A TALE OF TWO INTERNET SERVICE PROVIDERS:
A RISK MANAGEMENT PERSPECTIVE

by

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 of risk management and insurance in the finance department at the University of Nevada, Las Vegas.

Department of Finance
College of Business
University of Nevada, Las Vegas
4505 Maryland Pkwy.
Las Vegas, NV 89154-6008

A TALE OF TWO INTERNET SERVICE PROVIDERS:  
A RISK MANAGEMENT PERSPECTIVE

Most ISP supervisors are aware they possess legal rights to monitor employees’ Internet use. Laws such as the federal Electronic Communications Protection Act generally allow employer’s great leeway to monitor employees’ computer use [8]. Yet few ISP supervisors are aware that some courts are in the process of creating a legal duty for employers to monitor their workers. Two cases in the past two years, Doe v. XYC Co.¹ in New Jersey and Delfino v. Agilent Technologies, Inc.,² in California, demonstrate the increasing importance of properly managing workers’ use of the Internet. This article will discuss the facts of these two cases and the relevant legal doctrines. In the first case, XYC Co. made serious mistakes and exacerbated its legal exposure, while in the second case, Aligent’s prompt action allowed it to resolve its problems. Both cases provide important lessons in how to manage this imminent legal risk.

THE DOE CASE AND THE DUTY TO MONITOR

The unusual facts in the Doe case, a “perfect storm” of employer incompetence and employee deviance, are compelling and indicate the legal duty it creates may become far-reaching. 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. The company’s Senior Network Administrator (SNA) found that Doe’s computer logs contained sites with highly suspicious names such as “bestiality”

¹ 382 N.J. Super. 122, 887 A.2d 1156 (2005)  
and “necrophilia.” The SNA confronted Doe and ordered him to stop visiting “inappropriate sites.” Doe, however, disobeyed the order. 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 (Director) requesting a formal investigation. At this point the Director made a significant mistake. Instead of investigating the allegations, she “admonished” the SNA, told him never to access any employee’s Internet activity in the future and that further violations of this company policy could result in losing his job. Ironically, the company also had at the same time a second Internet use policy that allowed the company to access and review its employees’ sites if it was business related.

Doe, unaware of his supervisor’s latest discovery, continued to access the illicit sites and his suspicious behavior continued to agitate his co-workers. Some caught him, for example, shielding his computer and quickly minimizing images, as well as inadvertently leaving provocative images on his screen. Eventually Doe’s immediate supervisor entered his cubicle while he was at lunch and clicked on his “websites visited” where the supervisor discovered a number of probable child pornography sites. The supervisor, with permission from his superiors (who were not involved with the Director), told Doe to quit his unlawful Internet activities. Doe agreed to this second demand, yet defiantly continued accessing the sites. In the end, the company’s supervisors belatedly alerted the police. The police found nude photographs of Doe’s own 10 year old stepdaughter in the company dumpster. These pictures had also been sent out by Doe as “payment” for access to child pornography sites. The discovery of the

---

3 At this point, XYC Company arguably possessed sufficient “knowledge of facts or circumstances” to report Doe’s activities to authorities. The duty to report child pornography is required under federal law at 18 USC § 2252. Federal law imposes sanctions on those who fail to report at 42 USC § 13032(b)(4).
pictures formed the basis for a search warrant of Doe’s office and computer in which an additional seventy 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’ …” and “The existence of a duty is a matter of law derive[ing] from considerations of public policy.”

**DELFINO AND THE RIGHT TO MONITOR**

In contrast, Agilent Technologies’ intelligent approach to risk management allowed it to avoid the kinds of legal problems XYC suffered. Perhaps more importantly for ISP managers, Agilent’s prudent use of its right to monitor employees computer use

---

4 It is noteworthy that XYC Company did not assert immunity as an ISP under the broad protections of the Communications Decency Act, 47 USC §230. It is possible that XYC Company may have escaped liability if it had. For example, CDA §230 immunity was argued successfully in the *Delfino* case discussed herein. Still, immunity can be lost in certain circumstances, a complicated topic beyond the scope of this article.

5 *Doe*, 887 A.2d at 1156. The case was remanded to the trial court with instructions to resolve the issues of whether Doe’s actions were foreseeable by XYC Company and whether psychological damages were suffered by the stepdaughter. In a May 8, 2006 interview in the *Lawyers USA* magazine with the lead counsel who had represented the plaintiff ex-wife and child, it was revealed that the case was settled privately.

