

Unsolicited Communications as Trespass?

Attempting to stretch existing laws to address previously unforeseen technological issues.

Rare is the person who wants to receive unsolicited commercial email (aka spam). Unsolicited noncommercial email is often equally unwelcome. Due to a growing consensus that technology alone cannot solve the unsolicited email problem, various legal approaches to regulating unsolicited email have been proposed or adopted.

The most successful legal strategy thus far has been litigation challenging mass mailings of unsolicited email as a “trespass” to the recipient’s servers. Little objection arose when Internet service providers won lawsuits based on this theory against spammers who sent tens of millions of email messages to ISP subscribers and consumed voluminous server disk space.

Decisions in favor of ISPs in these cases required some stretching of trespass law because the harms caused by spam differ significantly from harms this old law was designed to deal with. These decisions have emboldened others to try to stretch trespass

law further in challenges to other unauthorized accesses of publicly accessible Internet sites and other unsolicited email.

The key question these cases

raise how far property rights should extend on the Internet. Some stretching of trespass law may be appropriate (for example, to stop spam from impeding the functioning of Internet servers), but if trespass law was construed so broadly that it was necessary to get advance permission from the

owner of a computer system before communicating with it or those having accounts with that owner at the risk of being held liable for trespass, trespass law would seem to be stretched too far.

An important case involving an unwanted email as trespass claim is *Intel v. Hamidi*, which the California Supreme Court decided in June 2003. In this case, the California Supreme Court accepted previous decisions upholding trespass claims against massive mailings of commercial email. But it decided that meaningful harm to a computer system must be shown before such a trespass claim can succeed. The California court recognized that stretching trespass law to stop unwanted but harmless email could interfere with free speech and other socially valuable interests. This decision brings much needed balance to the law of trespass as applied to the Internet. Although only California courts are bound to follow the *Hamidi* decision, the sound reasoning of the California decision will hopefully deter frivolous computer trespass

Legally Speaking

cases from being filed elsewhere and persuade other courts to reach the same legal conclusions.

Intel v. Hamidi

Ken Hamidi is a former Intel engineer who in 1995, with others, formed an organization known as Former and Current Employees of Intel (FACE-Intel) to share critical information about Intel's employment and personnel practices.¹ On behalf of FACE-Intel, Hamidi sent six

efforts were only partly successful because Hamidi sent email from different computer systems in order to evade blocking by Intel. In March 1998, Intel demanded that Hamidi stop sending email to Intel computers. Hamidi claimed he and FACE-Intel had a right to communicate with Intel employees who had not asked to be removed from the email distribution list. After Hamidi sent another mass mailing in September 1998, Intel sued him in a Cal-

ifornia state court for unlawful trespass on Intel computers. A trial judge ruled in favor of Intel and ordered Hamidi to stop sending email to Intel computer systems. A divided Court of Appeal affirmed this ruling. In June 2003, a divided California Supreme Court by a 4-3 vote reversed and ruled in favor of Hamidi.

no harm to the land. Legal liability for trespass does not depend on the trespasser's bad motives. For example, trespassing on another's land is just as illegal when the intruder's purpose is to distribute leaflets praising (or criticizing) the company that owns the land as when the intruder's motives are to break into an owner's home. Another less well-known legal rule forbids trespass to chattel. (Chattel is an old English word for cattle, which has come to be a

Trespass to chattel law has attained a new significance because of numerous successful lawsuits relying upon it to challenge unauthorized uses of computer systems.

ifornia state court for unlawful trespass on Intel computers. A trial judge ruled in favor of Intel and ordered Hamidi to stop sending email to Intel computer systems. A divided Court of Appeal affirmed this ruling. In June 2003, a divided California Supreme Court by a 4-3 vote reversed and ruled in favor of Hamidi.

email messages to thousands of Intel employees over approximately a two-year period. These messages criticized Intel's practices and policies as abusive, encouraged recipients to join FACE-Intel, and suggested that Intel employees should find other employment. The email also informed recipients they could be removed from the FACE-Intel mailing list if they wished to do so, and Hamidi honored such requests.

