The Common Law and Its Impact on the Internet

ROBERT AALBERTS

Department of Finance, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, Nevada 89154, USA

DAVID HAMES

Department of Management, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, Nevada 89154, USA

PERCY POON

Department of Finance, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, Nevada 89154, USA

PAUL D. THISTLE

Department of Finance, University of Nevada, Las Vegas, 4505 Maryland Parkway, Las Vegas, Nevada 89154, USA

Abstract

This chapter begins with a discussion of the English common law, the basis for much of American law today, and its evolving role in regulating the cyberworld. The common law, based on case precedents, has proven to be very adept at resolving new and difficult problems, at times more quickly and competently than legislation. This same mechanism is being used today to solve problems to protect Internet users from destructive "cyberevils" such as spamming and other kinds of cybertorts. In the second part of our chapter, we contrast the cases of *Doe v. XYC Co.* and *Delfino v. Agilent* to illustrate the application of common law doctrines in managing risks arising from employees' use of the Internet.

ISSN: 0065-2458/DOI: 10.1016/S0065-2458(09)01208-X

1. Introduction

When the Normans invaded England in 1066 AD, the bow and arrow was the most high-tech hardware they possessed. Still, the Normans leveraged this technology to vanquish its Anglo-Saxon enemy and impose a new legal regime called the common law. Today, we look to the same system to provide us with both a sword and a shield to thwart spam, adware, spyware, and other enemies lurking in a dangerous virtual world.

Still, how can such an ancient legal system offer protections in a nonphysical world the Normans could never have imagined? The common law legal system was devised in the eleventh century in an environment of great fear and repression. Few rules were in place. Yet, it has survived for many centuries and has evolved into arguably the most practical, adaptive, and functional legal system the world has ever seen. Indeed, in a seminal study by LaPorta et al. [1], in which they examined 49 countries with both common law and civil law legal systems, the authors concluded that the flexibility afforded by the common law, which uses independent judges and juries and applies law on a case-by-case basis, creates an environment in which there

are stronger property rights, less corruption, and more efficiency.[1] Moreover, the common law's flexibility, versus the rigidity of statutory and regulatory law used exclusively in the civil law system, is measurably better at creating new rules for protecting investors and other stakeholders.

The common law's importance in protecting activities on the Internet cannot be understated. The Internet is one of the greatest innovations and generators of wealth the world has ever seen. However, to be truly effective it cannot function properly in a lawless environment. Property rights need to be protected or the incentives necessary for the creation of wealth will be undermined. The common law has proven for centuries that it is up to the challenge.

This chapter will first explore how and why this thousand-year-old legal system has risen to such towering accomplishments and where it will likely evolve in its new role of protecting the cyberworld. The second part will discuss a case study concerning the liability of employers for the wrongful acts of their employees on the Internet at work. The aim of this section is to demonstrate how the courts applying the common law of two states, New Jersey and California, met the challenge. The lesson that was learned from these two cases is that the common law creates rights and duties that the users of the Internet must understand to protect their personal and property interests.

1.1 A Brief Primer on the Common Law

The common law's foundation was based on a very simple but inspired premise. After the successful invasion of England, a succession of Norman kings sent their most trusted administrators, later called judges, out into the shires or counties of the newly vanquished English realm. Here, they were instructed to set up a system to manage and pacify this new but very hostile frontier.

The judges quickly learned that pursuing a peaceful approach to settling disputes could avoid bloody uprisings and conflicts. They discovered that the local Anglo-Saxon inhabitants, in many cases, already possessed customs and common sense solutions that they could successfully draw upon to solve many local problems as well as to placate those who may pose a threat to them in the future.

Indeed, today much like the approach used by the old common law judges, the idea of listening first to those who are aggrieved and then hammering out a solution based on evolving common law principles has and will continue to solve many of the

[1] In the civil law system, legislation is primary source of law and courts base their decisions on provisions of the relevant codes and/or statutes. The civil law system is used in continental Europe and much of Latin America, East Asia, and Africa. In the common law system, cases have traditionally been the primary source of law and courts base their decisions on prior case law. The common law system tends to be used in countries, like the U.S., whose legal traditions originated in Great Britain.

Internet's most dangerous threats. After all, the Internet is, if anything, a new frontier marked by conflict and in a constant state of change. The more devious inhabitants of cyberspace (hackers, spammers, etc.), much like the local and hostile Anglo-Saxons of the eleventh century, are not only clever and destructive, but can regroup and strike quickly. 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 and hostile adversary in a new, albeit nonspatial, environment called cyberspace.

The common law's flexibility offers a number of advantages for managing cyberspace. The judge-made, common law can, in many instances, not only react faster, but has often performed historically more competently than legislatures. This has especially been the case in confronting the unpredictable threats posed by new technologies. Legislative bodies, such as Congress, are slow and often riddled with special interests. As a result, these elective bodies are reluctant to address issues that are too politically sensitive or are overly influenced by special interests. Moreover, the laws they produce, in the form of statutes and codes, are often narrow, as well as vague. Statutes can take years to decipher and often yield unintended consequences. Courts, on the other hand, are able to intervene and apply well-settled, centuries-old rules of law (i.e., trespass, nuisance, etc.) to the specific facts arising in modern conflicts. This allows courts the flexibility of adapting long-standing and well- understood legal principles to the many new problems created by modern technological developments.

