45(1).
163. Electronic Mail: Hearing on AB 1629 Before the Senate Floor (Cal. 1998) (California Committee Analysis) [hereinafter Electronic Mail].
164. See Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996)
165. See id. at 475.
even if the acts of the defendant were fraudulent or illegal. A showing of statistical evidence or hours spent on tracking down the particular defendant is not enough to show damages.

Section 17538.45 of the California Business and Professions Code changes the common law by disposing of the particularity of damages requirement. The statute now provides:

In addition to any other action available under law, any [Internet service provider]... may bring a civil action to recover the actual monetary loss suffered by that provider by reason of that violation, or liquidated damages of $50 for each electronic mail message initiated or delivered in violation of this section, up to a maximum of $25,000 per day, whichever amount is greater.

Therefore, it greatly reduces the burden on the Internet service providers to prove civil damages and increases the likelihood of recovery in suits that would have been difficult, if not impossible, to win under the common law.

For example, assume that a registered user of a particular Internet service provider sends one hundred random unsolicited commercial electronic mails to subscribers of that Internet service provider in the hope of selling widgets. Under the common law, the Internet service provider will have to prove that the additional one hundred electronic mails caused particular damage to the Internet service provider. Proving damages would be difficult because the quantity of mail was so negligible that it would be hard to prove specific and particular damages as a result of the one hundred electronic mails. Even under the more relaxed CompuServe standard, it would be difficult to prove damages as a result of loss of “goodwill” by the individual subscribers.

Section 17538.45 also arbitrarily discriminates between registered and non-registered users. The requirement of a “registered” user determines the ability to gain statutory damages, whereas the common law does not. The Internet service provider would be able to recover damages from the registered user even if the unsolicited electronic mail is sent to non-

166. See id.
167. See id.
169. Id. § 17538.45(f)(1).
170. See Thrifty-Tel, Inc., 54 Cal. Rptr. 2d at 475.
171. See generally Electronic Mail, supra note 163.
172. CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997). Assume that none of the one hundred recipients who received the electronic mail complained or switched Internet service providers. See id. at 1027 (“Defendants’ intentional use of plaintiff’s proprietary computer equipment exceeds plaintiff’s consent and, indeed, continued after repeated demands that defendants cease.” (emphasis added)).
subscribers of the Internet service provider. In order to have a claim against the registered user, the statute only requires that the registered user be notified of its policy against unsolicited commercial electronic mail and that the registered user “use or cause to be used that electronic mail service provider’s equipment” located in this state.\(^{7}\)

For example, say that a registered user of X Internet service provider sends one hundred unsolicited electronic mails advertising widgets to one hundred subscribers of Y Internet service provider. Assume that X Internet service provider cannot attribute a particular harm to the one hundred additional electronic mails because the volume is so low. Assume also that Y Internet service provider receives several complaints about the electronic mail. Under section 17538.45 of the California Business and Professions Code, X Internet service provider may seek $5000 in damages, whereas Y would not have a statutory basis to recover damages from the spammer because he is not a registered user. Registered users are defined as “any individual, corporation, or other entity that maintains an electronic mail address with an electronic mail service provider.”\(^{7}\) Since the spammer does not maintain an electronic mail address with Y Internet service provider, the Y Internet service provider will have to rely on the common law and must prove actual and particular damages. The results are different from the common law because the statutory damages may not be in proportion to actual damages. In this example, Y Internet service provider may have suffered greater damages than X Internet service provider, but satisfying the registered user requirement may mean that X Internet service provider may ultimately recover more in damages.

The liquidated damages provision is also significant because it changes the statutory law governing the law of contracts. Section 17538.45 seems to give Internet service providers damages that they would otherwise not be able to get from subscribers under pre-existing California contract law. Under section 1671 of the California Civil Code, “a provision in a contract liquidating the damages for the breach of the contract is valid unless the party seeking to invalidate the provision establishes that the provision was unreasonable under the circumstances existing at the time the contract was made.”\(^{15}\) It also states that the “section does not apply in any case where another statute

---

173. CAL. BUS. & PROF. CODE § 17538.45(b).
174. CAL. BUS. & PROF. CODE § 17538.45(a)(5).
175. CAL. CIV. CODE § 1671(b) (West 1985).
expressly ... prescribes ... liquidating the damages for the breach of the contract.” Therefore, section 17538.45 of the California Business and Professions Code escapes the usual limitations on liquidated damages under section 1671 of the California Civil Code, because section 17538.45 expressly prescribes liquidated damages.

First and foremost, in order for the liquidated damages to survive judicial scrutiny under section 1671 of the California Civil Code, there has to be a contract specifying liquidated damages. Section 1671 specifically refers to a “provision in a contract” for liquidated damages. Black's Law Dictionary defines liquidated damages as “the sum which [a] party to [a] contract agrees to pay if he breaks some promise and, which having been arrived at by good faith effort to estimate actual damage that will probably ensue from breach, is recoverable as agreed damages if breach occurs.”

