CHAPTER 12

Criminal Law and Tort Law Issues in Cyberspace

CRIMINAL LAW REFERS TO LAWS that the federal and state governments have created to define unacceptable behavior. People who violate acceptable levels of behavior commit crimes. Criminal law deals with crimes. Tort law refers to wrongful acts or harm for which an individual can sue the person who caused the harm. Tort law governs disputes between individuals.

This chapter focuses on criminal and tort law issues that are unique to cyberspace. In particular, it focuses on how people can use computers in cybercrime activities. It also reviews how people use computers to commit torts. Sometimes both criminal and tort law actions can be carried out against the same individual for the same actions.

Chapter 12 Topics

This chapter covers the following topics and concepts:

- What general criminal law concepts are
- What common criminal law issues in cyberspace are
- What general tort law concepts are
- What common tort law issues in cyberspace are
- What some case studies and examples are

Chapter 12 Goals

When you complete this chapter, you will be able to:

- Discuss common criminal law concepts
- Describe the common criminal laws used to prosecute cybercrimes
- Discuss common tort law concepts
- Describe common tort principles used in cyberspace
- Explain the difference between criminal and tort law

General Criminal Law Concepts

Cybercrimes, sometimes called computer crimes, involve situations where people use the Internet or computers as the medium for, or target of, criminal activity. Some crimes, such as computer trespass, are prosecuted by extending existing criminal laws to new situations that have arisen with new technology. Computer networks facilitate these crimes. Other laws define new crimes that didn't exist before computers. The use of computers as a medium to commit crimes is growing. Criminals also target computers and the data that they contain. Consider the following:

- A federal judge sentences a computer hacker to almost five years in prison for violating the Computer Fraud and Abuse Act. He created botnets and sold access to them. Other attackers used the botnets to launch distributed denial of service (DDoS) attacks.
- A federal judge sentences a defendant to 2.5 years in prison for taking nude videos of a news reporter and posting them to the Internet. The judge also orders the defendant to pay restitution to the victim.
- The federal government charges three members of a hacking group with hijacking the Web site of a telecommunications company. The company's users couldn't access the Web site for about 90 minutes.
- A man is charged with cyberextortion. He is alleged to have attempted to extort a life insurance company by threatening to send millions of computer spam messages. Authorities say he wanted to damage the reputation of the company.

Crimes are instances of wrongdoing, or actions that harm society. They're deviations from behavior that society, through its government, has defined as unacceptable. Some crimes don't even need individual victims. Society is the "victim" of the crime.

In simple terms, a crime is a violation of society's code of conduct. Crime and the concept of criminal law are very old. The Sumerian and Babylonian civilizations included codes of conduct in their laws in 2100 B.C.E. While these codes didn't resemble modern criminal law, they did define conduct that society decided wasn't acceptable.

The American legal system is based in large part on English common law. The U.S. Constitution is the main source of law for the United States. The Constitution presumes that U.S. citizens will behave in a lawful manner. However, it includes provisions for how the government should handle crimes in Article III. The Constitution even defines a crime. Article III, section 3, states that treason against the United States is a crime.

The U.S. Congress has passed laws regarding federal crimes since the formation of the government. Most states also have passed laws that have defined criminal offenses. Since crimes are wrongs against society, the government pursues the alleged wrongdoers. The federal government prosecutes violations of federal law. State governments prosecute violations of state laws.

> **NOTE**
>
> Federal cases are titled "United States" versus the name of the defendant. This is because the government of the United States is prosecuting the defendant for a crime. State cases are titled with the name of the state versus the name of the defendant.

Main Principles of Criminal Law

Criminal law is very different from civil law. Each system has different goals. Criminal law aims to deter wrongful behavior. It does this through a combination of punishment and rehabilitation of the offender. In contrast, civil law aims to right personal wrongs. It does this by allowing people to sue to recover monetary compensation for injuries.

This section focuses on substantive criminal law. Substantive law describes a person's rights and responsibilities. It defines how people should relate to one another and how they should relate to the government. Substantive law also is known as subject matter law. Criminal law is only one of many categories of substantive law. Contract law, business law, property law, and tort law are all different types of substantive law.

> **NOTE**
> Attorneys often specialize in different subject matter areas. This is because of legal ethics rules that require an attorney to be minimally competent. There are many areas of law. It's easier for attorneys to meet ethical competency rules by focusing their practices in certain areas.

Substantive criminal law defines the conduct that constitutes a crime. It also establishes penalties. Governments can specify criminal penalties in the same statute that defines a crime. They also can list them in a separate penalty statute.

Type of Wrongful Conduct

Society recognizes two basic types of wrongful conduct. The first type is conduct or acts that society universally agrees are wrong, morally repugnant, or dangerous to other people. For example, almost all societies agree that murder and rape are wrong. ***Mala in se*** is a Latin term that defines these types of wrongful conduct. *Mala in se* means "evil in itself." It describes conduct that's inherently wrong. Crimes that are *mala in se* include murder, rape, kidnapping, robbery, theft, and arson.

Other types of conduct are *mala prohibita*. ***Mala prohibita*** is Latin for "wrong because it is prohibited." Society defines conduct that is *mala prohibita*. This conduct isn't inherently evil, but society prohibits it. Crimes that are *mala prohibita* include intellectual property violations (where prohibited by law, such as federal copyright offenses), traffic law violations, and tax evasion. Many types of cybercrimes are *mala prohibita*.

Crimes generally are classified into two groups, misdemeanors and felonies. The two types of crimes are usually distinguishable by the way society punishes the criminals who commit these crimes. **Misdemeanors** are less serious than felonies. They bear a less severe penalty. A misdemeanor is generally punishable by no more than one year in prison.

Felonies are crimes that are more serious. They're usually punishable by more than a year in prison. The levels of felonies and misdemeanors may vary from state to state. Some states have different levels of misdemeanors and felonies. Language like "first degree" or "second degree" differentiates between different levels of crime. A state can prosecute some types of crimes as either a misdemeanor or a felony.

