Understanding the School's Duty Not to be ICT Negligent - an Introduction to the Law of Negligence.

In this White Paper, noted Legal Expert Dr. Brian Bandey discusses the Law of Negligence – in the context of the School's Legal Duty not to be "ICT Negligent".

The Law of Negligence produces a complex network of obligations on the School is relation to Student's use of ICT – and those obligations cannot be delegated and are inescapable. Using a "Worked Example" based entirely on Real Events – Dr. Bandey demonstrates how the Law of Negligence can make the unwary School liable to students, parents and other affected parties.

1. INTRODUCTION

It almost goes without saying that this White Paper cannot be a primer to the Law of Negligence. However, it is the Law of Negligence which produces a real and meaningful intensification of the School's Base-Line Legal Exposure where Schools provide E-Mail and Internet Access to children. It is the Law of Negligence which produces the most important, dense and complex network of Inescapable Legal Obligations that flow from School to Student. Legal Obligations that can only be satisfied – not avoided.

In order to introduce how this supremely important Doctrine of Law operates, I am going to introduce and analyze a "Worked Example" entirely based on Real Life Events. In other words – all that I described happened somewhere, at sometime, to someone.

The Worked Example is based on the fact that, no matter what we would all like (or prefer) to think; it is not too fantastic to imagine that a non-contact pedophile can be an employee of a school nor is it too fantastic to imagine child pornography or extreme pornographic images existing on a school server.

2. NEGLIGENCE 101

Let's be real about this and understand that this Paper hardly constitutes a 'primer' in negligence. What I have done is chosen a few of the components of this Tort to provide, at least, some entrée to understanding this very relevant Legal Doctrine.

In General Negligence is a form of extracontractual liability that is based upon a failure to comply with the duty of care of a reasonable person, which failure is the actual cause and proximate cause of damages. That is, but for the tortfeasor's[1] act or omission, the damages to the plaintiff would not have been incurred, and the damages were a reasonably foreseeable consequence of the tortious conduct.

Put another way – the Law of Negligence requires that persons conduct themselves in a manner that conforms with certain standards of conduct. Where a person's actions violate those standards, the law requires the person to compensate someone who is injured as a result of this act. In some instances, the law of negligence also covers a person's omission to act.

In Tort Law, Negligence is often described as a 'distinct cause of action' – meaning, most importantly, a right to sue can exist at the same time as (say) a breach of contract but also exist in the absence of a contract-based relationship. The Restatement (Second) of Torts defines negligence as "*conduct that falls below the standard established by law for the protection of others against unreasonable risk of harm.*" Negligence generally consists of five elements, including the following:

(1) a duty of care owed by the defendant to the plaintiff;
(2) a breach of that duty;
(3) an actual causal connection between the defendant's conduct and the resulting harm;
(4) proximate cause, which relates to whether the harm was foreseeable; and
(5) damages resulting from the defendant's conduct.

1 The legal technical term for the person committing the act. Negligence is a form of civil wrong known as a "Tort".

Breach. Breach is ordinarily established by showing that the defendant failed to exercise reasonable care. Some courts use the terms ordinary care or prudent care instead. Conduct is typically considered to be unreasonable when the disadvantages outweigh the advantages. Judge Learned Hand famously reduced this to algebraic form in *United States v. Carroll Towing Co.*: [2]

$$B < PL$$

This means that if the **b**urden of exercising more care is less than the **p**robability of **l**oss (damage, harm, etc.), and a person fails to undertake the burden, he is not exercising reasonable care and is thus breaching his duty to do so (assuming he has one).

The "But For" Test. Actual cause has historically been determined by the "But For" test. If the result would not have occurred but for the defendant's act, the act is an actual cause of the result. Several other tests have been created to supplement this general rule, however, especially to deal with cases in which the plaintiff suffers great harm, yet because multiple acts by multiple defendants, the but for test is unhelpful. This situation occurred in the famous case of *Summers v. Tice.* [3]

For example, Dan and Dave both negligently fire their shotguns at Paula. Paula is struck by only one pellet. It is impossible to determine which gun it was fired from. Using the but for test alone, Dan and Dave can both escape liability. Dan can say that but for his own negligence, Paula still might have suffered the same harm. Dave can make the same argument. As a matter of public policy, most courts will nonetheless hold Dan and Dave jointly and severally liable. The act of each defendant is therefore said to be an actual cause, even if this is a fiction.

An Associated Tort – NIED. The tort of negligent infliction of emotional distress (NIED) is a controversial cause of action, which is available in nearly all U.S. states but is severely constrained and limited in the majority of them. The underlying concept is that one has a legal duty to use reasonable care to avoid causing emotional distress to another individual. If one fails in this duty and unreasonably causes emotional distress to another person, that actor will be liable for monetary damages to the injured individual. The tort is to be contrasted with intentional infliction of emotional distress in that there is no need to prove intent to inflict distress. That is, an accidental infliction, if negligent, is sufficient to support a cause of action.