The structure of the common law can also bestow the benefits of learning from the past while constructing a better-managed future. This key attribute can help guide the Internet. One of the bases of the common law is the deference given to precedents. Once a precedent is established other judges generally must, because of the doctrine of *stare decisis*, apply these precedents. Indeed, the common law has enjoyed widespread credibility and functionality due to its strong adherence to *stare decisis*. Courts are able to impart certainty, fairness, and predictability upon those who are seeking their guidance. Of course, judges can overrule established precedent. But if they do, they must be prepared to articulate compelling socioeconomic, political, or technological reasons. Overruling precedent, in the words of Chief Justice of the Supreme Court John Roberts during his confirmation hearings, inflicts a "jolt" on the legal system [2]. Tradition and practicality dictate an almost sacred respect for this venerable doctrine.

1.2 Common Law Actions and the Internet

In recent years, the common law has protected Internet users from a variety of threats and intrusions often originating from the broad sweep of tort law.[2] We will begin by discussing one very old common law action in tort called trespass to chattels

[2] A tort is defined by West's Legal Dictionary as "A civil wrong (other than a breach of contract) that has caused harm to person or property."

and then explain its present legal utility to managing the Internet. After that, we will 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. To this end, our chapter will hopefully reveal how the common law will, in a number of key instances, offer some of the protections for combating the Internet problems of the future.

1.2.1 Trespass to Chattels

The common law action of trespass to chattels[3] was created centuries ago to battle those who were transporting or carrying off another's personal property. Often, this was a farmer's livestock—hence the word chattel, the Norman French word for cattle. Today, it encompasses all direct interferences with another's personal property [3].

For years, trespass to chattels was overshadowed by its more popular legal brother—conversion[4]—which often afforded better monetary relief. The Internet, however, has spawned a legal renaissance for this long ignored action. As one commentator notes: "[Trespass to chattels is] a centuries-old. . .theory that languished for years in the dusty archives of obscure legal doctrine learned and then promptly forgotten in the first year of law school, which has unexpectedly found new life courtesy of the Internet" [4].

The efficacy of trespass to chattels in combating Internet incursions was signaled in a 1996 case titled *Thrifty-Tel, Inc. v. Bezenek* [5]. In *Thrifty-Tel*, the defendants were accused of "phreaking"—the practice of cracking a phone network, usually as a way of making free long-distance calls. Since existing state or federal statutes did not, at least at that time, 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.

The significance of *Thrifty-Tel* cannot be understated. Just 1 year later, in *CompuServe, Inc. v. Cyber Promotions, Inc.* [6], an Ohio court followed the same logic but applied it for the first time to spammers. The court argued that science now afforded the opportunity to quantify what was, in the past, not possible. This includes gases, shockwaves, and particulates. Furthermore, the electronic message sent through CompuServe's ISP by Cyber Promotions caused harm to CompuServe's ISP because

[3] Trespass to chattels is defined by West's Legal Dictionary as a "Tort with the following elements (a) personal property-Chattel, (b) plaintiff is in possession of the chattel or is entitled to immediate possession, (c) intent to dispossess or to intermeddle with the chattel, (d) dispossession, impairment, or deprivation of use for a substantial time, (e) causation of the dispossession, impairment, or deprivation."

[4] Conversion is defined by West's Legal Dictionary as the "unauthorized exercise of dominion or control over someone's personal property (chattel)."

the "multitudinous electronic mailing" demands the disk space and drains 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" [7].

Possibly the most important trespass to chattels case involving the Internet was *eBay v. Bidder's Edge, Inc.* [8]. In *eBay* the defendant Bidder's Edge infiltrated eBay's Web site with search "spiders" which "screen scraped" eBay's Web site and placed the information on its own Web site. eBay argued that Bidder's Edge caused its Web site to lose the use of a section of its computer space and therefore its efficiency. This, it claimed, constituted a trespass to chattels. Although Bidder's Edge scraped a relatively small load of 1.53% off of eBay's listing servers, the court maintained that if its actions were not stopped, more companies would do the same. In the aggregate, the court argued, "eBay would be brought to its knees by what would be then a debilitating load" [8]. Trespass to chattels, however, hit a jurisprudential detour a few years later. While some may view this as a weakness, the dynamic that unfolded further showed how adaptive the common law can be as it solves the complexities of the cyberworld. In the now famous case of *Intel Corp. v. Hamidi* [9], a disgruntled Intel ex-employee sent out, over a 2-year period, in excess of 30,000 inflammatory and uncomplimentary emails about his former employer to Intel employees. Hamidi's behavior, while troublesome, did not reach the point where he could be prosecuted under existing statutes. He did not, for example, breach computer security barriers. When asked, he obligingly removed recipients from his mailing list. His barrage of emails also did not cause physical damage or a disruption of Intel's computer system nor were employees kept from using their computers. The havoc that Hamidi wreaked was more pedestrian. His emails sparked a swell of water cooler talk setting off productivity and morale issues at Intel. Apparently Hamidi's email struck some sensitive nerves at the chip giant.