Elements of a Crime

Criminal law is based on the principle that a guilty mind must accompany a criminal act. Another principle is that criminal conduct harms society. In short, the American system of law holds people responsible for their actions. A government must prove the following elements to show that a crime has been committed:

- *Mens rea*
- *Actus reus*
- Causation

To prove that a crime has been committed, a government must show that a person acted with criminal intent. It must show that a person knowingly, intentionally, or recklessly engaged in criminal conduct. The Latin term ***mens rea*** means "guilty mind." *Mens rea* describes a person's intent to commit a crime. Someone who lacks *mens rea* can't be held responsible for a crime.

Most criminal laws have language that specifies the amount of *mens rea* that a person must have in order to be held responsible for a crime. For example, the Wisconsin first-degree murder statute states: "Whoever causes the death of another human being with intent to kill that person or another is guilty of a Class A felony."[1] The "intent to kill" portion of the statute describes the *mens rea* required to commit a crime.

Acts that are purely accidental don't meet the required mental showing for criminal prosecution. However, that doesn't mean that the government prosecutes only intentional actions. The government also can prosecute a person who acts recklessly for criminal behavior.

A showing of recklessness means that a person acted in a manner that consciously disregarded whether or not harm could result from the actions. For example, the Wisconsin first-degree reckless homicide statute states: "Whoever recklessly causes the death of another human being under circumstances which show utter disregard for human life is guilty of a Class B felony."[2] The "which show utter disregard for human life" portion of the statute describes the *mens rea* required to commit this crime.

Criminal statues don't require governments to prove damages in order to prosecute a defendant for a crime. However, governments can use the amount of harm that a defendant causes to increase the level of the crime.

The *actus reus* is the wrongful act that constitutes a crime. ***Actus reus*** is the Latin term for "guilty act." To be a crime, the action must be voluntary. The *actus reus* requires a physical act. For example, the U.S. Supreme Court held that a California law that punished people for being addicted to illegal drugs violated the Constitution.[3] The California law made being "addicted" to drugs the offense, even if the person who was addicted to drugs never used or possessed drugs in the state.

NOTE

Some crimes don't require a particular mental state. For example, in most states, driving a car while under the influence of drugs or alcohol is a crime. It's a crime regardless of the mental state of the driver.

NOTE

In civil law, no showing of mental state, or *mens rea*, is required. Under civil law, wrongdoers are responsible for their actions even if they didn't intend to cause harm to another person.

In *Robinson v. California* (1962), the U.S. Supreme Court said that there were many ways that the state could make certain acts related to drug use illegal. However, simply making the status of being an addict illegal was a violation of the Constitution. The case stands for the proposition that criminal activity requires a voluntary, physical act.

A wrongful act also can include the failure to act when there's a duty to do so. For example, parents have a duty to care for their children. A state may punish a parent that fails to take care of his or her children when that failure rises to a level of criminal conduct. For instance, in March 2010 the South Korean government arrested a couple for child neglect. The government alleged that the couple's video game addiction led them to neglect their daughter. The child starved to death. Sadly, the video game that the couple was addicted to involved caring for a "virtual child" in an online game.[4]

Jurisdiction

Courts have the ability to hear only *cases*, or disputes, that are within their jurisdiction. Jurisdiction describes the types of cases that a court has the authority to hear.

Jurisdiction can be described in a number of different ways. Jurisdiction can be used to describe the function of a court. For example, trial courts generally have original jurisdiction. This is the ability to conduct trials and to hear initial disputes between parties. Appellate courts like the U.S. Supreme Court have appellate jurisdiction. They can only review decisions made by lower courts.

Jurisdiction also can describe the power of a court to hear a certain type of case and make a binding decision in that case. Courts must have the proper jurisdiction in order to make valid judgment. In order to make a valid judgment, a court must have:

- Subject matter jurisdiction
- Personal jurisdiction

Subject matter jurisdiction is the power of a court to decide certain types of cases. A court can't decide cases where it has no subject matter jurisdiction. For example, federal courts have jurisdiction only to decide cases about federal laws. This is federal question jurisdiction. They also can decide certain types of disputes between citizens of different states. This is diversity of citizenship jurisdiction. In contrast, state courts can decide only cases about state laws or actions that occurred within the geographic boundaries of the state.

FYI

In both state and federal court, jurisdiction also looks at geographical and political boundaries. If a person violates a federal law in Massachusetts, federal district courts in Massachusetts most likely have subject matter jurisdiction to decide the case. If the person violated only a state law, Massachusetts state courts would have jurisdiction to decide the case.

Personal jurisdiction refers to a court's ability to exercise power over a particular defendant. If a court doesn't have personal jurisdiction over a defendant, then it can't impose a sentence on that person. Personal jurisdiction is important for both criminal and civil cases. Typically, state courts can exercise personal jurisdiction over people who commit acts within the state.

For criminal law, personal jurisdiction comes into play when criminal acts are committed in a number of different states. It's also implicated when crimes affect residents in a number of different states. The U.S. Supreme Court addressed this issue in 1911.[5] In *Strassheim v. Daily*, the Supreme Court used a "detrimental effects" test to determine if a state could exercise criminal jurisdiction over a person who committed acts outside of the state. The Court's test had three parts:

- Did the act occur outside the state?
- Did the act produce detrimental effects within the state?
- Were the acts the actual cause of detrimental effects within the state?

The test focuses on the defendant's intent. It also looks at the consequences of the defendant's actions in a particular state. Under the detrimental effects test, a state criminal court can exercise jurisdiction over a person who commits actions outside of the state if those actions cause harm within the state.

The Supreme Court's detrimental effects test used in the *Strassheim* case is a common law rule. Many states have enacted legislation that codifies the detrimental effects test. For example, Alaska law states that state courts have jurisdiction over crimes that are "commenced outside the state but consummated inside."[6]

Issues about jurisdiction aren't just questions between the states. Personal jurisdiction also can be an international issue. It's one of the main obstacles in cybercrime cases. This is because of the truly global nature of the Internet. The Council of Europe Convention on Cybercrime increases cooperation in the investigation and prosecution of cybercrimes. It went into force in 2004. Members of the convention must adopt legislation to criminalize certain types of cyberoffense and copyright infringement. They also agree to assist one another in criminal investigations. Fifty-three nations have signed the Convention on Cybercrime; forty-two nations have ratified it.[7] The United States ratified the treaty in August 2006.