NIED is particularly relevant to the School and student's use of School ICT since exposure to inappropriate or illegal image-based material and cyberbullying almost inevitably lead to emotional distress – both for the Student and their family.

The School's Duty to Monitor its Employees. The New Jersey Appellate Division, in *Doe v. XYC Corp.*[4] ruled that an employer may be held liable in tort to the victim of pornography when it has actual or implied knowledge that its employee is using his workplace computer to access pornography, including child pornography, but does not investigate or stop the employee's conduct. Interpreted broadly, the decision stands for the proposition that New Jersey employers have **a legal duty**, not simply a right, to monitor employees' e-mail and internet use.

Interpreted more narrowly, the decision stands for the proposition that when an employer knows or should know that an employee is viewing pornography, it has a duty to investigate and take prompt action to stop the activities.

With regard to pedophilic material, considered as "contraband" by the Supreme Court [5], the Risks are High and the potential for damage is Substantial.

If XYC Corp. in the Doe case had implemented Active Supervision Technology [6]; and followed those up with Acceptable Use Policy enforcement – **NO liability** would have arisen.

A minor would also have been protected.

The employee used his workplace computer to view child pornography and to transmit nude photographs of his stepdaughter to a child pornography website. His wife sued the employer for negligence, alleging that it should have taken action to prevent the employee from transmitting pornography at work because it knew or should have known that he was viewing pornography.

2 159 F.2d 169 (2d. Cir. 1947
3 159 33 Cal.2d 80 (1948)
4 N.J. Super., 2005 WL 3527015 (App. Div. Dec. 27, 2005),
5 United States v. Kimbrough, 69 F. 3d 723, 731 (5th Cir. 1995).
6 In this White Paper, the term "Active Supervision Technologies" means Computer software technology which: (i) reads or views Internet based traffic; or (ii) reads or views the content of computer display peripherals (whether the computer is offline or online); and, if such traffic or content meets certain criteria: (a) prevents the intended recipient's access to it; or (b) prevents the display of the content; or (c) automatically generates alerts or reports in respect of such traffic or content.

Beginning in 1998 or 1999, there were at least four occasions when co-workers, IT personnel, or managers learned that the employee had accessed pornographic sites on his company computer. Yet, the employee was not reprimanded or counseled by his supervisor. Nor did the employer investigate the websites visited by the employee to ascertain whether they included child pornography, a crime under state and federal law, even though the employer recognized the sites as pornographic based on the computer log it maintained of the websites visited.

Finally, in March 2001, a supervisor told the employee that the company had received reports of inappropriate computer usage and directed the employee to stop the conduct. No other disciplinary action was taken and no investigation was done into what sites were being accessed. In early June 2001, the supervisor learned that the employee continued to access pornographic sites. The supervisor left for a business trip without taking disciplinary action against the employee.

On June 15, 2001, the employee transmitted three nude photographs of his ten year old stepdaughter from his workplace computer to a child pornography site. The employee was arrested on June 21, 2001 after pornographic photos of his stepdaughter were found in a company dumpster. Following his arrest, the police discovered that the employee had downloaded 1000 pornographic images while at work and had sent several e-mails regarding child pornography.

Reversing the trial court, which had granted the employer's motion for summary judgment, the Appellate Division found that the employer had actual or implied knowledge of the employee's conduct. The court speculated, that, had the employer enforced its own internet policy by investigating the employee's activities, it would have discovered the employee's predilection for child pornography, and in turn, it would have fired the employee or taken other disciplinary action in time to prevent the photographs of the stepdaughter from being sent to a child pornography site. The court next relied on well-settled law from the Restatement (Second) of Torts, that an employer is under a duty to exercise reasonable care to control an employee acting outside the scope of his employment to prevent him from harming others if:

(i) the employee uses the employer's property to commit the harm

(ii) the employer knows or should know of the necessity and opportunity for exercising such control.

Applying these principles, the court found that a reasonable inference existed that the employer "*had knowledge that [the] [e]mployee was engaging in activities that posed the threat of harm to others, although not necessarily to [the stepdaughter]. We see no unfairness in imposition of duty on defendant in these circumstances.*"

The employer in this case had an internet policy that prohibited employees from accessing pornography. Yet, the employer failed to investigate reported breaches of that policy or to take meaningful disciplinary action. Faced with these facts, the Appellate Division reaffirmed the employer's right to monitor employee internet use and took the company to task for not doing so. Although the ramifications of this decision have yet to be seen, it underscores the importance of not only having adequate internet and e-mail policies in place, but also the need to enforce those policies through the use of Technology.

3. THE WORKED EXAMPLE

So let us now hypothesize and extrapolate a known set of facts into a School-centric scenario in the form of a mock examination question for a Law Undergraduate. The facts I am going to used are based on an amalgamation of real-life cases. In this way we can see how the unwary and, indeed, the negligent school can suffer serious and immediate financial and reputational loss.