What the *Hamidi* case did trigger legally, however, 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 that there must be a showing of actual damage to Intel's servers, such as slowing it down or causing a loss of a quantifiable amount of its system. This, as stated, did not occur in the *Hamidi* case.

1.2.2 Will Nuisance Emerge as a Viable Action in Internet Law?

The outcome of the *Hamidi* case was not completely unanticipated, at least by legal scholars and commentators. Before the decision was issued, some worried that trespass to chattels, especially after the *eBay* and *CompuServe* rulings, might be traveling in an

unreasonable and dangerous direction. For example, 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. Undoubtedly, other courts felt the same need for an alternative action.

The early, but decidedly savvy common law lawyers were, if anything, able to seek out alternative methods for solving their clients' troubles. They were some of the earliest practitioners of arguing fine distinctions and analogies for advancing their cases. Times have not changed. 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 has helped this process along.

Nuisance, like trespass to chattels, 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.[5] Unlike a trespass, however, it does not require an actual physical invasion. Invisible incursions, like foul smells, fumes, and electromagnetic energy, can constitute a nuisance.

Possibly the greatest contribution that nuisance may offer the Internet is a method for determining fair outcomes. Nuisance requires a balancing of the extent of the harm caused versus its social utility as a means to determine whether it is reasonable to outlaw a purported nuisance. Or 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" [10].

The *Hamidi* court consistently hinted that a burden/benefit approach may be the best way to counter the various injurious Internet activities—especially those that cannot be quantified. For example, the 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 impost 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 generally, in lost ease and openness of communication and in lost network benefits" [9]. For these reason, a case-by-case analysis is likely the best method for making these determinations.

1.2.3 The Future of Pop-up Ads, Spyware, and Adware

Pop-up ads are quite possibly the most irritating features we face on the Internet. Can trespass to chattels or nuisance take on these annoyances? One argument is that pop-ups, including those embedded on our hard drives by spyware and adware, can

[5] Nuisance is defined by West's Legal Dictionary as the "an unreasonable interference with the use and enjoyment of land."

slow down a system or even cause a computer to crash. This could occur, for example, when a user's project takes up most of his computer's processing power, memory, and hard drive space only to be lost by the uninvited arrival of pop-ups, not to mention spiders, Webcrawlers, and robots. In such a case, valuable data would be lost if the system crashes. However, such an outcome is probably rare. Thus, nuisance may be a better bet.

1.2.4 Spam and Electronic Nuisance

Although nuisance has not been directly applied to spam, it could likely provide computer users with legal protection. And even though 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. Thus, interference with personal property located in, say, a house can be a nuisance to its inhabitants. Expanding the doctrine to computers in homes is a foreseeable extension.

As discussed, nuisance employs a burden/benefit framework to determine its social utility. Assuming that spam is defined as illegitimate commercial solicitations, spam received over time can be not only highly annoying, but is often used to sell fraudulent products and services. Moreover, it may even threaten the proper functioning of a system as well as individual computers. Its benefit, of course, is economic. Spam helps unscrupulous individuals make huge amounts of money—a decidedly small amount of social utility.[6]

1.3 The Common Law Versus Statutes

State and federal legislative bodies have, of course, addressed some of these Internet evils. There can be problems with statutes, however. Statutes are typically created to target a specific problem raised by special interest groups ranging from corporations to consumer protection groups and then brought to the attention of lawmakers. A good example of this is Congress' 2003 CAN-SPAM Act. The Act outlaws unsolicited commercial email sent by illegitimate marketers. However, it has been criticized as ineffective for several reasons. First, a private person cannot

[6] Based on data from the National Technology Readiness Survey [11], Aalberts, Poon, and Thistle [12] estimate the cost of the approximately one trillion spam emails sent in 2004 at $22 billion. This includes the cost of sending spam and the value of time spent dealing with spam. Since 4.7 million adults purchased a product or service advertised in spam emails, they would have to value their purchases at over $4600 per person in order for the benefits of spam to outweigh the cost.

use it; only the FTC, state authorities and ISPs can. Second, it preempts similar state laws, some of which were in place and were stronger and arguably better. Lastly, Congress, for whatever political reason, furnished spammers with an enormous break by incorporating an opt-out provision which implies consent to receive spam unless the recipient states otherwise. Of course, the task of opting out of thousands of spam messages can be, if anything, daunting. In addition, the act of opting out verifies that the email address is valid and active, which almost certainly leads to even more spam in the future. Apparently, Congress, with perhaps the exception of well-heeled lobbyists, does not normally listen as well as a judge might to those who have something valuable to offer.

2. The Common Law in Action: Employer Liability to Third-Party Victims on the Internet

To demonstrate the common law's importance for settling ongoing disputes that arise in cyberspace we present two quite recent cases, one from New Jersey, *Doe v. XYC Co*. [13] and the other, *Delfino v. Agilent Technologies, Inc*. [14] from California. These cases reveal the increasing importance of managing employees properly in their use of the Internet and both concern well-settled common law principles that have been applied to resolve disputes occurring in the physical realm for centuries.