NOTE

The United Nations is to discuss international cooperation to fight cybercrime at its 13th Congress on Crime Prevention in Criminal Justice in April 2015. You can view the agenda at *http://www.huffingtonpost.com/2012/10/17/sarah-palin-hacker-david-kernell_n_1973641.html.*

Jurisdictional Issues for Cybercrime Cases

Jurisdiction is a particularly challenging issue with respect to cybercrimes. Geographical boundaries don't limit computer networks. Cybercriminals can easily commit crimes that span across states and countries. This makes it difficult for law enforcement to investigate these crimes. It's particularly difficult for law enforcement to identify criminals and collect evidence across the globe. It also makes it difficult for courts to hold cybercriminals responsible for their actions.

Nigerian scams highlight the jurisdiction issues in cybercrime cases. These types of scams also are called "419 scams" or "advance fee fraud" schemes. This type of scam has been around since the early 1900s, when it was called the Spanish Prisoner Con. Today it's associated with the country of Nigeria. The "4-1-9" refers to the section of the Nigerian criminal code that addresses fraud schemes.

Criminals originally conducted these scams via fax or mailed letters. They now conduct them with ease through e-mail. In a Nigerian scam, a person receives an e-mail from someone purporting to be an official of a foreign government or agency. The e-mail writer usually offers large sums of money in return for helping someone in trouble. In some cases, the e-mail claims that the Nigerian government has made it difficult for the wealthy writer to cash a large check. The writer asks the victim to advance the victim's own funds to cover the check, and to help cash it. The writer promises that the victim will get a hefty reward for his or her assistance.

A victim who advances funds soon learns that the check or underlying business transaction is fraudulent. The money advanced is lost. People operating outside the United States who send targeted e-mails to U.S. residents commit many of these types of crimes.

These cases are extremely difficult to investigate and prosecute. How would a victim in Lafayette, Indiana, be able to use the resources of local law enforcement to investigate a crime committed by a person that lives in another country? Local police, prosecutors, and courts have limited power to investigate and prosecute these types of international cases. State subpoenas and court orders don't usually apply across international boundaries. These jurisdictional issues are becoming more common as Internet crime grows.

The Federal Trade Commission (FTC) has issued a consumer alert about Nigerian scams. You can read about it at *http://www.consumer.ftc.gov/articles/0002l-nigerian-email-scam.*

Criminal Procedure

Criminal procedure is the body of rules that govern how governments prosecute people for crimes. These procedural rules make sure that criminal defendants receive due process. Under *due process*, a defendant in a criminal case is entitled to a fair and consistent process within the courts. The laws of criminal procedure make sure that the government safeguards the defendant's constitutional rights. They also provide the government with a method for fairly prosecuting defendants for their crimes.

FYI

A *prosecutor* is a government official who represents the government in criminal cases. Prosecutors decide whether to charge a person with a crime and put on the court case against that person. *U.S. Attorneys* are federal prosecutors. States usually grant prosecutorial power to county governments. State prosecuting attorneys might be called district attorneys, county attorneys, state's attorneys, or simply county prosecutors.

Most criminal procedure principles stem from the U.S. Constitution. This means that many processes are similar among the states and the federal government. However, there are some procedural rules that are unique to each jurisdiction. The description provided here is intentionally general. The process also can be different depending upon whether the crime committed is a misdemeanor or felony.

A criminal case begins when a law enforcement agency begins an investigation. Law enforcement agencies have certain rules that they must follow as they conduct their investigation. When law enforcement officers complete their investigation, they send the case to the prosecutor.

A prosecutor then reviews the case and decides whether to bring charges against the person that law enforcement identified as the perpetrator of the crime. Prosecutors have a lot of discretion in determining whether to charge a person with a crime.

A prosecutor who decides to charge a person with a crime must file a written document in court to start the criminal process. In some states, a prosecutor may file a document called an *information*. An information specifies the charges against the perpetrator of the crime. The prosecutor can exercise discretion when filing an information.

In other states, defendants have a right to a grand jury indictment. A *grand jury* is a panel of citizens who hear evidence presented by a prosecutor. The grand jury determines if there's enough evidence to bring a person to trial for a crime. The grant jury issues an *indictment* if it determines that the evidence is sufficient. An indictment is the formal written criminal charges issued by a grand jury. At this point, the perpetrator of the crime becomes a *defendant*. In a criminal case, the defendant is the person accused of a crime.

FYI

The Fifth Amendment to the U.S. Constitution requires that a federal grand jury issue charges for some federal crimes. A defendant can waive the grand jury requirement. If a defendant waives the grand jury requirement, then the federal prosecutor files an information to start criminal proceedings. Federal grand juries contain between 16 and 23 people. The Federal Rules of Criminal Procedure sets this number. Grand juries conduct their deliberations in secret. You can read the Handbook for Federal Grand Jurors at *http://www.uscourts.gov/Viewer.aspx?doc=/uscourts/FederalCourts/Jury/grand-handbook.pdf*.

A criminal prosecution begins once a grand jury returns an indictment or after a prosecutor files an information. The next step in the criminal process is the *initial hearing*. This is sometimes called an *arraignment*. The purpose of this hearing is to begin the formal court process. At this hearing, a court must:

- Inform the defendant about the charges
- Advise the defendant about his or her legal and constitutional rights

At this point, the defendant must enter a response to the charges. This response is a *plea*. A defendant can enter a plea of guilty or not guilty. In some cases, she or he also can enter a plea of *nolo contendere*. *Nolo contendere* is Latin for "I do not wish to contend." It's also called a plea of no contest. A no contest plea isn't a guilty plea. However, it has the same effect as one. Most jurisdictions have limits on how and when defendants can use this type of plea.

If a defendant enters a guilty plea, the court will set a date to sentence the defendant. In 2009, the U.S. Department of Justice issued a special study on felony sentences in state courts. That study found that 94 percent of felony defendants pleaded guilty in state court cases.[8] In 2010, 91 percent of felony defendants pleaded guilty in U.S. federal district court cases.[9]

NOTE

The defendant's right to an attorney arises when a criminal proceeding begins. A defendant may voluntarily waive the right to counsel and represent himself or herself. A court must decide that a person is mentally competent in order to do this. The court also must warn the person that there are dangers to self-representation.

