By Robert J. Aalberts, Percy Poon, and Paul Thistle

**Trespass, Nuisance, and Spam: 11th Century Common Law Meets the Internet**

Even in the instantaneous world of cyberspace, common law still provides a protective shield over many Internet problems.

The English common law legal system has succeeded and thrived for over 900 years due to its functional and adaptive nature. This article will explore how the common law’s old but still practicable doctrines are being applied to problems on the Internet and where it will likely evolve. In particular, we will examine the viability of two common law actions—trespass to chattels and nuisance.

*Illustration by Paul Wiley*
The old common law judges were very successful in managing conflict. They listened to those who were aggrieved and then hammered out a sensible solution. The solutions they applied would later become the common law doctrines we use today. Although these judges were appointed to advance the King’s interests, their ideas have endured and have generally survived Constitutional scrutiny in the U.S. These same doctrines will likely solve many of the Internet’s most dangerous threats. The Internet is, if anything, a new, conflicted frontier that is in a constant state of flux. The common law came into being as a system to do precisely what we are trying to do today in pacifying the Internet—manage a threatening adversary in a new and hostile environment.

The common law’s flexibility offers a number of advantages for managing cyberspace. The common law reacts faster, but has often performed more competently than legislatures, especially in coping with unpredictable threats posed by new and rapidly developing technologies. Legislative bodies, such as Congress, move slowly, are affected by special interests and reluctant to address politically sensitive issues. The laws they produce are often too narrow in some areas, yet too vague in others.

Statutes can take years to decipher and often yield unintended consequences. Courts are able to intervene and apply well-settled, centuries old rules of law such as trespass to chattels and nuisance to modern factual situations as cases arise. Moreover, state judges today are generally elected and so must be sensitive to the needs of their electorate. Thus, judges are in the unique position of protecting the public’s interests while at the same time possessing the flexibility to quickly resolve some of our most vexing technological problems while state legislatures can codify, modify, or reject the common law after the fact. Just as importantly, the structure of the common law provides the benefits of learning from the past while guiding us in the future. One of the bases of the common law is the doctrine of *stare decisis*, or deciding cases by adhering to precedent on questions of law. This principal allows courts to provide certainty, fairness, and predictability for those who are seeking their guidance. A judge can overrule established precedent, but must be prepared to articulate compelling reasons for doing so. Overruling precedent, in the words of Chief Justice of the Supreme Court John Roberts, inflicts a “jolt” on the legal system.

**Common Law Actions and the Internet**

In recent years, the common law has been applied to protect Internet users from a variety of threats and intrusions. We first discuss one very old common law action—trespass to chattels—and explain its present legal utility in managing the Internet. Then we turn to another venerable common law action—nuisance. One important doctrinal development concerning the applicability of trespass to chattels and nuisance to the Internet will also be presented to demonstrate the dynamic and flexible nature of the common law. In the end, we will reveal how the common law can offer some protection for combating certain Internet problems in the present and the future.

**Trespass to Chattels.** The common law action of trespass to chattels was created centuries ago to battle those who were carrying off another’s personal property. Today it encompasses all direct interferences with another’s personal property [6]. Trespass to chattels requires intentional non-trivial physical contact or use of another’s personal property that is the prox-
imate cause of actual harm.

For years trespass to chattels was overshadowed by conversion, which afforded better monetary relief. The Internet, however, has spawned a legal renaissance for this long-ignored action. The efficacy of trespass to chattels in combating Internet incursions was foreshadowed in the 1996 case *Thrifty-Tel, Inc. v. Bezenek*. In *Thrifty-Tel*, the defendants were accused of phreaking—the practice of cracking a phone network, usually to make free long-distance calls. Since existing state or federal statutes did not address phreaking, the court was forced to rely on the common law. Importantly, the court ruled that the flow of electrons was sufficiently tangible to constitute physical contact, a required element of a trespass to chattels.

One year later, in *CompuServe, Inc. v. Cyber Promotions, Inc.*, an Ohio court applied the same logic to spammers for the first time. The court argued that science now allows us to quantify gases, shockwaves, and particulates. Furthermore, the court stated, the electronic messages sent by Cyber Promotions caused harm to CompuServe because the “multitudinous electronic mailing demand the disk space and drain the processing power of plaintiff’s computer equipment. This, in turn, caused “the value of that equipment to CompuServe [to be] diminished even though it is not physically damaged by defendants’ actions.”
The same logic was later applied in other cases, notably *Register.com v. Verio* ¹ and *eBay v. Bidders Edge*.²

Trespass to chattels, however, hit a jurisprudential detour a few years later. The dynamic that unfolded further shows how the common law can adapt to solve the complexities of the cyberworld. In the now famous case of *Intel Corp. v. Hamidi*, a disgruntled Intel ex-employee sent out, in a two-year period, over 30,000 inflammatory and uncomplimentary email messages about Intel to Intel employees. Hamidi’s behavior, while troublesome, did not reach the point where he could be prosecuted under existing statutes. He did not breach computer security barriers and obligingly removed recipients from his mailing list. His barrage of email also did not cause physical damage or a disruption of Intel’s computer system. Employees were not kept from using their computers. But his email sparked a swell of watercooler talk, setting off productivity and morale issues at Intel. Apparently Hamidi’s email struck a nerve at the chip giant. Intel, arguing trespass to chattels, sought, and was initially granted, an injunction barring Hamidi from sending further email messages to Intel employees.