2.1 A Study in Failure to Protect Third Parties: The XYC Corp.

Most ISP supervisors are aware they possess legal *rights* to monitor employee Internet use. Laws, such as the federal Electronic Communications Protection Act and others, generally allow employers great leeway to monitor [15]. Yet, as mentioned, statutes can only go so far, often lacking the flexibility to react to unique but important disputes that may arise both in the physical and cyber realm. One such development arose in a 2005 New Jersey decision, *Doe v XYC Corp*. This case created a legal *duty* to monitor workers properly and reasonably in order to protect third parties. The case, the first of its kind, has subsequently sent shockwaves as well as garnered support throughout both the legal and business communities [16].

The compelling facts in *Doe* portend just how far-reaching the case and the duty it created may become. XYC's problems began when employees lodged complaints concerning a fellow employee, Doe, who was apparently accessing and viewing pornographic sites on his company computer. To verify the information, the company's Senior Network Administrator (SNA) checked Doe's computer logs

revealing sites with highly suspicious names such as "bestiality" and "necrophilia." Sensing an obvious legal and moral problem looming, the SNA confronted Doe and ordered him to stop visiting "inappropriate sites." Doe, however, continued to disobey the order. Sensing his lack of cooperation, the SNA and Doe's immediate supervisor continued to probe and found evidence of similar sites. In response the SNA went directly to the Director of the Network and PC Services (the Director) requesting an investigation. At this point, the Director made a significant mistake. Instead of investigating the allegations, she "admonished" the SNA and told him never to access any employee's Internet activity in the future. In fact, the SNA was told that violations of this policy could result in his job loss. Doe, unaware of his supervisor's latest discovery, continued to access the illicit sites. Ironically, the company also had a second Internet use policy that allowed the accessing and review of its employees' sites if it was business related.

Doe's suspicious behavior continued to agitate his coworkers. Some caught him, for example, shielding his computer and quickly minimizing images, as well as leaving provocative pictures inadvertently on his screen. Finally, in reaction to the latest developments and in apparent defiance of the Director's injunction, Doe's immediate supervisor entered his cubicle while he was at lunch and clicked on his "Web sites visited." He discovered a number of probable child pornography sites including one with the title "Teenflirts.org: The Original Non-Nude Teen Index." Thereafter, the supervisor, with permission from his superiors (who were not involved with the Director) told Doe to quit his unlawful Internet activities. He agreed to this second demand, yet defiantly continued accessing the sites.

Doe's behavior continued for approximately 2 years after the initial complaints by coworkers. Eventually, company supervisors notified the police, who found nude photographs of Doe's own 10-year-old stepdaughter in the company dumpster. These were the same pictures that he had sent out as "payment" for access onto the child pornography sites. The discovery of the pictures formed the basis for a search warrant of his office and computer in which an additional 70 downloaded pictures were discovered, including more pictures of his stepdaughter.

Doe's ex-wife subsequently sued XYC for failing to investigate and protect her daughter. XYC prevailed at the trial level in a motion for summary judgment, but the appellate court overruled it stating: ". . .[the] defendant had a duty to report Employee's activities to the proper authorities and to take effective internal action to stop those activities." The court further maintained that: "Defendant was under a duty to exercise reasonable care to stop Employee's activities, specifically his viewing of child pornography which by its very nature has been deemed by the state and federal lawmakers to constitute a threat to 'others'. . ." The court's use of the phrases "duty to report" and "duty to exercise reasonable care" are particularly significant.

The case was subsequently sent back to the trial court to determine if the victim had suffered psychological harm.[7]

2.2 *Delfino v. Agilent Technologies*: A Case of Competence

In contrast to XYC's botched ISP management, Agilent Technologies performed competently thereby avoiding the kinds of legal problems XYC suffered. Perhaps more importantly for ISP managers, Agilent's prudent crisis management may serve as a valuable common law precedent to counter the heightened legal responsibilities the *Doe* case may have created.

In *Delfino*, the plaintiffs Michelangelo Delfino and Mary Day received a series of threatening messages, as well as postings on a message board, from a source with the screen name of "Crack_smoking_jesus." In fact, an Agilent employee named Cameron Moore was sending the messages to apparently harass and intimidate the plaintiffs due to litigation pending against him instigated partly by the plaintiffs. Ultimately, it was discovered that some of Moore's threats had been sent from work. For this reason, the plaintiffs also sued Agilent for, among other actions, negligent supervision and retention of Moore.

Agilent first learned of the threats against the plaintiffs when an FBI special agent requested information on an IP address that originated from Agilent. Agilent's IT personnel quickly agreed to cooperate with the FBI and succeeded in tracing the threats to Moore. When the Agilent ISP personnel confronted him with the information, Moore apologized, but contended that no threats had gone through Agilent's computer systems. He was told to agree *in writing* to never engage in this kind of activity again. Agilent management then gave Moore a "stern warning" but acknowledged that they had no proof that any of the threatening emails had gone through its system. Moore was also reminded that the company's Standards of Business Conduct does not allow employees to use company systems for personal reasons.