If the defendant enters a not-guilty plea, the court sets the case for trial. The U.S. Constitution guarantees criminal defendants the right to a trial by jury. Article III of the Constitution guarantees this right. The Sixth Amendment to the Constitution clarifies the scope of the right.

Under the Sixth Amendment, criminal defendants are entitled to a court-appointed attorney if they can't afford one on their own. Courts usually grant this request only when a defendant faces a prison sentence. The Supreme Court case of *Gideon v. Wainwright* (1963) held that a court must appoint an attorney to an indigent defendant charged with a felony.[10] The defendant must prove that he or she is indigent and can't afford an attorney. The Supreme Court in the *Gideon* case also held that a conviction is automatically reversed if a state denies a defendant the right to counsel.

After the arraignment, the prosecution and the defendant's attorneys will begin the discovery process. *Discovery* is the process where the government gives the defendant the evidence that it plans to use in the defendant's trial. U.S. Supreme Court cases have held that the government must disclose:

- Any deals that the prosecution made with a witness *(Giglio v. United States)*.[11]
- Any evidence it has that might help prove the defendant's innocence *(Brady v. Maryland)*.[12]

Courts strictly regulate the criminal discovery process. The rules for the process are clear. A court has a wide range of actions it can take against parties that fail to comply with discovery rules. A court can even dismiss the case if the prosecution fails to comply

with the rules of the process. Failure to turn over evidence that might help prove the defendant's innocence can cause a conviction to be overturned.

If a criminal case goes to trial, the government bears the burden of proving that the defendant violated the law. In criminal cases the government must prove the defendant's guilt beyond a reasonable doubt. This is the highest burden of proof that a prosecutor must meet. Reasonable doubt doesn't mean that a juror is 100 percent convinced of the defendant's guilt. It does mean, however, that a juror must be fully satisfied that the prosecution has eliminated reasonable doubt about the defendant's guilt.

> **NOTE**
>
> The Sixth Amendment to the U.S. Constitution guarantees defendants a speedy trial. State criminal procedure rules include time limits for all the steps in the criminal process. In *Strunk v. United States* (1973), the U.S. Supreme Court held that a court must dismiss a criminal charge if a state violates the defendant's speedy trial rights.[13]

The government has a high burden of proof in criminal cases because criminal punishments infringe on a person's fundamental rights. These rights include the right to liberty, property, and life. Criminal penalties can include jail time, probation, financial penalties, or even a death sentence. A court may impose these penalties only if the government meets its high burden of proof.

A criminal case ends when a jury decides that a defendant is innocent or guilty. It also ends if the jury can't reach a decision. A *hung jury* is a jury that is unable to reach a decision because the jurors disagree. A court will declare a *mistrial* if the jury can't reach a decision. In this case, the government may decide to refile the charges and prosecute the defendant again.

A defendant who is convicted may appeal. There are different rights that allow a defendant to appeal a ruling or conviction to a higher court. These rules are beyond the scope of this discussion.

Common Criminal Laws Used in Cyberspace

It's important to distinguish three different types of crimes: crimes that may now be committed using computers, crimes that use computers or the Internet as a medium to commit a crime, and crimes where the computer is the target of the crime. The first example isn't cybercrime. For example, a person simply using a computer and printer to create a forged document commits a criminal act. It's no different than if that same person used a printing press and ink to forge the document. The crime is still a forgery. In this example, the computer is a tool used to commit the crime.

Cybercrimes are different. Cybercrimes also are called computer crimes. Cybercrimes are crimes that use computers as a medium to commit crime or where the computer itself is the target of the crime. Cyberstalking, identity theft, and phishing scams are examples of crimes facilitated by computers. Denial of service (DoS) and DDoS attacks, computer viruses, and communications sabotage are examples of crimes where the computer itself is the target of the crime. The distinction between the types of crime is subtle, but important.

Both the federal government and individual states have created a number of laws that address cybercrime. This chapter talks primarily about federal cybercrime laws. It's likely that federal laws will have the most impact on cybercrime. This is because geography or state and national borders don't matter to cybercriminals. The Internet truly blurs these lines. A criminal can easily initiate a cybercrime in one state and harm a victim in another. In addition, since cybercrime statues vary widely between the states, federal laws may end up being more comprehensive.

> **NOTE**
> It's important to remember that many states criminalize the same behavior that federal cybercrime laws address.

The Computer Fraud and Abuse Act (1984)

Congress passed the Computer Fraud and Abuse Act (CFAA) in 1984.[14] It's the first piece of federal legislation that identified computer crimes as distinct offenses. The CFAA provides both criminal and civil penalties. In enacting the CFAA, Congress chose to address computer-related offenses in a single statute. The CFAA limits federal jurisdiction to situations where cybercrime is interstate in nature or when the computers of the federal government are the target of crime.

> **NOTE**
> The Internet Crime Complaint Center (IC3) is a partnership between the U.S. Federal Bureau of Investigation (FBI) and the National White Collar Crime Center. Their 2013 "Annual Report on Internet Crime" showed that the total loss linked to online fraud was $525.4 million.[15] You can read the report at *http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf.*

Congress amended the CFAA with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. PATRIOT Act) in 2001. It amended the CFAA again in 2008. These amendments increased the penalties for CFAA violations. They also lowered the required damage thresholds in light of terrorism and identity theft concerns.

The CFAA criminalizes the act of causing certain types of damage to a protected computer. A protected computer is any of the following:

- A federal government computer
- A financial institution computer
- A computer used in interstate or foreign commerce[16]

The definition of a protected computer is very broad. Under the statute, the Internet is a protected computer because the Internet facilitates commerce between different states. The CFAA definition of "financial institution" includes organizations that provide financial services to customers such as banking, investment, and insurance services.