Before the final decision was issued, some worried that trespass to chattels, especially after the *eBay* and *CompuServe* rulings, might be going too far. As Burk [1] points out, Intel’s email system worked exactly as intended. The important characteristic of Hamidi’s email, and of spam more generally, is that the recipient finds the content of the message undesirable. Trespass to chattels was being transformed into a general right to deter any message the recipient decides is unwanted. How chilling would it be to Internet activity if anyone who sends out information that any recipient thinks is spam, could be sued? These kinds of questions were taken seriously in the *Hamidi* decision and lead the California Supreme Court to overturn the injunction against Hamidi.

**Will Nuisance Emerge As A Viable Action in Internet Law?**

What the *Hamidi* case apparently triggered is a repositioning of the common law concerning a trespass to chattels and the future emergence of the common law action of nuisance as a legal weapon. Under California’s common law, trespass to chattels requires a showing of actual damage to Intel’s servers, such as slowing it down or causing a quantifiable loss of system capacity. This did not occur in the *Hamidi* case.

The narrowing of trespass to chattels has only opened up the action of nuisance as another means for solving Internet woes. Interestingly enough, it was the *Hamidi* court that helped this process along. Nuisance is also a very old common law action. It is invoked when one landowner unreasonably interferes with the use and enjoyment of another’s land. Unlike a trespass, it does not require an actual physical invasion. Invisible incursions, like foul smells, fumes, and electromagnetic energy, can constitute a nuisance.

**Weighing the Burdens versus the Benefits**

Possibly the greatest contribution that nuisance may offer is a method for determining fair outcomes. Nuisance requires a balancing of the extent of the harm caused versus its social utility to determine whether it is reasonable to outlaw a purported nuisance. As one economic commentator explains: “Unreasonableness alternatively may exist if the activity is meritorious, but the defendant fails properly to internalize the costs of his activity, thereby imposing a negative externality on society in addition to whatever social utility his activity provides” [3].

---

¹Defendant Verio, Inc. and plaintiff Register.com were competitors in providing Web site development services. Verio used a search robot to access plaintiff’s system for its customer list, then sent confusing advertisements to Register.com’s customers to lure them away. The court ruled in Register.com’s favor that Verio “could interfere with Register.com’s use of its own systems and issue an injunction ordering Verio to cease its activities.”

²Bidders’ Edge, the defendant, provided information to its customers on the price of items on online auctions. It employed search “spiders” to penetrate or “screen scrape” eBay’s Web site thousands of times a day to collect information. The court ruled that this encroachment, as well as the potential of many more, would result in the degradation of the plaintiff’s system.
The Hamidi court strongly hinted that a burden/benefit approach may be the best way to counter the various injurious Internet activities, especially those difficult to quantify. For example, the Hamidi court noted that “Creating an absolute property right to exclude undesired communications from one’s email and Web servers might help force spammers to internalize the costs they impose on ISPs and their customers. But such a property rule might also create substantial new costs to email and e-commerce users and to society in general, in lost ease and openness of communication, and in lost network benefits.” For these reasons, a case-by-case analysis applying such a test is likely the best method for making these determinations.

O’Rourke [5], discussing unauthorized access to Web sites (for example, deep-linking, unauthorized spidering), suggests a balancing test that is essentially the same as nuisance. While we cannot predict the outcome of any particular case, we can provide some “back-of-the-envelope” calculations of the benefits and burdens of spam. The 2004 National Technology Readiness Survey (NTRS) [7] estimates that in 2004 each of the 170 million adults online received an average of 18.5 spam email messages per day, or 1.15 trillion spam email. Sipior, Ward, and Bonner [9] report that approximately 76 billion spam email were sent in January 2004, or 912 billion per year. This suggests that one trillion messages is a reasonable estimate of the amount of spam sent during 2004. Goodman and Roundthwaite [2] report that spammers charge between 0.00125 and 0.1 cents per message to send spam; their discussion suggests 0.03 cent as a reasonable estimate of the cost per message. These numbers imply that $300 million is a reasonable approximation to the cost of sending spam in 2004, although the figure could be as low as $12.5 million or as high as $1 billion. The NTRS also reports that recipients of spam spend an average of three minutes per day dealing with spam. This adds up to 1.19 billion hours, which, valued at the average U.S. wage, means dealing with spam cost $21.6 billion in 2004. This yields an approximate cost of spam of $21.9 billion for 2004.5