After several more months of investigation, the FBI told Agilent that it was about to arrest Moore. Agilent's management inquired whether the arrest was related to Moore's use of Agilent systems. The FBI assured them that it was not. Still, Agilent did not put the matter to rest but continued to stay on top of the investigation. It asked the FBI for its arrest affidavit and continued to interrogate Moore. During the latest line of questioning, Moore admitted that he had sent, while at work, emails that "weren't nice and could be interpreted as threats." After the admission, Moore

[7] In a 8 May 2006 interview in the Lawyers Weekly USA with the lead counsel who represented the plaintiff's ex-wife and child, it was revealed that the case was privately settled.

was put on administrative leave and several days later terminated for "misuse of Agilent's assets."

The facts in the Doe case are a good example of how a company can become liable through the fault, in this case negligence, of its supervisory personnel for failing to intervene competently once they become aware of a potential legal problem. The Delfino case, on the other hand, demonstrates that when a company's management quickly and adeptly reacts to a problem, they can avoid liability. The following discussion delves into the law regarding the supervision of employees and how the court resolved both cases.

2.3 Employer Liability Without Fault—The Doctrine of Respondeat Superior

In both cases, it is apparent that the employees were *not* engaged in activities that were within the normal scope of their workplace duties. And because they were not, neither XYC nor Agilent was found liable under the theory *respondeat superior* (see Endnote). Still, an understanding of this doctrine is important to understand how companies can be found liable for their employees' wrongful acts. Under *respondeat superior*, employees' wrongful acts or torts impute liability onto their employers [3]. Simply put, liability is assigned to the employer (usually a business entity such as a corporation or a limited liability company) even if it (through its management and supervisory personnel) did not approve or consent to the employee's particular act. Still, the employee's acts must, as mentioned, occur within the scope of the employee's workplace duties. For ISP and other management personnel, the doctrine is particularly worrisome since their companies become *strictly or vicariously liable* once these acts are committed.[8] The Restatement (Second) of Agency Section 228 provides the generally accepted definition of what constitutes the scope of employment.

The conduct of the employee is within the scope of employment if:

1. It is of the kind the employee is employed to perform.
2. It occurs within authorized space and time limits.
3. Some or all of it is done to serve the employer.
4. If the employees use force against each other [7].

[8] Strict liability is liability without fault. Under strict liability, the plaintiff only needs to prove that the tort happened and that the defendant was responsible. Vicarious liability is liability for the wrongful acts of another. Negligence is behavior that falls short of what a reasonable person would do to protect others from foreseeable harm. Under negligence, the plaintiff must prove that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, that the breach of duty was the proximate cause of harm to the plaintiff, and that the plaintiff suffered injuries to his person or property. See generally West's Legal Dictionary.

Although the doctrine has existed for decades, it remains controversial since the employer is liable even after its management personnel exercises due diligence in selecting and supervising an employee who subsequently commits an illegal act.

In contrast to the foregoing, in which employees are engaged in the course and scope of their jobs, actions in which the employer would not be liable under this doctrine are those that are "purely motivated by personal interests or are outrageous in nature. . ." Exceptions to these may occur when the "employee harms another because of the opportunity that the job offers" [19]. This class of employer liability could arise due to an employee's negligence or even when he intentionally harms another such as when an employee defrauds a third party on the job to enrich himself [3].

2.4 Negligent Supervision and Retention of Employees

Since the errant employees in both the *Doe* and *Delfino* cases were not engaged in activities that fell within the scope of their jobs, the pertinent legal issue was whether their employers had negligently supervised and retained these employees. This means that even if employees on the job are not acting within the scope of employment or are not furthering their workplace duties, the employers themselves can be negligent for the hiring, supervision and retention of dangerous or careless employees. This means that an employer will *not* be subject to strict or vicarious liability like they would be under the doctrine of *respondeat superior*[3], but directly could still be liable for negligence. This theory is pertinent since, as it will be discussed below, XYC was found to be negligent in its supervision/retention of Doe, while Agilent was not in respect to how it managed Moore.

2.5 Intentional Harm on the Internet

Employers may also incur liability when their employees engage in intentionally harmful acts at work. If an employee intentionally injures another's person or property, the employer can be liable if it is "reasonably connected with the employment as to be within its 'scope'" [3]. An exception to this occurs if the employees' motives, for example, are "purely personal," that is, are "unprovoked, highly unusual, and quite outrageous" [3]. Even under this scenario a company's liability can attach if management knew or should have known that the employee would act in such a personal or outrageous way. An example of this occurs when an employee, such as a bouncer, possesses known dangerous and aggressive behaviors, and then injures someone while on the job.

Both Doe and Moore engaged in intentional acts that hurt others outside their companies. Although the case, as mentioned, was remanded to the trial court to determine what injuries his stepdaughter may have suffered, Doe's intentional transmission of "kiddie porn" is considered under the law to constitute a threat to others.[9] Moore was accused of a tort known as the intentional infliction of emotional distress, among other acts.

2.6 Cybertorts

Cybertorts are torts committed in cyberspace [17]. The legal environment surrounding cybertorts is complicated and evolving. For example, in the first part of this chapter, we explored the torts of trespass to chattels and nuisance and how they pertain to the Internet. Now the legal duty imposed on employers, after *Doe* in particular, may significantly expand the legal landscape for these and other kinds of torts committed in the workplace.