The CFAA addresses the following types of criminal activity:

- Unauthorized access of national security information
- Unauthorized access to a government computer
- Compromising the confidentiality of a protected computer
- Unauthorized access to a protected computer with an intent to defraud
- Unauthorized access to a protected computer that causes damage

- Intentional transmission of malware, viruses, or worms that damage a protected computer
- Unauthorized trafficking of passwords or other computer access information that allows people to access other computers without authorization and with the intent to defraud
- Extortion involving threats to damage a protected computer

The CFAA doesn't just address intruders or outsider attacks on protected computers. It also takes into account that insiders may exceed the access that they have been granted in a protected computer system. Since these people already have access to these systems, their access isn't unauthorized. However, in some cases, they commit a crime if they exceed their scope of authorized access. Under the CFAA, a person exceeds authorized access when he or she accesses a computer with authorization, but uses that access to get or alter information that he or she isn't allowed to use or alter.

Insiders can be charged under the CFAA with exceeding authorized access if they access national security information inappropriately. They also can be charged if they compromise the confidentiality of a protected computer, or exceed their authorization in a protected computer with intent to defraud.

Some sections of the CFAA require the government to show that the intruder caused damage. Under the CFAA, "damage" is whatever does any of the following:

- Causes loss of $5,000 or more of total damage during one year
- Modifies medical care of a person
- Causes physical injury
- Threatens public health or safety
- Damages systems used by or for government entity for administration of justice, national defense, or national security
- Causes or attempts to cause death or serious bodily injury

The federal government uses the CFAA to prosecute many different computer crimes. It used the CFAA to charge a 20-year-old University of Tennessee student with unauthorized e-mail access. In late 2008, the student accessed Vice Presidential candidate Sarah Palin's personal Yahoo! e-mail account. The student then posted her e-mail messages online. A criminal grand jury indicted the student under the CFAA and the federal Electronic Communications Privacy Act (ECPA). In April 2010, a jury convicted the student of unauthorized access to a computer and obstruction of justice. The convinction was upheld on appeal.[17]

> **NOTE**
> The federal government used the CFAA in 1990 to prosecute the creator of the Morris worm. This was the first prosecution under the CFAA.

Table 12-1 summarizes the Computer Fraud and Abuse Act provisions and potential penalties. In all instances the penalties described below are increased significantly if a defendant has a previous CFAA conviction.

TABLE 12-1 Computer Fraud and Abuse Act summary.

CRIMINAL ACTIVITY	ACTION	ADDITIONAL ELEMENTS	PENALTY
Obtaining National Security Information	Unauthorized access Access in excess of authorized access		Felony. A defendant can receive a fine, or 10 years in prison, or both.
Trespass in a government computer	Unauthorized access	Access must affect use of the government computer (low threshold to meet)	Misdemeanor. A defendant can receive a fine, or up to one year in prison, or both.
Compromising confidentiality of a protected computer	Unauthorized access Access in excess of authorized access		Misdemeanor. A defendant can receive a fine, or up to one year in prison, or both. The defendant also can be sentenced for a felony and up to five years in prison if aggravating factors exist.
Access of a protected computer	Unauthorized access Access in excess of authorized access	Intent to defraud	Felony. A defendant can receive a fine, or up to five years in prison, or both.
Access of a protected computer that causes damage	Unauthorized access	Must cause damage: • Intentionally • Recklessly • Negligently	Different penalties depending upon *mens rea* for damage caused • **Intentional:** Felony. A defendant can receive a fine, or 10 years in prison, or both. The defendant also can receive 20 years in prison for subsequent convictions or causing damage leading to serious bodily injury. A defendant can receive life imprisonment if the offense causes or attempts to cause death. • **Reckless:** Felony. A defendant can receive a fine, or five years in prison, or both. • **Negligent:** Misdemeanor. A defendant can receive a fine, or up to one year in prison, or both.

TABLE 12-1 Computer Fraud and Abuse Act summary, *continued.*

CRIMINAL ACTIVITY	ACTION	ADDITIONAL ELEMENTS	PENALTY
Transmission of malware, viruses, or worms that damage a protected computer	Intentional transmission	Must cause damage	Felony. A defendant can receive a fine, or 10 years in prison, or both.
Trafficking in passwords	Knowing, with intent to defraud	Affects interstate commerce or computer used by government	Misdemeanor. A defendant can receive a fine, or up to one year in prison, or both.
Threatening to damage a computer	Intent to extort	Transmits threat in interstate or foreign commerce	Felony. A defendant can receive a fine, or up to five years in prison, or both.

Computer Trespass or Intrusion

The Computer Fraud and Abuse Act is the main federal law addressing cybercrime. In addition to the CFAA, the federal government has a number of other laws that address computer trespass or intrusion. These laws generally address computers that the U.S. government owns or controls. Some laws, such as the CFAA, expand this definition to include computers used in interstate commerce.

State Laws Against Computer Trespass

It's important to keep in mind that states also may have computer trespass statutes that prohibit unauthorized access to computer systems or networks. Depending on the jurisdiction, these crimes have a variety of names. In many states, the mere act of intentionally entering a computer system or network without permission is a crime. In most jurisdictions, first-time computer trespass is a misdemeanor. The penalties for computer trespass may escalate if a person is charged and convicted of more than one offense.

Most trespass statutes address only unauthorized access into a computer system. They stop short of addressing actual computer tampering, access of information, or the injection of computer viruses or worms. These types of crimes, which are malicious in nature, typically are addressed in other statutes.

Federal law addresses fraud and related activity in connection with access devices. It outlaws the production, use, or sale of counterfeit or unauthorized access devices.[18] Access devices include any item that can be used to obtain money, goods, or things of value. They include items such as card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications services. A person who violates this law commits a felony. He or she can be imprisoned for 10 to 20 years depending upon the nature of the violation.

Theft of Information

Theft of information via computer networks is on the rise. Most of these crimes take the form of theft of personal identifying information or financial information. Financial gain is nearly always the motive for these crimes. In 2014, the U.S. Federal Trade Commission (FTC) announced that identity theft was number one on its list of top 10 consumer complaints for 2013.[19]

The federal Identity Theft and Assumption Deterrence Act (1998) makes identity theft a federal crime.[20] If a person violates the law, she or he is subject to criminal penalties of up to 15 years in prison. This period increases to 30 years in special circumstances. Violators also can be fined. They also must give any personal property used to commit identity theft crimes to the government.