Q

XYZ High School teaches children from the ages of 14 to 18. Although computerized and offering every child Internet Access and a school E-Mail address; the School Board and the Principal have not implemented any Active Supervision Technology. They have not done so on the grounds that:

(a) there was no legal obligation on the school to implement the technology;
(b) there was no regulatory obligation on the school to implement the technology;
(c) the technology did not offer a return on investment;
(d) and that, although the school could afford the technology, the school "just didn't want to go there" in respect of monitoring their student's e-mail and Internet use.

It would be obvious that a chemical company negligently permitting the escape of toxic waste which poisons the farmer's land next-door would be liable to him in Negligence.

Exactly the same principles apply when students encounter the toxic content and illegal images that exist in Cyberspace and then, through the negligence of the School, suffer.

John is a Freshman at XYZ High School. His teachers have always noticed his secretive demeanor when using the school computers and a number of classmates have been seen giggling with embarrassment and have mentioned to their teachers they believe they have seen naked pictures of women on his screen when passing his desk. But no technology has been implemented which would assist the teacher in actively supervising this use.

The teacher in charge of these classes decided not to investigate the matter afraid as to what they would discover and were reluctant to admit that they did not have any technology tools to control this class well when they were using computers.

John, when under stress finishing a school project, inadvertently attaches a mixture of Hard-Core and Extreme Pornographic Images to his e-mail to his best friend at XYZ High (copying several other children). He makes the mistake since he 'hides' his images by giving them duplicate class work filenames.

Ten students at XYZ High receive the images, all tell their teachers and five show their parents. The police are called and an investigation launched. However, as some of the images involve children (a possible case of sexting) – the FBI is called. Many of the recipients are traumatized by what they see and have to take time off school on medical advice. Some of the children require counseling but others require psychiatric assistance. Parents threaten suit for nervous distress, hurt feelings and so on.

(Q1) **Is it possible for:** the parents of the 'exposed' children to have a right to sue the Teacher (on their children's behalf) for not reporting their finding and concerns and thus, for want of their omission, negatively affecting their children's mental and emotional health (a Negligence Action)?

It is, in Law, reasonably foreseeable that both children and parents will suffer (psychologically and economically) when a School negligently exposes children in its care to hard-core or extreme pornographic images.

A teacher cannot be everywhere in a classroom at once – but Active Supervision Technologies can.

It is, in Law, reasonably foreseeable that both children and parents will suffer (psychologically and economically) when a School negligently exposes children in its care to hard-core or extreme pornographic images.

A teacher cannot be everywhere in a classroom at once – but Active Supervision Technologies can.

A To question (1) – YES.

(Q2) **Is it possible for:** the parents of the 'exposed' children to have a right to sue the School (on their children's behalf) for the School's Employee's failure to report their finding and concerns and thus, for want of their omission, negatively affecting their children's mental and emotional health (a Negligence Action founded in the Doctrine of Vicarious Liability)?

A To question (2) – YES.

(Q3) **Is it possible for:** the parents of the 'exposed' children to have a right to sue the School (on their own behalf) for their personal loss and damage (including costs, expenses, upset, distress and loss of earnings as they attend to their children's needs to the detriment of their employment or careers) - (a Negligence Action founded in the Doctrine of Vicarious Liability)?

A To question (3) – YES.

(Q4) **Is it possible for:** the parents of the 'exposed' children to have a right to sue the School (on their children's behalf) for their personal loss and damage (including costs, expenses, upset, distress and cost of medical care) in relation to the School's failure to put in place Active Supervision Technology which would have stopped their children seeing the images in question - (a Negligence Action founded in the Doctrine of Vicarious Liability)?

A To question (4) – YES.

(Q5) **Is it possible for:** the parents of the 'exposed' children to have a right to sue the School (on their own behalf) for their personal loss and damage in relation to the School's failure to put in place Active Supervision Technology which would have stopped their children seeing the images in question - (a Negligence Action founded in the Doctrine of Vicarious Liability)?

A To question (5) – YES.

4. CONCLUSIONS

The Law of Negligence has certain essential attributes which indisputably fall on the shoulders of educators and the organizational structure above and behind them. It is an important Doctrine of Law that operates very strongly between School and Student.

The Duty of Care that arises on Teacher, Principal, Superintendant, School Board Member and ICT Risk Manager cannot be 'delegated away'. It cannot be avoided. it cannot be ignored. To operate in circumstances of ignorance of the law or willful blindness to it affords no defense to it whatsoever.

The toxicity of parts of the Internet to young and developing minds, the interest of children in inappropriate risk taking and the susceptibility of School ICT to be used as a vector of hostility and bullying are now unarguable given facts.

Taking all of the above into account – the School and all of the organizations and personnel that support it must look to their Duty of Care that arises when students access the School's ICT. The Duty of Care should be acknowledged, calculated and understood. Since only then can appropriate measures (whether procedural, structural or technological (Active Supervision Technologies)) be introduced so that this inescapable duty is fulfilled.

Copyright Information