In 1996, the law surrounding ISP liability for cybertorts was greatly clarified when Title V of the Telecommunications Act of 1996, better known as the Communications Decency Act (CDA) was passed. Under the CDA, Section 230 Congress shielded commercial ISPs from civil liability should they fail to remove or block tortious activities as long as the ISP does not actually have input in the creation of the offensive material. The law also protects ISPs that attempt to block and screen offensive material under the so-called "Good Samaritan" exception. Initially the law was passed to protect ISPs from defamation but has since been expanded to include virtually all tort liability. With ISP immunity, which includes other intermediaries such as Web sites and online information content providers, successful prosecution of cybertort activities has generally been thwarted, most often because the victims are unable to locate and sue the victimizers. Still, even if they can be located, they are usually not "deep pocketed" corporate defendants who are heavily insured and able to pay off large judgments [11]. Thus, cases like *Doe* and *Delfino*, in which economically viable corporations are being sued, will likely increase.[10]

[9] The duty to report child pornography once it becomes known is required under federal law at 42 USC Section 13032(b) and imposes sanctions on ISPs at 42 USC Section 13032(b)(4).

[10] It is noteworthy that XYC Company did not assert that it had immunity as an ISP under the broad protections of the Communications Decency Act, 47 USC Section 230. The court in Delfino, on the other hand, did argue for CDA immunity successfully. Not all employers, however, own and operate their ISP's and so may not be protected by this provision. Moreover, immunity can be lost in certain circumstances. For example, in a potentially influential case from the 9th Circuit, *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 2008 WL 879293 (9th Cir., 3 April 2008), an ISP lost its immunity under CDA Section 230 when it became a non-neutral "information content provider." *Roommates.com* contains facts different from both the *Doe* and *Delfino* cases discussed in this chapter. Moreover, as stated above, there is an affirmative duty to report child pornography once an ISP operator becomes aware of it.

The law concerning employer liability is complex and a full discussion is beyond the scope of this chapter. However, the main legal issues can be summarized with the aid of Fig. 1. The first question is whether the individual is an independent contractor or an employee (Node A in Fig. 1). Employers are not strictly liable for the acts of independent contractors, but may be liable for negligent selection or retention of the contractor (Node B). If the individual is an employee, the next question is whether the employee is acting within the scope of employment (Node C). If the employee is acting within the scope of employment, as described in the Restatement (Second) of Agency, then the employer is strictly liable. If the employee is not acting within the scope of employment, other issues become important (Node D). The employer may be liable for negligent supervision and retention of the employee (Node E), if the employee intentionally harms a third party (Node F) or if the employee commits cybertorts (Node G).

3. Why Doe Lost and Delfino Won—A Case of Risk Management

Even though both XYC Co. and Agilent were sued under the same cause of action—negligent supervision and retention—the differing outcomes are easy to understand.

3.1 Why the Court Said *XYC* Was Liable

The *Doe* case illustrates the harm that can be caused by highly imprudent behavior both in the way a company generally manages its workers, and its failure to effectively respond to trouble.[11] One of XYC's biggest mistakes was the confusion caused by having two computer use policies. One policy was well-distributed and specifically stated that emails were the company's property and should not be considered confidential. The policy also stated that anyone aware of the "misuse of the Internet for other than business reasons was to report it to Personnel" [14].

[11] How influential the *Doe* case will be on future common law courts is highly speculative. Although it is important to point out that, while a company like XYC may not be liable for the contents posted on its ISP if it qualifies under the CDA immunity, once an employer does learn of employee wrongdoing, at least under the reasoning of *Doe*, it takes on a legal duty to supervise and retain its employee in a non-negligent manner, One case, besides *Delfino*, has also found employers not liable for the wrongful acts of employees on the Internet. In that case, *Booker v. GTE.Net LLC*, 214 F. Supp.2d 746 (E.D. Ky. 2002), the employer GTE.Net, much like Agilent Company, was considerably more careful in how it handled the wrongful acts of its employees than the XYC Company.