6 *Doe*, 887 A.2d at 1167.
may serve as an illustration of how 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 and was told that it was not. Agilent did not put the
matter to rest but continued its own investigation. It asked the FBI for its arrest affidavit and continued to interrogate Moore. Moore eventually admitted that he had sent, while at work, emails that “weren’t nice and could be interpreted as threats.” After the admission, Moore was put on administrative leave and several days later terminated for “misuse of Agilent’s assets.”

The facts in the Doe and Delfino cases are good examples of how a company can become liable and how a company can avoid liability. The following sections discuss the law regarding the supervision of employees and how the courts applied the law to resolve both cases.

**EMPLOYER LIABILITY WITH AND WITHOUT FAULT**

The law governing employer liability is complex. Figure 1 provides a guide to the ways that employers can be potentially liable for their employee’s activities.

First, the law makes a distinction between employees and independent contractors (see node A). As a rule of thumb, independent contractors control the conditions of their work while employees do not. Employers are generally not strictly liable for the actions of independent contractors but may be liable if the employer is negligent in the selection or retention of the contractor (see node B). Our focus here is on liability for employee actions. An important distinction is whether the employee’s actions are within the scope of employment or not (see node C).
Respondeat Superior

Under the legal doctrine of *respondeat superior* employees’ wrongful acts or torts imputes liability to their employers [2]. Liability is assigned to the employer even if it did not approve or consent to the employee’s particular act as long as the act was within the “scope of employment.” The Restatement (Second) of Agency § 228 provides the generally accepted definition of the scope of employment [5]:

“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 of it or it is done to serve the employer; and;
4. If the employees use force against each other.”

For ISP and other management personnel, the doctrine is particularly worrisome since their companies become *strictly or vicariously liable* once these acts are committed. Although the doctrine has existed for decades it remains controversial since the employer is liable even after its management exercises due diligence in selecting and supervising an employee, who subsequently commits an illegal act.

The employer would not be liable under this doctrine for acts 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” [4]. This could occur due to an employee’s negligence or when the employee intentionally harms another such as when an employee defrauds a third party on the job in order to enrich himself [2].
Negligent Supervision and Retention of Employees

In both *Doe* and *Delfino*, 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, the pertinent legal issue was whether the companies had negligently supervised and retained these employees (see node E in Figure 1). 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 supervision and retention of dangerous or careless employees. In this case an employer will *not* be subject to strict or vicarious liability like they would be under the doctrine of *respondeat superior* [2], but the employer 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 Moore.

Intentional Harm on the Internet

Employers may also incur liability when their employees engage in intentionally harmful acts at work (see node F in Figure 1). If an employee intentionally injures another’s person or property, the employer can be liable if it’s “reasonably connected with the employment as to be within its ‘scope’” [2]. An exception to this occurs if the employees’ motives, for example, are “purely personal,” that is are “unprovoked, highly unusual, and quite outrageous.” Still, even under this scenario a company’s liability can still 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 [2].

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

Cybertorts

Cybertorts are torts committed in cyberspace (see node G) [6]. The legal environment surrounding cybertorts is complicated and evolving and so employer liability issues are beyond the scope of this paper. Still, the legal duties imposed on employers, after Doe in particular, may significantly expand their potential risk of legal liability. 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. In section 230 of the CDA, Congress shielded commercial ISP’s from civil liability should they fail to remove or block tortious activities. The law was initially passed to protect ISPs from defamation but has since been expanded to include virtually all tort liability. The immunity includes other intermediaries such as websites and online information content providers. Successful prosecution of cybertort activities have generally been thwarted, most often because the victims are unable to locate and sue the victimizers. Still, even if the perpetrators can be located, they are usually unable to pay large judgments [6]. Thus, cases like Doe and
Delfino, in which economically viable corporations who are viewed as “deep pockets” are being sued, will likely increase.

WHY XYC LOST AND ALIGENT 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 difference between the outcomes is easy to understand. The Doe case illustrates the harm that can be caused by highly imprudent behavior both in the way a company generally manages its workers, as well as its failure to effectively respond to trouble. 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. This policy also provided that anyone aware of the “misuse of the Internet for other than business reasons was to report it to Personnel.”7 At the same time it had a second policy, communicated by email, which prohibited 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 its employees. In effect the court decided that the former policy negated the latter, stating that “[d]efendant [XYC Co.] recognized its right to monitor employee website activity and e-mails by promulgating and distributing a policy to that effect during the relevant time period.”8 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

---

7 Doe, 887 A.2d at 1161.
8 Ibid.
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.”

The Delfino case clearly demonstrates how a computer use policy that is clear,
consistent and expeditiously enforced can save a company from civil liability. Thus,
Delfino is significant as a positive Internet management model for ISP personnel.
Delfino is also significant because it also suggests that a company like Aligent can be
shielded as a “provider or user of an interactive computer service” under CDA section
230. A complete discussion of this issue is beyond the scope of this article. What is
important to note is the court’s statement that “even if the [CDA] immunity did not
apply,” Aligent 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.

