

Module 14

N480 Technology and the Law

Module 14: Other Legal Issues

Goals and Objectives

The goals and objectives of Module 14 are to:

- Describe the law of negligence, strict liability and intentional torts and how they apply in the context of high-tech industries.
- Discuss how the legal system is responding to negligent and malicious behavior on the Internet and with software programs.
- Highlight the balance between individual privacy and the needs of government and business to monitor and gather information.
- Describe some of the laws and court cases related to monitoring communications and personal activities in the workplace.
- Describe some of the technology used to gather personally identifiable information through the Internet and some of the legislation that has been developed to address the extent to which this is permissible.
- Discuss the legislation and court cases related to controlling content on the Internet, particularly with respect to protecting children.
- Consider how laws on defamation and rights to publicity can impact what we say - or include - about individuals on the Internet, in email or in developing new media and informatics products and services.
- Highlight the important points in Chapters 12 and 13 of *Legal Aspects of Managing Technology*.

Module 14: Summary of Major Points

Please read **Chapter 12** and **Chapter 13** in *Legal Aspects of Managing Technology*. Please also read a brief article on *rights of publicity* and a one-page history of **copyright law**

<https://iu.instructure.com/courses/1874392/files/96596117/download?wrap=1>

<https://iu.instructure.com/courses/1874392/files/96596117/download?wrap=1> ,

<https://iu.instructure.com/courses/1874392/files/96596117/download?wrap=1>

<https://iu.instructure.com/courses/1874392/files/96596117/download?wrap=1> which celebrated its

300-



year birthday in April 2010.

By next Sunday, **by Noon**, please go to the **Discussion Forum - Module 14: Other Legal Issues** (https://iu.instructure.com/courses/1874392/discussion_topics/9043982) and discuss:

- In terms of thinking about tort liability for informatics and new media professionals and paralegals, what are some of the risks you will keep in mind as you continue in your careers? Are the laws of negligence and strict liability sufficient to protect people from harms caused by information technology such as computer programs? Do they go too far?
- What about conduct using the Internet and other technologies that is intended to cause harm to people, data, computers or networks? Are the current laws and penalties sufficient to address such tactics as spam, viruses, trojan horses, worms and spyware?
- How do you see the balance between individual privacy versus government intrusion shifting? Are you concerned? Where should we draw the line in terms of allowing an employer or the government to monitor email or Internet searching and other activities using technology? What about issues related to the collection of personal information for business purposes?
- How will knowing about laws related to defamation and the rights of publicity impact what you development in terms of informatics and new media work or as a paralegal?
- From the reading assignment for Module 14, select one of the cases, describe why it is important for new media and informatics professionals and paralegals and note what it teaches us in terms of the law in that area. Are there issues in the case that are still unsettled?
- Any other interesting issues related to Module 14 or the reading assignment.

Please read the following **mini-lecture**.

As stated in the introduction to **Chapter 12** of *Legal Aspects of Managing Technology*, one cannot be involved in a high-technology enterprise without being concerned about possible tort liability. As noted on page 419, the term *tort* has a wide umbrella, covering a number of personal harms, but is generally any unwanted intrusion on a protected personal right that causes physical, economic or psychological injury. Modern technologies have actually increased both the degree and range of potential harms that individuals may suffer, thereby increasing the exposure of firms providing or working with these technologies.

The first major type of tort covered in Chapter 12 is negligence. The CoolEdge scenario on pages 419-420 demonstrates a classic case of negligent behavior. Although negligence is primarily governed by state law, there is some uniformity of approach through the Restatement of Torts. Notice that important principles in negligence include the standard of care and whether or not a person's conduct was reasonable. Other elements of the test for negligence include causation, proximate cause and defenses, as described on pages 420-423 and illustrated in Exhibit 12.1 on page 421. In terms of how courts determine whether someone has exercised the care that a reasonable person would have used under the circumstances, pages 424-245 present the case of *Vuono v. New York Blood Center, Inc.* This case makes it clear that negligent conduct cannot be defined in terms of hard-and-fast rules. What a reasonable person should do under the circumstances depends on a

number of factors and may be influenced by industry custom, legal standards and economic principles.

Strict products liability is another important concept for individuals and companies working in high-tech industries. As stated on page 426, for those companies involved in the manufacture or distribution of products, as opposed to services, the development of strict products liability principles has somewhat usurped the importance of negligence. The policy reasons for the development of the doctrine related to strict products liability are discussed on page 426. Note that the overarching principle behind imposing a strict liability standard for products is to avoid having products in the marketplace that are unreasonably dangerous. Product defects can include either manufacturing defects or design defects (see *Barker v. Lull Engineering Co.* on pages 427-230). Note that the *Barker* case represented an expansion in products liability law by requiring that design defects be evaluated both in terms of consumer expectations and by balancing risks with benefits. As alluded to in *Barker*, a third kind of product defect that can subject a manufacturer to strict liability is the failure to provide adequate warnings about possible hazards. The discussion of the Optimizer and of disposable lighters on pages 430-431 illuminate the problems in determining whether a warning is adequate and whether a warning should allow a manufacturer to escape liability for a dangerous design.