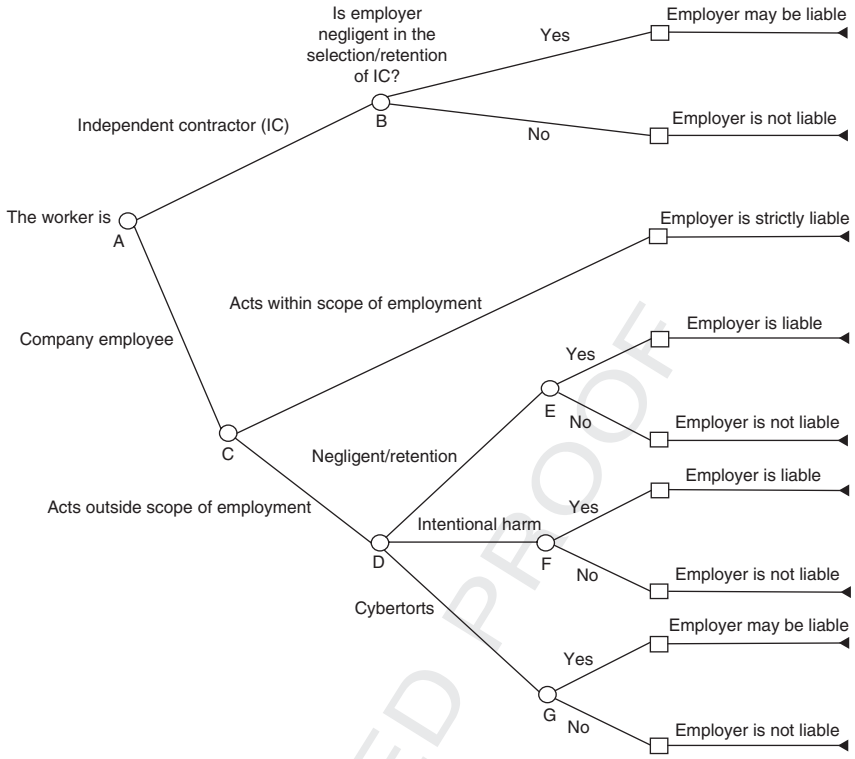

FIG. 1. Employer liability for the actions of its employees on the Internet.

Yet, at the same time it had another company policy, communicated by email, prohibiting the monitoring of employee computer usage.

The inconsistency prompted the court to rule that the first policy, in which XYC reserved rights, conflicted with the privacy rights it conferred to their employees under the second policy. In effect the court decided that the former policy negated the latter stating that "[d]efendant [XYC Co.] recognized its right to monitor employee Web site activity and emails by promulgating and distributing a policy to that effect during the relevant time period" [13]. Moreover, the court explained, XYC produced its own duty to monitor but then failed to carry it out properly. Consequently, once management had notice of Doe's dangerous actions, it had a "...duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third parties" [13].

The *Delfino* case clearly demonstrates how a prudent policy that is clear and expeditiously enforced can save a company from civil liability. *Delfino* is significant, not only as a positive Internet management model for ISP personnel, but also because it suggests that a company, like Agilent, can be shielded as a "provider or user of an interactive computer service" under CDA Section 230. What is important to note is the court's statement that "even if the [CDA] immunity did not apply" Agilent still would not have been liable for the torts the plaintiffs alleged. These actions help us to better understand and apply the lessons the case offers. It also may benefit other ISP supervisors in the future who may not presently enjoy this special immunity, since it is currently a binding precedent only in a portion of California.

3.2 Why the Court Said Agilent Should Not Be Liable

The *Delfino* court gave three reasons for exonerating Agilent for the negligent supervisor/retention of Moore. First, the court stated that Agilent owed *no* duty of care (a required element in proving negligence) to the plaintiffs. Although there are a number of factors a court looks at to determine whether a duty exists, several of the factors were considered of particular importance for Agilent. One was that Agilent, despite its careful procedures, had no prior notice that Moore was harassing the plaintiffs. Foreseeability of harm is very important in creating a legal duty. XYC, on the other hand, experienced ample opportunities to foresee the kind of harm Doe might inflict on someone. Moreover, the court explained, Agilent should shoulder no "moral blame," another factor, since it had promulgated a clear, consistent policy for discovering and thus preventing this sort of activity. A *tougher* policy meant to prevent harm might have even, according to the court, resulted in a "chilling effect" and "extreme employer oversight of employee's [Internet] activities." This language suggests that Agilent did what it was supposed to do, but not to excessive lengths. The court additionally argued that imposing "a duty to the world for all acts of its employees" even when some are not business related, would be too burdensome. The court concluded by maintaining that such a risk, one that is an "unknown malicious act of an employee bearing no relationship to his job," is not likely to be insurable. Courts, it noted, have been very reluctant to impose an uninsurable duty on employers [14].

4. Conclusion

The common law has been called upon for centuries to settle some of the most troublesome problems confronting individuals, businesses, and government. Now, some of these problems have morphed from those occurring in physical space to those creating havoc in cyberspace.

These "cyberevils" range from such cybertorts as defamation, "cyberassment" (including Webjacking, spoofing, cybersquatting, denial of service attacks or email bombs, sending viruses, cyberbullying, sexual harassment, etc.) [18], intentional infliction of mental distress, as well as spamming, trespass to chattels (personal property) mentioned in the first part of this chapter. Unfortunately, all of these will continue to occur. Then again, the common law will likely be up to the task of addressing the problems as they arise and helping victims to be compensated for losses they may incur.

The *Doe* case, discussed in the second part of this chapter, portends the potential for large-scale harm that can befall ISP personnel who fail to manage prudently while also giving guidance to those who follow Agilent's example. Both cases were cases of first impression, that is, there were no previous cases or precedents for the courts to follow. Given the general paucity of Internet cases and the doctrine of *stare decisis*, they will likely be influential on courts in the future.

In the end, management personnel must be aware of the law and what it can offer both as a sword and as a shield in combating the cyber enemies who may impair property and harm people. Those, for example, who chose to imitate Agilent's management approach can feel confident relying on that legal outcome, while companies, like XYC, which retain malicious employees who harm others outside the company and possess ineffectual management policies and personnel, may become vulnerable to lawsuits and expensive judgments. These two cases, both the product of the common law, will likely influence the cyberworld of tomorrow.

Endnote Legal Definitions*

Conversion: The unauthorized exercise of dominion or control over someone's personal property (chattel).