Section 17538.45 of the California Business and Professions Code allows for recovery of $50 in liquidated damages without the requirement that the registered user expressly promise to pay the liquidated damages in case of a breach. Internet service providers may be entitled to liquidated damages if they prove that they notified the registered user of their general policy against spamming and that the registered user in fact sent unsolicited commercial electronic mail in violation of that policy. There is no requirement that the Internet service provider modify the contract with the registered user to reflect the liquidated damages provision since the liquidated damages are statutory.

The liquidated damages provision would probably not survive the challenge that it was unreasonable under the circumstances existing at the time the contract was made. In Aetna Casualty & Surety Co. v. Board of Trustees, the California Court of Appeal cited section 1671 of the California Civil Code and ruled that “[l]iquidated damages are a penalty not favored in equity and should be enforced only after he who seeks to enforce them has shown that he has strictly complied with the contractual requisite to such enforcement.”

In Greenbach Brothers, Inc., v. Burns, the California Court of Appeal examined the difference between invalid penalty clauses and liquidated damages provisions by examining the proportion of the

176. Id. § 1671(a).
177. See id. § 1671(b).
178. See id.
181. 35 Cal. Rptr. 765 (Ct. App. 1963).
182. Id. at 767 (emphasis omitted).
183. 54 Cal. Rptr. 143 (Ct. App. 1966).
money in relation to actual damages. The court noted that what “distinguishes a provision for liquidated damages from one that is in the nature of a penalty” is that the “characteristic feature of a penalty is its lack of any proportionate relation to actual damages that may arise upon breach.”

Even assuming that Internet service providers include the $50 damages in all new contracts, the figure seems excessive and unreasonable. The $50 minimum statutory damage award per offending electronic mail message does not mirror the actual damages suffered by the Internet service provider. In the hypothetical described in Part V.A regarding one hundred unsolicited electronic mails to sell widgets, the Internet service provider could hardly argue that it suffered $5000 in damages. Actual damages suffered by Internet service providers are real and significant. However, $50 per offending electronic mail does not bear a proportionate relation to actual damages that may arise upon breach. If we assume that unsolicited electronic mail totals 10% of all electronic mail sent, then there are approximately 80.3 trillion unsolicited commercial electronic mail messages sent yearly.

In order to justify the $50 in liquidated damages per electronic mail, the Internet service industry must somehow come close to suffering $4.015 quadrillion a year in losses attributable to spam activity. Of course, this figure is not proportional to the actual loss suffered by the industry. America Online, the largest Internet service provider, has a total market valuation of a little over $162 billion. The Internet service providers themselves attribute the total cost borne by the industry at about 10% of revenues.

184. See id. at 147.
185. Id.
186. Assume that a registered user of X Internet service provider sends one hundred unsolicited electronic mail messages advertising widgets to one hundred subscribers of Y Internet service provider. X Internet service provider cannot attribute a particular harm to the one hundred additional electronic mails because the volume is so low. Assume also that Y Internet service provider receives several complaints about the electronic mail.
187. See Wylie, supra note 5.
188. See Stroh, supra note 6.
190. See Wylie, supra note 5.
VI. PROPOSED REVISION OF THE CALIFORNIA STATUTES

The economic damage suffered by both the recipients and the Internet service providers as a result of unsolicited commercial electronic mail is significant. For recipients and Internet service providers to bear the cost of receiving unwanted mail is against public policy and should be remedied. The common law may not be well suited or adequate to deal with the problem because it demands that the plaintiff prove a particularized damage, whereas the Internet service providers can show only cumulative damages as a result of unsolicited electronic mail. California's two statutes dealing with the problem of unsolicited commercial electronic mail also fall short of relieving the problem. First, the statutes tolerate the vast majority of unsolicited commercial electronic mail. For example, the statutes would have had no bearing on CompuServe's suit against Cyber Promotions had the statute been in effect at that time because the parties were not in privity of contract. These two statutes seem to have been drawn hastily as interim measures to deal with unsolicited commercial electronic mail until federal legislation is enacted. This may partly explain why the statutes seem unable to effectively promote the public policy of reducing unwanted spam and to discriminate fairly between senders of spam.

In analyzing California's statutes regulating unsolicited commercial electronic mail, the following revisions should further the public policy goals of minimizing the harm caused as a result of receiving unsolicited commercial electronic mail and getting rid of unnecessary and unfair discrimination between registered and non-registered senders of spam. First, section 17538.4 of the California Business and Professions Code should allow Internet service providers, with the consent of the registered recipient, to give notice to the sender on behalf of the recipient of unsolicited commercial electronic mail. In the alternative, the law could prohibit any unsolicited commercial electronic mail without a prior business or professional relationship or without express

191. See id.
194. See id. at 1028.
195. See CAL. BUS. & PROF. CODE § 17538.4. The statute specifically states that it will become inoperative as soon as a federal law is enacted. See id. § 17538.4(i) (Supp. 2000). Due to the limited scope of this Comment, the discussion of possible constitutional issues arising out of the interstate commerce clause has been intentionally excluded. See generally David T. Bartels, Recent Legislation, Canning Spam: California Bans Unsolicited Commercial E-mail, 30 McGeorge L. Rev. 420 (1999) (discussing constitutional issues).
consent of the recipient similar to the federal anti-fax legislation. Second, civil punitive damages should be available to both the recipient and the Internet service provider for violations of the statute. Finally, section 17538.45 of the California Business and Professions Code should be repealed.