Senior Intel officials quickly became aware of Hamidi's email messages and tried to employ technical measures to block further email from Hamidi. These

Trespass to Chattel

It may not be obvious to *Communications* readers why sending unwanted email could conceivably be illegal trespass, since trespass is a concept typically associated with land. An owner who objects to another's presence on his or her land can sue the trespasser and get an injunction to stop further trespass, even if the intrusion caused

generic legal term for items of personal property, such as books, desks, cars, and computers.) Trespass to chattel is like trespass to land in that it allows property owners to challenge unwanted interferences with their property. However, trespass to chattel law requires proof of some intentional intermeddling with the chattel and some cognizable harm to the chattel, for example, to its physical condition, quality, or value. If, for example, I jump on your car in order to annoy you and this dents the car, you can sue me for trespass to chattel and a court is likely to order me to pay the cost of fixing the dent. Harmless intermeddling with a chattel, such as sitting on someone else's car without denting it, annoying though it may be, is not illegal.

¹At the time this column was written (late summer), Hamidi was one of a group of candidates running for the governor of California in the recall election.

Until very recently, trespass to chattel was a little-known and rarely used legal rule. Indeed, for centuries, nothing interesting or noteworthy had occurred in this minor niche of the law. Trespass to chattel law has, however, attained a new significance because of numerous successful lawsuits relying upon it to challenge unauthorized uses of computer systems. This trend started with legal challenges to spamming and spread to challenges to robotic Web crawlers and then to unwanted email such as what Hamidi sent to Intel employees.

Spam as Trespass

There are many reasons why ISPs want to stop unsolicited commercial email. Their subscribers typically dislike receiving spam, are likely to complain about it, and may even unsubscribe if these services cannot stop, or at least significantly reduce, the amount of spam that arrives in subscriber inboxes. ISPs must expend considerable resources to develop or license technology to block spam. The high volume of spam sent via the Internet consumes valuable server space and can slow functioning of ISP services.

Notwithstanding the development and deployment of ever-improved anti-spam technologies, unsolicited commercial email continues to flow through the Internet in alarmingly large quantities. In the hope of deterring spam, a number of states in the U.S., including California and Washington, as well as a number

of other countries around the world, have enacted anti-spam laws. Some of these laws require subject lines of email headers to indicate the mail is an advertisement; some forbid false or misleading point of origin and transmission information; and some require spam email messages to contain accurate opt-out information. (An excellent resource about anti-spam laws can be found at www.spamlaws.com/us.html.) Consumer protection authorities may also be able to challenge some spam activities under false advertising or unfair trade practice laws.

Because anti-spam laws are neither ubiquitous nor uniform—and because these laws typically do not forbid the sending of spam, but only regulate some aspects of sending unsolicited email—ISPs have initiated lawsuits under common law rules, such as those forbidding trespass to chattel, hoping to get a court to order spammers to stop sending unsolicited commercial email.

CompuServe, for example, won a trespass to chattel lawsuit in 1997 against Cyber Promotions, which had sent tens of millions of unsolicited commercial email messages to CompuServe customers. CompuServe alleged many kinds of injuries from Cyber Promotions' spamming, including lost customer revenues, costs of dealing with customer complaints, expenditure of resources trying to block Cyber Promotions' mailings, and sub-

stantial clogging of server disk space and processing power owing to the extremely large number of messages Cyber Promotions had sent to CompuServe customers. Of these, the impairment of server processing power seemed the most plausible as a harm to CompuServe's "chattel" (that is, its servers) within the traditional purview of trespass to chattel law. AOL and other ISPs brought similar suits successfully challenging spamming as trespass to chattel.

eBay v. Bidder's Edge

The success of these ISP trespass to chattel claims against spammers spurred further challenges to unwanted uses of Internet-accessible servers on the same legal theory. eBay, for example, successfully sued Bidder's Edge for trespass to chattel because Bidder's Edge robots were visiting eBay's auction Web site 100,000 times a day to collect updated information about prices for which specific items were selling on eBay so that users of its auction information aggregation Web site would have comparative price information to aid their auction bidding.