In order for an activity to be a nuisance, the costs of the activity must outweigh the benefits. Spam provides some benefits since some recipients do respond to it. The NTRS reports that 4.7 million adults purchased a product or service advertised in a spam email message. If the subjective value these individuals place on their purchases is large enough, then it may outweigh the cost of spam. This would require the individuals to value the purchases they made at $4,659 per person. Respect for consumer sovereignty implies we cannot claim these individuals are incorrect in how they value the goods and services they bought. However, we think that $4,659 will strike most readers as a very high value to put on access to pornographic Web sites, refinance offers, and credit counseling offers that comprise the majority of spam. This figure seems even higher if we consider the large proportion of spam designed to defraud the respondent.

**SPAM AND ELECTRONIC NUISANCE**

Although nuisance has not yet been directly applied to spam, it could provide us with some legal protection. While it has been traditionally tied to invasions to real property, nuisance has already been successfully invoked in at least two cases: one involving a series of unwanted and intrusive phones calls and another when someone caused another to have electronic disturbances to his TV reception, suggesting that interference with personal property located in a house can be a nuisance to its inhabitants [4]. Thus, expanding the doctrine to intrusions to computers in homes and businesses is a reasonable and foreseeable doctrinal extension. Since courts have already ruled that the flow of electrons is sufficiently tangible to constitute physical contact, these invisible incursions could also be deemed a nuisance.

As discussed, nuisance employs a burden/benefit framework to determine its social utility. Spam insinuates itself into unwanted places with offers to sell unwanted goods and services with virtually no cost or risk to the sender and may even threaten the visited site’s quality and existence.6 Its benefit, of course, is

---

5This estimate is conservative, since it does not include expenditures by ISPs to manage spam or expenditures by consumers on spam-blocking software. The 2005/2006 NTRS [8] did not collect data on the incidence of spam.

6The federal statute CAN-SPAM, passed in 2003, appears to have had little success in combating spam in general. The law still allows unsolicited, non-fraudulent spam, although a recipient can opt-out of receiving legal spam. Many, however, do not expend the often time-consuming effort that opting out entails. The act also doesn’t allow private enforcement. CAN-SPAM, however, does allow states to regulate fraudulent spam as well as broader laws that are not specific to email, but regulate cyberspace in general. The reconciliation of state laws with CAN-SPAM is still a gray area, but commentators are suggesting that much state statutory and common law are likely to be viable. For more information, see R.D. Ford’s  “Preemption of State Spam Laws by the Federal CAN-SPAM Act,” University of Chicago Law Review 72 (2005) 358–382.
The common law action of nuisance is more likely to lead to reasonable outcomes in Internet law. The most important benefit of nuisance is that it offers a method for determining fair outcomes by balancing the costs of the activity against the potential social benefits.

CONCLUSION
The common law action of trespass to chattels has been applied to protect ISPs, and indirectly their customers, from the costs incurred by encroaching spiders and robots. However, the expansion of what was considered damage was transforming trespass to chattels into a more general right to deter any electronic contact the recipient deemed undesirable. A general right to deter unwanted contact, that is, to protect one’s real and tangible personal property, has important benefits in physical space. Still, the Internet is not the same as physical space. In particular, the network externalities that are a dominant feature of the Internet are much less important in real property. Thus, a general right to deter unwanted contact is likely to have unwanted negative consequences in cyberspace. This possibility of unintended and unwanted negative consequences was recognized by the Hamidi court.

The common law action of nuisance is more likely to lead to reasonable outcomes in Internet law. The most important benefit of nuisance is that it offers a method for determining fair outcomes by balancing the costs of the activity against the potential social benefits. The fact that the social benefits are considered in the equation means the detrimental effects on networks can be taken into account. In the end, we all benefit by providing private parties with this legal weapon. The costs to spammers will be internalized, requiring them to self-regulate in order to ensure their existence. Our calculations, while clearly a rough approximation, suggest the cost of spam will almost certainly outweigh any benefits it provides. The courts should decide (like most of us have already) that spam is a nuisance.

REFERENCES

Robert J. Aalberts (Robert.Aalberts@unlv.edu) is the Lied Professor of Legal Studies at the University of Nevada, Las Vegas.
Percy S. Poon (Percy.Poon@unlv.edu) is an associate professor and chair of the finance department at the University of Nevada, Las Vegas.

Paul D. Thistle (Paul.Thistle@unlv.edu) is a professor in the finance department at the University of Nevada, Las Vegas.

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.

© 2007 ACM 0001-0782/07/1200 $5.00