The biggest problem with section 17538.4 of the California Business and Professions Code is that it tolerates the vast majority of unwanted and unsolicited electronic mail and places the burden of being removed from the mailing list on the recipient. For example, the statute would do little to address the problem involved in *CompuServe v. Cyber Promotions*.196 In that case, Cyber Promotions sent out huge volumes of unsolicited electronic mail to subscribers of CompuServe.197 Several subscribers responded to Cyber Promotions directly, but millions of unsolicited electronic mail messages were sent and would continue to be sent unless all of the individual subscribers individually requested that they be removed.198 By granting CompuServe the right to notify Cyber Promotions under the statute, millions of repetitive and unnecessary electronic mail messages notifying the sender would not be necessary. CompuServe should be required to get consent of the subscribers, but this can be readily accomplished with a revision of their service agreement.

In the alternative, the statute should prohibit any unsolicited commercial electronic mail without a prior business or professional relationship or without express consent of the recipient, as was done with unsolicited electronic faxes by federal law.199 This revision would basically put the same prohibition imposed on registered users on non-registered users. The benefit of the second approach is that it will reduce the multiple spammer problem. For example, if there are ten thousand spammers sending out one million electronic mail messages to the same subscribers of an Internet service provider, the first suggested revision approach would require that the Internet service provider send out ten thousand notices. The flat prohibition on unsolicited commercial electronic mail would avoid the burden of the notice requirement on the Internet service provider. However, the burdens of receiving unsolicited

---

196. 962 F. Supp. 1015. Cyber Promotions received notice only from CompuServe rather than from millions of individual subscribers. See id. at 1017. Also, Cyber Promotions did not have a contractual relationship with CompuServe. See id.

197. See id. at 1017.

198. See id. at 1023.

The legislature should consider whether a complete ban would be preferred over a severe restriction on this emerging technology.

The second revision to the statute should be to allow civil punitive damages for both the recipient and the Internet service provider. The Thrifty-Tel requirement of proving a particular harm by a particular act of the defendant may be difficult if not impossible to prove. The legislature imprudently watered down the original language of the statute and eliminated the $500 in penalties per transmission. Since both the recipient and the Internet service provider suffer the harm or damage, and the damage is difficult to prove for both parties, the statute should be revised both to compensate the victims and to deter sending unsolicited commercial electronic mail in violation of the statute.

Finally, section 17538.45 of the California Business and Professions Code should be repealed. The legislature intended the legislation to allow easier compensation for Internet service providers. However, it probably will not deter prolific spammers, such as Cyber Promotions, and would be unfair to unsuspecting registered users who may engage in some commerce that the legislature may not have intended to prohibit. Prolific spammers can avoid paying any liquidated damages so long as they do not send unsolicited electronic mail to the same subscribers of their own Internet service provider. For example, if they want to target the largest Internet service provider, America Online, they merely have to sign up with a different Internet service provider and escape the statutory liquidated damages. Discriminating in this fashion is neither warranted nor effective. It also seems unfair to impose the liquidated damages provision to a contract without mentioning the damages and

200. See supra notes 112-13 and accompanying text.
202. See id.
204. Although the current statute offers some deterrence against the sending of spam with a misdemeanor penalty, it offers no easy vehicle for victims to seek damages.
205. See Electronic Mail, supra note 163.
206. A consumer sending a few electronic mail messages to members of a discussion group may be liable to Internet service providers. For example, a person trying to sell an airplane ticket that he cannot use may decide to send a few electronic mails to a discussion group about European travel.
207. All the spamming party must do is not be a registered user of a particular Internet service provider. See CAL. BUS. & PROF. CODE § 17538.45(a)(5) (West 1997 & Supp. 2000).
208. See Jespersen, supra note 189.
without the consent of both parties. The legislature should dispense with the liquidated damages language and impose statutory penalties for sending unsolicited commercial electronic mail.

If the legislature incorporates these recommendations, it will accomplish the goal of minimizing the harm caused by unsolicited commercial electronic mail to both consumers and Internet service providers by decreasing or eliminating unsolicited commercial electronic mail. The suggested punitive damages should also provide an effective remedy to deter senders, and compensate victims, of unsolicited commercial electronic mail. While the growth and emergence of the Internet and electronic mail should not be hindered by legislation, the shifting of costs and burdens onto consumers and Internet service providers by aggressive marketers should not be tolerated.

CALVIN WHANG

209. There is no requirement that the Internet service provider notify the registered user of the statutory liquidated damages amount. See CAL. BUS. & PROF. CODE § 17538.45.