**Why the Court Said Agilent Should Not Be Liable**

The Delfino court offered several reasons for exonerating Agilent for the
negligent supervision/retention of Moore. First, the court stated that Agilent owed no
duty of care (a required element in proving negligence) to the plaintiffs. The courts
consider a number of factors to determine if there is a duty of care; several of the factors
were considered of particular importance for Agilent. The factor of “foreseeability” of
harm is very important in creating a legal duty. Agilent, despite its careful procedures,

---


10 For example, in a potentially influential case from the 9th Federal Circuit Court, *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 2008 WL 879293 (9th Cir. Apr. 3, 2008), an ISP lost its immunity under CDA § 230 when it became a non-neutral “information content provider.” *Roommates.com* contains facts different from those in the cases discussed in this article.
had no prior notice that Moore was harassing the plaintiffs until it was contacted by the 
FBI. XYC, on the other hand, experienced ample opportunities to foresee the kind of 
harm Doe might inflict on someone.

The factor of “moral blame” is also important in determining if there is a legal 
duty. The court explained that Agilent has no moral blame since it had promulgated a 
clear, consistent policy for discovering and thus preventing this sort of activity. 
According to the court, a tougher policy meant to prevent harm might have 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 and but not to 
extensive lengths. The factor of “insurability” is also considered in determining if there 
is a duty of care. The court 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 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 was noted, have 
been very reluctant to impose an uninsurable duty on employers.\(^\text{11}\)

**CONCLUSION**

Employers’ tort liability for their employees’ harmful acts in cyberspace is a 
serious legal threat. Cybertorts such as defamation, spamming, trespass to chattels 
(personal property) “cyberassment” (including webjacking, spoofing, cybersquatting, 
denial of service attacks or e-mail bombs, sending viruses, cyberbullying and sexual 
harassment) [7] will continue to occur. Similarly, viewing and sending pornography and 
intentional infliction of mental distress will continue to occur. Moreover, as Clineburg

\(^\text{11}\) *Delfino*, 145 Cal. App. 4\textsuperscript{th} at 816.
and Hall point out, employees engaged in “blogging” on Web logs and pages and posting to message board and email groups on the job could also be legally troublesome for an employer [1].

The Doe case portends the potential for large-scale harm that can befall ISP personnel who take on the task of monitoring their employees but then fail to manage prudently. Delfino gives guidance to those who follow Agilent, which reacted quickly and effectively once they had learned of its employee’s offensive activities. Indeed, the Delfino case suggests that no duty exists until the employer becomes aware of the problem, a legal development that, if followed by other courts, would be fortuitous to ISP managers. Both the Doe and Delfino cases were cases of first impression (there were no precedents for the courts to follow). Due to the general paucity of Internet cases, these cases are likely to be influential on courts in the future.12 Thus, companies who chose to imitate Agilent’s approach of developing and enforcing consistent computer use policies can feel confident relying on that legal outcome. Companies which have inconsistent polices or ineffectual enforcement, like XYC, may be putting themselves at considerable risk.

12 How influential Doe and Delfino will exert on future courts’ decisions is highly speculative. At least one case, besides Delfino, has found employers not liable for the wrongful acts on the Internet of employees at work. See Booker v. GTE.Net LLC, 214 F. Supp.2d 746 (E.D. Ky. 2002).
REFERENCES


Figure 1. Employer Liability for the Actions of Its Employees on the Internet

- **The Worker is**
  - **Company Employee**
    - Acts Within Scope of Employment
      - Is Employer negligent in the selection/retention of IC? (Yes/No)
      - Employer is Liable
    - Acts Outside Scope of Employment
      - Intentional Harm
        - Yes: Employer is Liable
        - No: Employer is Not Liable
      - Cybertorts
        - Yes: Employer May be Liable
        - No: Employer is Not Liable
  - **Independent Contractor (IC)**
    - Employer May Be Liable (Yes/No)
    - Employer is not Liable