> **NOTE**
>
> The FTC's identity theft Web site provides useful information about preventing identity theft. You can read it at *http://www.consumer.ftc.gov/features/feature-0014-identity-theft.*

This law recognizes that the victims of identity theft aren't just the businesses that grant credit. The person whose identity was stolen also is a victim. The law also requires the FTC to keep a record of identity theft complaints. The FTC must give identity theft victims educational materials to help them repair any damage to their credit and personal data.

The law makes it illegal for anyone to knowingly transfer or use another person's identification with the intent to commit a crime. Under the law, an identification document is any document made or issued by the federal or a state government. Identifying information includes items you may be familiar with as *personally identifiable information*, such as name, Social Security number, and driver's license number. It also includes:

- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation
- Unique electronic identification number, address, or routing code
- Cellular telephone electronic serial number
- Any other piece of information that may be used to identify a specific person

The U.S. Secret Service, FBI, U.S. Postal Inspection Service, and Social Security Administration's Office of the Inspector General all have the power to investigate crimes committed under this law.

Interception of Communications Laws

Federal laws that address the illegal interception of communications forbid the use of eavesdropping technologies without a court order. Communications covered by the statutes include e-mail, radio communications, electronic communications, data transmission, and telephone calls. The federal Wiretap Act (1968, amended) governs real-time interception of the contents of a communication.[21]

> **NOTE**
> The Pen Register and Trap and Trace Statute governs access to the real-time interception of headers, logs, and other transmission information.[22]

The Electronic Communications Privacy Act (1986) governs access to stored electronic communications.[23] This includes access to the contents of the communication and the headers and other transmission information. The ECPA is an amendment to the original Wiretap Act.

The U.S.A. Patriot Act amended both the Wiretap Act and ECPA. The Patriot Act enhances law enforcement tools to intercept electronic communications to fight computer fraud and abuse offenses.

Spam and Phishing Laws

Congress created the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act in 2003.[24] The act covers unsolicited commercial e-mail messages. These messages are known as spam. **Spam** is electronic junk mail. It's unsolicited e-mail that a user may receive. Spam is a nuisance to the recipient. The CAN-SPAM Act has both civil and criminal provisions.

The CAN-SPAM Act requires commercial e-mail senders to meet certain requirements. Commercial messages are messages with content that advertise or promote a product or service. The act also forbids sending sexually explicit e-mail unless it has a label or marking that identifies it as explicit.[25]

Commercial e-mail message senders must meet the following CAN-SPAM requirements:

- Don't use false or misleading header information
- Don't use deceptive subject lines
- Identify the e-mail message as a commercial advertisement
- Include a valid physical postal address
- Inform message recipients how to opt out of future e-mail messages
- Promptly process opt-out requests
- Monitor the actions of third parties that advertise on the sender's behalf[26]

> **NOTE**
> The FTC helps businesses understand the CAN-SPAM Act. You can view their business compliance guide at *http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business.*

Each separate e-mail sent in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.[27] The FTC enforces the civil provisions of the Act. It also has promulgated rules for businesses to follow.

The CAN-SPAM Act also has criminal provisions. It includes penalties for:

- Accessing another person's computer without permission to send spam
- Using false information to register for multiple e-mail accounts or domain names
- Relaying or retransmitting spam messages through a computer in order to mislead others about the origin of the e-mail
- Harvesting e-mail addresses or generating them through a dictionary attack
- Taking advantage of open relays or open proxies without permission in order to send spam[28]

The U.S. Department of Justice enforces the criminal provisions of the CAN-SPAM Act. Criminal penalties include fines or imprisonment of up to five years.

The first conviction under the CAN-SPAM Act occurred in 2004. In that case, the defendant searched for unprotected wireless access hotspots and exploited them to send spam messages. The spam messages advertised pornographic Web sites. Eventually the court sentenced the defendant to three year's probation and six months of home detention. He also had to pay a $10,000 fine.

Spam e-mail messages also can be phishing attempts. They're scams that typically take place via e-mail or instant messaging. They're a form of Internet fraud where attackers attempt to steal valuable personal information from their victims.

There's no federal anti-phishing law. However, phishing attacks can be prosecuted under a number of different federal laws. This includes many of the laws already discussed in this section. For example, if the phishing attackers are attempting to steal personal information, they may be committing identity theft. The federal Identity Theft and Assumption Deterrence Act would apply. They also may be committing computer fraud or access-device fraud. Some phishing attacks also can be prosecuted under the CAN-SPAM Act.

If a phishing attack includes malicious activity, such as spreading computer viruses, then the Computer Fraud and Abuse Act would apply. Phishing scams also can violate state laws on fraud and identity theft.

Cybersquatting

Cybersquatting is the bad-faith registration of a domain name that is a registered trademark or trade name of another entity. Congress created the Anti-Cybersquatting Consumer Protection Act (ACPA) in 1999.[29] It's designed to stop people from registering domain names that are trademarks that belong to other entities.

The ACPA allows entities to sue cybersquatters. To prove such a case, the plaintiff must show that the cybersquatter registered the trademark in bad faith with intent to profit from the registration. The ACPA includes nine factors that help a court determine bad faith.[30] Those factors are:

- A person's intellectual property rights in the domain name
- Whether the domain name consists of the legal name of the person
- The person's prior use of the domain name in connection with the sale of goods or services
- The person's noncommercial or fair use of the domain name
- The person's intent to divert consumers from the mark owner's own Web site
- The person's offer to sell the domain name without having used the domain name for the sale of goods or services
- Whether the person gave false or misleading contact information when registering the domain name
- Whether the person registered multiple domain names that are identical or confusingly similar to marks owned by others
- Whether the mark incorporated in the domain name is famous and distinctive

Under the law, a plaintiff can recover damages and ask the court to issue an injunction that stops the cybersquatter from using the contested domain name. The court also can award statutory damages of up to $100,000 per domain name violation. Courts also can award the contested domain name to the winning party.

Malicious Acts

Common malicious information security acts include malware, worms, viruses, and Trojan horses. For the most part, the federal government can prosecute these types of activities under the Computer Fraud and Abuse Act.

Under the CFAA, the intentional transmission of malware, viruses, or worms that damage a protected computer is a felony. Remember that for the purposes of the CFAA, almost any computer connected to the Internet is a protected computer. The government can charge people who violate this provision of the CFAA with a felony. They can be punished with up to 10 years in prison.