As indicated on pages 431-433, the American Law Institute published a new chapter of the Restatement of Torts in 1998 to deal specifically with issues related to strict liability. Note that 2(b) of the Restatement adopts a risk/benefit approach to determine the adequacy of product designs. Likewise, the Restatement also provides new guidance describing when a failure to warn makes a product unreasonably dangerous. It may be most helpful to concentrate on Exhibit 12.2 on pages 432-433, which provides an excellent summary of the issues in analyzing strict liability for product defects and failure to warn. In addition to state law, there are also many federal policies related to manufacturing. Note especially pages 434-435 on strict liability for computer programs. The most important federal regulatory body is the Consumer Product Safety Commission, described on pages 435-436. Various tort reform measures are always on the minds of business leaders and those who represent them, such as the Chamber of Commerce. Note the significant fines that have been assessed for failure to report product defects presented in Exhibit 12.3 on page 436.

The remainder of Chapter 12 of *Legal Aspects of Managing Technology* is devoted to finding liability for behavior that is intentional. Computer systems are vulnerable to various forms of intrusive behavior. While some kinds of behavior are clearly wrong and can be prosecuted under a number of traditional and special federal and state laws, other kinds of practices raise more unique questions. For example, the use of electronic robots to gather publicly available data may seem innocuous when in fact the robot may be intruding on a computer system run by someone else. The law of trespass to a chattel is discussed on pages 437-438. *Ebay, Inc. v. Bidder's Edge, Inc.* (see pages 438-439) is a landmark case because it was the first to evaluate the legality of software robots, which are computer programs that automate key functions over the Internet, including searching, copying and retrieving.

Spam is another consequence of the Internet and spammers have been challenged on the basis of the law of trespass, with mixed success (see pages 440-442). Therefore, state and federal legislation (CAN-SPAM) was developed to help individuals and ISPs reduce the quantity of unwanted spam. The history and elements of CAN-SPAM are presented on pages 443-446, with the major provisions of this legislation summarized in Exhibit 12.4 on page 444. The European Union also adopted a new e-commerce data protection directive that prohibits companies from soliciting new customers with email messages unless those individuals have given previous consent.

Dealing with computer viruses, trojan horses and worms has raised legal issues, particularly with how those who engage in this kind of behavior can be prosecuted under state and federal law. Fortunately, there is federal legislation, such as the Federal Computer Fraud and Abuse Act, that makes this behavior a crime and provides increased penalties, including prison time. Those responsible for transmitting computer viruses may be subject to criminal laws in foreign countries as well.

Chapter 13 in *Legal Aspects of Managing Technology* presents one of the most interesting - and controversial - aspects of our legal system, particularly considering the capabilities of technology and how it might be developed in the future. If the 1960s-1990s were all about civil rights, women's rights, the rights for persons with disabilities, etc., I really believe that the 2010s and beyond will be about privacy/individual rights. Every citizen should be informed about the right to privacy and the sources of laws that regulate privacy, which are outlined on pages 450-451. Note that what we attempt to do is balance the importance of the business or government purpose against the degree of intrusion on an individual's reasonable expectation of privacy. Recent issues that required a balancing of these interests have included drug and alcohol testing in schools and the workplace, genetic testing and polygraph testing. Other advances in technology that raise privacy concerns are biometrics, GPS systems, RFID tagging, cell phones and Google Maps. Exhibit 13.1 on page 453 illustrates the relevant considerations in analyzing privacy rights versus the goals of business or government.

A particularly interesting issue is the extent to which employers can monitor communications and personal activities in the workplace. Of course, there are many kinds of technology that allow employers to measure employee efficiency in conducting routine duties, whether through counting keystrokes, video monitoring, timing the duration of telephone calls or biometric fingerprint attendance systems. But what about monitoring an employee's Internet activity? (see pages 458-459) What about monitoring email communications? (see Exhibit 13.2 on page 460 and the case of *Smyth v. The Pillsbury Company* on pages 461-462. Pages 462-466 discuss the history and provisions of the Electronic Communications Privacy Act and how it has evolved from concerns over the interception of telephone calls (Wiretap Act) to hacking (Stored Communications Act). However, as illustrated by the case of *Fraser v. Nationwide Mutual Insurance Co.*, courts continue to be frustrated with the application of the ECPA to email. As stated on page 465, due to the uncertainties and criticisms in the courts, momentum is building for Congress to amend the statutory language of the ECPA so that the law provides reasonable expectations of privacy for email messages. The safest advice for employers that want to avoid the risk of violating the ECPA is to rely on the specific

exception that allows them to access employee communications when there has been notice and consent. Note the how the recommendations regarding electronic monitoring activities are applied to CoolEdge on pages 465-466. Exhibit 13.3 on page 467 lists the important elements of a computer use policy and how it should be presented to employees.