Negligence: Behavior that falls below what the average reasonable person would do to protect others from foreseeable risks of harm. The plaintiff must prove that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, that the breach of duty was the cause of harm to the plaintiff, and that the plaintiff suffered injuries to his person or property.

Nuisance: An unreasonable interference with the use and enjoyment of land.

Respondeat superior: The liability of an employer for the wrongful acts of his employee.

Stare decisis: To abide by or adhere to decided cases.

Strict liability: Liability without fault.

Tort: A civil wrong (other than a breach of contract) that has caused harm to person or property.

Trespass to chattels: Tort with the following elements: (a) personal property-Chattel, (b) plaintiff is in possession of the chattel or is entitled to immediate possession, (c) intent to dispossess or to intermeddle with the chattel, (d) dispossession, impairment, or deprivation of use for a substantial time, (e) causation of the dispossession, impairment, or deprivation.

Vicarious liability: Liability for the wrongful acts of another.

*W. Statsky, West's Legal Thesaurus/Dictionary, West Publishing Company, St. Paul, MN, 1985 (ISBN 0-314-85305-7).

Reference Books on Internet/Cyberlaw

I. Ballon, E-Commerce and Internet Law: Treatise with Forms, Glasser Legal-Works, Little Falls, NJ, 2001 (ISBN 1-88807-94-5).

G.B. Delta, and J.H. Matsuura, Law of the Internet, Aspen Publishers, Inc., New York, NY, 2001 (ISBN 0735522197).

M.A. Lemley, P.S. Menell, R.P. Merges, P. Samuelson, Software and Internet Law, third ed., Aspen Publishers, Inc., New York, NY, 2006 (ISBN 9780735558649).

D.G. Post, P.S. Berman, P. Bellia, Bellia, Berman and Post's Cyberlaw, West Publishing Company, St. Paul, MN, 2002 (ISBN-13: 9780314166876).

D.M. Powers, The Internet Legal Guide: Everything You Need to Know When Doing Business Online, John Wiley & Sons, New York, NY, 2001 (ISBN 0471164232).

D.W. Quinto, D. Desai, Law of Internet Disputes, Aspen Publishers, Inc., New York, NY, 2001 (ISBN 0735525927).

R.A. Spinello, Regulating Cyberspace: The Policies and Technologies of Control, Quorum Books, Westport, CT, 2002 (ISBN 1-56720-445-7).

Acknowledgments

The authors wish to express their appreciation to Diane Crawford and the *Communications of the ACM* for allowing us to use research and articles we have published in that journal as the basis for this chapter.

References

[1] R. LaPorta, F. Lopez-de-Silanes, A. Scheifer, R. Vishny, Law and finance, J. Polit. Econ. 105 (1998) 1113.

[2] S. Stolberg, A. Liptak, Roberts fields questions on privacy and precedents, The New York Times. com, 2005.

[3] W. Keeton, D. Dobbs, R. Keeton, D. Owen, Prosser and Keeton on Torts, fifth ed., West Publishing Company, St. Paul, MN, 1984 (ISBN 0-314-74880-6).

[4] T. Loomis, Internet trespass: companies turn to an old tort for a new reason, New York Law J. 227 (2000) 5.

[5] Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1996.

[6] CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (ND Ohio, 1997).

[7] American Law Institute, Restatement (Second) of Agency, American Law Institute Publishers, St. Paul, MN, 2005 (ISBN 0-314-96119-4).
[8] eBay v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (ND Cal., 2000).
[9] Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 4th Cir., 2003).
[10] S. Kam, Intel v. Hamidi: trespass to chattels and a doctrine of cyber-nuisance, Berkeley Technol. Law J. 19 (2004) 427.
[11] Rockbridge Associates, National Technology Readiness Survey, Center for Excellence in Service, R.H. Smith School of Business, University of Maryland (available at http://www.rhsmith.umd.edu/ces/ntrs.html; last checked 1 May 2008), 2004.
[12] R. Aalberts, P. Poon, P. Thistle, Trespass, nuisance and spam: eleventh century common law meets the Internet, Commun. ACM 50 (2007) 40.
[13] Doe v. XYC Co., 382 N.J. Super. 122, 887 A.2d 1156, 2005.
[14] Delfino v. Agilent Technologies, Inc., 145 Cal App. 4th 790, 52 Cal. Rptr. 3rd 376 (Cal. App. 6th Dist., 2006).
[15] L. Sotto, et al., Workplace privacy in the U.S.: what every employer should know, Practicing Law Inst. 861 (2006) 201.
[16] H. Gunnarsson, Must employers try to stop employees "unauthorized activity"? Illinois Bar J. 94 (2006) 172.
[17] M.L. Rustad, T.H. Koenig, Rebooting cybertort law, Wash. Law Rev. 80 (2005) 335–361.
[18] C.E. Smith, Intentional infliction of emotional distress: an old arrow targets the new head of the hate hydra, Denver Univ. Law Rev. 80 (2002) 1–58.
[19] L. Papa, S. Bass, How employees can protect themselves from liability for employees' misuse of computer Internet, and email systems in the workplace, Boston Univ. J. Sci. Technol. Law 10 (2004) 110.