Cyberstalking is also a malicious act. Cyberstalking is the use of the Internet to stalk another person in a threatening way. Cyberstalkers could use e-mail, instant messages, blogs, social networking platforms, and even entire Web sites to target their victims. Cyberstalking is sometimes also referred to as cyberharassment.

Many traditional state laws on stalking and harassment have been updated to include language about cyberstalking. Like many other cybercrimes, cyberstalking often crosses state borders. At the federal level, cyberstalking is prohibited under a number of different laws:

- **The Telephone Harassment Act**—Makes it illegal to use the Internet to transmit any message to harass or threaten another person.[31]
- **The Interstate Stalking and Prevention Act**—Makes it illegal for anyone who travels across states to use any interactive computer service to cause substantial emotional distress.[32]
- **The Interstate Communications Act**—Makes it illegal to transmit in interstate commerce any threat to injure another person.[33]

Cyberbullying is closely related to cyberstalking. The distinction is that cyberbullying is harassment that takes place between school-aged children.[34] Depending on the situation, state cyberbullying or cyberstalking laws tend to apply most in these situations. Currently, no federal law directly addresses cyberbullying. The federal government has attempted to expand the use of the Computer Fraud and Abuse Act into the area of cyberbullying with little success.

In 2008, the Department of Justice indicted Lori Drew for violating the CFAA.[35] The government argued that her activities on a social networking service exceeded her authorization in the use of a protected computer. She exceeded her authorized access by using the site in excess of the use authorized by the site's terms of service agreement. A jury found her guilty of a misdemeanor CFAA violation. That conviction was set aside in August 2009. The judge found that there were several problems in applying the CFAA to the case.[36] The government didn't appeal the judge's reversal.

> **NOTE**
> Learn more about preventing cyberbullying at *www.stopbullying.gov*.

Well-Known Cybercrimes

The list of well-known cybercrimes changes every day. The Computer Fraud and Abuse Act is the "go to" act for federal prosecution of cybercrime. It's very broad, and almost any type of Internet-related crime involving computers will fall within its scope. Prosecutors often include CFAA charges with other federal criminal charges if a computer is involved in the commission of a crime.

Some cybercrimes are well known because they were "first." For example, the Morris worm was one of the first computer worms on the Internet. At the time, it infected and overwhelmed a number of government systems. The creator of the worm was the first person charged with violating the Computer Fraud and Abuse Act.

The CFAA also was used to prosecute the creator of the Melissa virus. When it was released, the Melissa virus was one of the fastest-moving and most destructive viruses. David Smith created and distributed the Melissa virus in 1999. The virus caused more than $80 million in damage. He was sentenced to 20 months in federal prison in May 2002. He also was fined $5,000.

Other cybercrimes are well known because they're the biggest. For instance, one of the hackers in the TJX Companies, Inc. case received the harshest-ever sentence for a hacking case in March 2010. The federal government had charged him with violating the CFAA, federal laws related to access device fraud, and the Identity Theft and Assumption Deterrence Act. The hacker, Albert Gonzalez, was sentenced to 20 years in prison. He was also fined $250,000.

> **NOTE**
>
> You can learn how the federal government is prosecuting cybercrime by visiting the Department of Justice Computer Crime and Intellectual Property Web page. The "Press Releases" page lists recent cybercrime prosecutions. The Web page is available at *http://www.justice.gov/criminal/cybercrime/.*

General Tort Law Concepts

A *tort* is some sort of wrongful act or harm that injures a person. A person who is injured by a tort may sue the wrongdoer for damages. The word tort is from the Latin word *tortus,* which means wrong or twisted.

In the United States, tort law has evolved from English common law. Many states give either common law or statutory recognition to most torts. When states enact tort laws, they typically are trying to expand or limit common law tort liability.

Common law tort principles are similar among the states. The American Law Institute has prepared a review of tort law. The *Restatement (Second) of the Law of Torts* summarizes the common law tort rules.

> **NOTE**
>
> A **tortfeasor** is a person who commits a tort. In this discussion, a person charged with committing a tort is called a defendant. A plaintiff is the person allegedly injured by the defendant's actions.

Tort law is based on the premise that people should go about their daily business in a way that doesn't harm other people or their property. So long as people are acting reasonably, this is easy to accomplish. Tort law allows people a way to recover for their injuries if another person doesn't act reasonably.

Tort law uses the reasonable person standard to determine whether a person acts appropriately. Courts use this standard to determine if a person acts reasonably in response to a particular situation. This standard determines whether conduct is tortious.

> **NOTE**
>
> *Tortious conduct* is wrongful conduct. It's conduct that is unreasonable given the situation.

There are three types of torts. They are:

- Strict liability torts
- Negligent torts
- Intentional torts

This section will briefly describe all three types of torts. However, you should keep in mind that most torts involving computers probably will fall under the intentional torts category.

Strict Liability Torts

Strict liability is a legal concept that means that people can be held responsible for their actions even if they didn't intend to cause harm to another person. A number of areas of law apply this concept.

In tort law, a person is held liable for strict liability torts regardless of intent or negligence. Courts usually impose strict liability theories in unreasonably dangerous situations. These are situations where even a reasonable person can't prevent risk. The main reason for imposing strict liability is to discourage unreasonably risky behavior.

The classic example of a strict liability tort is when a person keeps wild animals as pets. Wild animals are inherently dangerous. Even if the owner of the animal takes reasonable precautions, there's still a risk to the public if the animal escapes. If an animal were to escape and injure a person, courts would hold the owner liable for any damages that the animal caused. Courts hold the owner liable even if the owner takes every precaution available to ensure safety.

In a tort based on strict liability, the plaintiff must show that the defendant engaged in unreasonably dangerous activities. The plaintiff also must show that he or she was harmed. The defendant bears the burden of proving that the activities were not unreasonably dangerous.