Another significant issue related to personal privacy is the collection of personally identifiable information. As stated on page 466, an important attribute of personal privacy is that one can act as one wants without fearing that the behavior will be recorded in a form that is accessible to public scrutiny. I knew a colleague who was a librarian for many years and, under state law, she was required to have a policy about who would have access to library records and when. She would give a regular presentation called "Is There a Spy in Your Stacks?" about the various kinds of information that the FBI, law enforcement, the media and others had requested about the borrowing and research activities of library patrons. Would it have a "chilling effect" on your use of a library if the government or law enforcement could find out what books you borrowed or what you asked the librarian to help you find? Although there are a number of laws that might prohibit specific types of behavior, as outlined on page 468, there are still not comprehensive laws that govern the collection and dissemination of personal information. Data collection on the Internet is a particularly contentious topic and pages 468-471 describe some of the technology available for this and why it is causing such concern.

Identity theft is the fastest growing crime in the U.S., so pages 471-473 should be essential reading for anyone who uses the Internet for any kind of personal, health or financial transaction. Security breaches are now almost a daily occurrence. As indicated in on pages 473, many state legislatures have passed anti-spyware laws. In fact, Indiana already has a statute covering spyware - including definitions, prohibited conduct and relief and damages.

There have been a number of legislative and regulatory actions in the U.S. to address the ways in which commercial Internet companies obtain and disseminate information. One of the basic foundations of this issue is freedom of choice. In this regard, the Federal Trade Commission (FTC) announced a set of fair information principles that it claimed were essential for websites. These principles are notice, choice, access and security. The application of these principles to the Internet environment is described on pages 475-476. Other legislative and industry initiatives include The Children's Online Privacy Protection Act (see pages 476-477) and privacy seal programs (see pages 477-478). Traditionally, European Union countries have had much stricter standards for privacy protection than the U.S. The European Union Directive on Information Privacy Protection, described on pages 478-479, had far-reaching implications for international trade because it prohibits the transfer of personal data to countries outside of the EU that do not guarantee an adequate level of protection. Because of this situation, negotiators from the EU and U.S. agreed to a safe harbor framework so that U.S. companies can continue to do business in the EU even when it involves the transfer of personal information. The recommendations for CoolEdge in terms of handling the personal information of its customers are described on pages 479-480.

The final major topic in Chapter 13 of *Legal Aspects of Managing Technology* is the extent to which the government or other entities can control the content of what is transmitted over the Internet, particularly when that content might be considered indecent. One of the early pieces of legislation that attempted to control speech on the Internet was The Communications Decency Act of 1996.

This legislation and the *Reno v. American Civil Liberties Union* case that challenged it were of great interest to me. Of course, another way to address these issues is through private control through personally-selected software filtering or rating systems. However, these mechanisms are certainly not perfect and have the potential to be manipulated. The next legislative attempt related to preventing children from accessing objectionable content was the Child Online Protection Act of 1998. The constitutionality of this legislation was also challenged in the case of *Ashcroft v. American Civil Liberties Union*. According to the Supreme Court, COPA did not meet constitutional standards because the government could not prove that the law was more effective than filtering technologies.

Another interesting issue related to children's ability to access to objectionable content over the Internet was whether public libraries should control what their patrons could view through the use of filtering software. In 2000, President Clinton signed the Children's Internet Protection Act (CIPA) into law. Although CIPA did not require public libraries to install Internet filters, it provided substantial incentives for them to do so.

As stated on page 484, the growth of electronic communication has brought new life to the old tort of defamation. One engages in defamation by making a false statement about another person to the public in a way that harms the person's reputation. Of course, the Internet and email make it much easier to disseminate information about people and companies. A line of cases attempted to determine whether ISPs would be liable for transmitting defamatory comments of its subscribers, as described on pages 485-486 and including *Sidney Blumenthal v. Matt Drudge and American Online, Inc.* on pages 487-488. Exhibit 13.4 summarizes the key aspects of defamation law in the U.S. and how the decisions have evolved. As stated on page 488, Section 230(c) of the Communications Decency Act has been an important source of protection for online service providers, including those who operate websites.

One final right is described on pages 490-491 - the right of publicity. It is very important for new media and informatics professionals to understand this legal doctrine because it provides significant limitations on the extent to which you can use the images, likeness, walk, voice, persona and individual style of a famous person in any kind of content you develop without that person's permission. In fact, Indiana has been on the forefront of the development of the right to publicity, spearheaded by a company called **CMG Worldwide** (<http://www.cmgworldwide.com/>) that manages these rights for a long list of famous people, both living and dead. The list of disputes on pages 490-491 may be helpful, because it illustrates the lengths to which movie stars, musicians and other celebrities will go to in protecting the rights to their personas.

Another violation of personal rights is the use of the Internet, including social media sites, to harass and humiliate people, a practice which is referred to as cyberbullying. There have been at least two

suicides in the Central Indiana area that have been attributed to cyberbullying. Note that the tort of intentional infliction of emotional distress has been used to sue for personal damages and that many school districts are required to develop policies to prevent cyberbullying and to take disciplinary action when needed.

Next Steps

Module 15 will include a final mini-lecture on legal issues from an international perspective. Please remember to check the Final Paper Assignment found **HERE**, **(<https://iu.instructure.com/courses/1874392/assignments/10090170>)** so that you know what to cover in the Final Paper.

Please let me know if you have questions on Module 14 or the reading assignment.