eBay, like CompuServe, asserted that its expenditure of considerable resources to block the intruder's unwelcome actions was evidence of harm arising from the trespass. It also argued that unless the court enjoined Bidder's Edge from sending robots to eBay's site, other auction information aggregators

Legally Speaking

would follow the example of Bidder's Edge. While the Bidder's Edge robots had not yet caused harm to the operation of eBay's servers, the proliferation of unlicensed robots on the eBay site would, eBay argued, cause a significant diminishment in server responsiveness akin to that established in *CompuServe v. Cyber Promotions*. The trial judge in *eBay v. Bidder's Edge* was persuaded by eBay's argument, and issued a preliminary injunction against Bidder's Edge as to further deployment of robots to search for auction information on the eBay site.

The *eBay v. Bidder's Edge* decision was controversial for several reasons. It not only loosened the showing of harm necessary to establish a viable claim for trespass to chattel, but at one point in the opinion, the judge indicated that unauthorized uses of eBay servers could be challenged as trespass insofar as they "deprived eBay of the ability to use that portion of its personal property for its own purposes." The law, said the judge, "recognizes no such right to use another's personal property." Although Bidder's Edge appealed the preliminary injunction ruling, eBay and Bidder's Edge settled the lawsuit while the case was on appeal, leaving the lower court ruling intact and giving firms such as Intel reason to think they too could enjoin unwanted intrusions on their servers.

Intel's Property Rights Theory
Intel relied heavily on the power

of the property rights metaphor in its lawsuit against Hamidi. It emphasized the millions of dollars it expended in developing and maintaining its computer systems as a property interest that should be protected. Intel developed its computer systems "not to act as a public forum [for speakers such as Hamidi] but to enhance the productivity of its employees," said the three judges in the *Hamidi* case who would have ruled in Intel's favor. They agreed with Intel that "[t]he time required to review and delete Hamidi's messages diverted employees from productive tasks and undermined the utility of the computer system." This constituted, in their view, an unlawful interference with Intel's property rights. Ruling in favor of Hamidi would force Intel to use its own property to advance Hamidi's messages.

Respect for property rights helps to explain why the U.S. Supreme Court has repeatedly ruled that individuals are not required on free speech grounds to welcome unwanted speech into their homes, whether from a door-to-door solicitor, postal mail, radio waves, or amplified sounds. *Rowan v. U.S. Postal Service*, for example, established the right of an individual to order the postal service to stop delivery of unwanted mail (free newspapers) to his home, even though the publisher claimed a free speech interest in being able to use the postal system to reach its intended audience. The same principle

applies to organizations. In *Loving v. Boren*, the Supreme Court upheld the right of the University of Oklahoma to bar pornographic materials from its computer system, again relying in part on the university's property rights in the system. According to the dissenters in *Hamidi*, these cases establish that "[a] private property owner may choose to exclude unwanted mail for any reason, including its content." Hamidi's free speech interests could be exercised by maintaining a Web site for FACE-Intel, but Hamidi had no right to use Intel's property to deliver his message.

Why Harm Matters

Property rights are, of course, vitally important, but they are not the only issue in a trespass to chattel case. Trespass to chattel law doesn't just require unwanted use of another's property, but also some showing of harm. Authoritative sources on trespass to chattel law indicate the harm must be to the chattel itself.

The California Supreme Court majority opinion in *Hamidi* pointed out "[t]he consequential economic damage Intel claims to have suffered, i.e., the loss of productivity caused by employees reading and reacting to Hamidi's messages and company efforts to block the messages, is not an injury to the company's interest in its computers—which worked as intended and were unharmed by the communications—any more than the personal distress caused by reading an unpleasant

letter would be an injury to the recipient's mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient's telephone equipment." Intel had, in the majority's view, not suffered a kind of injury trespass to chattel law was meant to redress.

But this was not the end of the California Supreme Court's inquiry. The court went on to consider whether trespass to chattel law ought to be extended to encompass the kinds of harms

of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other employees and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable."

The California Supreme Court recognized that extending trespass to chattel law as far as Intel

brief in support of Hamidi's appeal pointed out, mean that "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they might want to communicate and anyone who owns a server through which their message might travel." This would substantially reduce freedom of communications over the Internet—even unwanted linking could be a trespass according to this theory.

Although creating an absolute

Intel v. Hamidi is not the first case, nor will it be the last, in which courts have been asked to stretch existing property law to respond to challenges posed by digital technologies.

Intel claimed against Hamidi and whether the law should dispense with the harm requirement altogether in cyberspace trespass cases.

The Court was reluctant to do the former in part because it recognized that Intel employees were not distracted from their work because of the quantity of email sent by Hamidi, but rather because of the content of the email, that is, by the statements and opinions Hamidi expressed in these messages. The contents upset some employees and caused discussion among employees and between employees and their supervisors. The California Supreme Court majority observed that "Intel connected its email system to the Internet and permitted its employees to make use

wanted would create a precedent under which virtually any unsolicited communication could be challenged as a trespass insofar its contents were unwelcome by the recipient (an Intel employee) or the intermediate transmitter (Intel) by "fictionally recharacterizing the allegedly injurious effect of a communication's contents on recipients as an impairment to the device which transmitted the message." Fictions of this sort, the *Hamidi* majority concluded, "promise more confusion than clarity in the law."

The California Supreme Court was even more reluctant to rule that unsolicited communications could be challenged as trespass without any showing of harm. This would, as a law professor

property right might force spammers to internalize the costs they now impose on users and ISPs, the California Supreme Court decided this rule "might also create substantial new costs, to email and e-commerce users and to society generally in lost ease and openness of communications and in lost network benefits." In view of this, the California Supreme Court declined to eliminate the harm requirement in trespass to server cases.

Conclusion

Intel v. Hamidi is not the first case, nor will it be the last, in which courts have been asked to stretch existing property law to respond to challenges posed by digital technologies.

Legally Speaking

Fifteen years ago, Apple Computer and Lotus Development Corp. asked courts to extend copyright law to protect the “look and feel” of computer software, but the courts rejected broad “look and feel” claims as a distortion of copyright law.

Ten years ago, MAI asked the courts to rule that unlicensed persons infringed its computer program copyrights when they turned on computers to repair them because temporary copies of licensed computer programs were made in the random access memory of computers. Although it was a stretch of copyright law to do this, a federal appellate court in California agreed with MAI’s aggressive theory.

Five years ago, aggressive trademark owners asked courts to rule that registering a domain name of a famous trademark (commonly known as cybersquatting) infringed these trademarks. When serious questions arose about the consistency of cybersquatting rulings with existing trademark law, legislation was enacted to make cybersquatting illegal.

These examples illustrate that courts sometimes stretch existing law in order to apply it to an unforeseen technology issue, and sometimes they don’t. Sometimes also the appropriate venue for stretching the law is a legislature rather than a court. Trespass to chattel law as applied to Internet communications is undergoing a similar refinement process.

Spammers will not find any comfort in the California Supreme Court opinion in *Intel v. Hamidi*. The California court

made clear that ISPs would continue to be able to use trespass to chattel law to stop unsolicited commercial email messages sent in sufficient quantities that they impair a computer system’s functioning. The same rule would apply to noncommercial email that impairs computer system operations. The court in *Hamidi* did not directly endorse the *eBay* theory of threatened harm to a computer system if others did the same as the defendant, although it did not criticize this theory either.

The *Hamidi* decision did, however, question whether trespass claims could be based on other kinds of harm (for example, harm to a firm’s reputation). It clarified that trespass can’t be based on harm arising from the recipient’s reaction to the contents of the communication. The California court also rejected the position that the owner of a computer system has an inviolable right to control access to and use of a computer system connected to the Internet. Extending trespass law that far would impair too many socially desirable uses of the Internet. The *Hamidi* decision is a significant victory for those who use the Internet to communicate. **C**

PAMELA SAMUELSON

(pam@sims.berkeley.edu) is a Chancellor’s Professor of Law and Information Management at the University of California at Berkeley.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

© 2003 ACM 0002-0782/03/1000 \$5.00