Negligence Torts

Negligence torts are based on the premise that a person is liable for any injuries or harm that are the foreseeable consequences of his or her actions. In order to prove a negligence-based tort, a plaintiff must show that:

- The defendant owed the plaintiff a duty of due care
- The defendant breached his or her duty
- The breach of duty caused the plaintiff's foreseeable injuries
- The plaintiff was damaged

Plaintiffs must prove that the defendant owed them a **duty of due care**. A duty of due care is a person's obligation to avoid acts or omissions that can harm others. The level of duty that one person owes to another is based on the reasonable person standard. The reasonable person standard is a legal concept used to describe how an ordinary person would think and act. The plaintiff will present evidence on what a reasonable person in a similar circumstance would have done. This evidence shows the level of care that the defendant owes the plaintiff.

> **NOTE**
>
> The standard of care for professionals in learned occupations is important in professional malpractice cases.

There are special duty of due care rules for people in learned occupations. Learned occupations are professions where special training and skill are required. Under the law, people in these occupations are held to a higher standard of care. They are held to a standard that's reasonable for members of that profession. For example, a lawyer's duty of due care toward his or her clients is based on a reasonable lawyer standard. Doctors, architects, engineers, and airplane pilots are held to reasonableness standards based on their professions.

The plaintiff must show that the defendant breached a duty of due care. That is, the plaintiff must prove that the defendant's behavior fell below what a reasonable person would have done in the same situation. The plaintiff will compare the defendant's behavior against the evidence that was used to show that the defendant had a duty of due care. The plaintiff can show that the defendant breached his or her duty by showing that the defendant acted in a way that was unreasonable given the situation and the defendant's duty.

NOTE

A plaintiff also can prove a breach of duty by showing that the defendant failed to take a required action. This is called an omission.

The Reasonable Information Security Professional

Torts based on a professional's duty to provide competent services are among the oldest negligence torts. Is an information security professional a member of a learned occupation? Will information security professionals be held to a "reasonable security professional" standard when giving advice to clients? There's some argument that this could be the case sometime in the future.

Information security as a career path continues to evolve. Many information security professionals are highly educated individuals who are experts in their fields. Most of them have certifications in various technical aspects of information security. Many computing vendors offer technology-specific security certifications for their products.

A number of independent organizations offer security-related certifications as well. The International Information Systems Security Certification Consortium $(ISC)^2$ grants certifications to many information security professionals. This organization certifies that information security professionals have varying levels of experience and knowledge in the field. You can learn about $(ISC)^2$ at *http://www.isc2.org/*.

The Global Information Assurance Certification (GIAC) program also grants information security certifications. It offers special certifications in areas such as audit, intrusion detection, and operating system security. These certifications test technical skills. Many information security professionals hold GIAC certifications. You can learn about GIAC at *http://www.giac.org/*.

Both $(ISC)^2$ and GIAC require certificate holders to follow a code of ethics. Each group has a code that defines acceptable levels of behavior for certificate holders. Both codes require certificate holders to act responsibly when giving information security advice. These organizations also require certificate holders to engage in activities that keep their information security skills up to date.

As of this writing, no U.S. court has recognized a professional duty for information security professionals. Think about whether information security certifications and the ethical obligations that they sometimes require could be used to show that information security professionals are part of a learned profession. Could this change how information security professionals help their clients secure information systems?

For example, a plaintiff may be able to establish that people have a duty to keep their sidewalks free from ice in the wintertime. To prove that the defendant breached this duty, the plaintiff would present evidence that the defendant didn't shovel his or her sidewalks. The plaintiff also would have to show that the defendant's failure to keep the sidewalks clear injured the plaintiff.

The plaintiff also must show that the defendant's breach caused the plaintiff's foreseeable injuries. Often courts use the "but for" test to meet this requirement. Would the plaintiff's injuries have occurred "but for" the defendant's actions? Once it's established that the defendant caused the plaintiff's injuries, courts review whether those injuries are compensable.

The law recognizes that there are some instances where the defendant is no longer responsible for the plaintiff's injuries. This happens when the plaintiff's injuries aren't foreseeable. The famous case that explored this concept is *Palsgraf v. Long Island Railroad* (1928).[37]

In the *Palsgraf* case, a passenger was running toward a moving train. Train employees tried to help the passenger board the train. As they helped him, they bumped a package from his arms. The package contained fireworks. The fireworks exploded on the train tracks. The explosion caused a scale on the train platform to topple over. When it fell, it injured Mrs. Palsgraf. She sued the railroad for her injuries.

> **NOTE**
> In New York, the Court of Appeals is the state's highest court.

The New York Court of Appeals decided the case. The court held that the plaintiff's injuries were not a foreseeable result of the actions of the railroad's employees. The court also held that the defendant had no duty to the plaintiff. The duty was owed to the passenger that the train employees were trying to help onto the train. Since there was no duty owed to the plaintiff, there could be no liability.

The *Palsgraf* case has come to stand for the rule that there's no duty to an unforeseen plaintiff for unforeseeable injuries. If there's no duty to an unforeseen plaintiff, then there's no negligence. This is known as proximate or legal cause. It means that a plaintiff's injuries must be the natural and foreseeable results of the defendant's negligence.

Once the plaintiff proves that the defendant committed a negligent act, the plaintiff must prove damages. In a tort case, damages can be economic or non-economic. Economic damages are damages that have a monetary value. They include compensation for medical bills, lost wages, and damage to property. Non-economic damages are harder to prove. They include compensation for items such as pain and suffering, or loss of companionship.

A court awards damages in a tort case in an attempt to make a plaintiff whole. These are called compensatory damages. Compensatory damages try to place the plaintiff in the same position that he or she would have been in had no tortious act occurred. This is the primary goal of tort lawsuits.

A court doesn't usually award punitive damages in a negligent tort case. It may award punitive damages if the defendant's actions are grossly negligent. This doesn't happen often. Many states have placed limits on the amount of punitive damages that a court or jury can award in a tort lawsuit.

There are some defenses to negligence torts. A defendant can use these defenses to help escape or limit liability. A defendant has the burden of proving her or his defenses. The three most common defenses are:

- **Assumption of Risk**—The plaintiff had assumed the risk of the defendant's actions and any injuries resulting from those actions. If the defendant proves assumption of risk, he or she has no liability to the plaintiff.
- **Contributory Negligence**—The plaintiff should recover nothing because his or her own actions also contributed to his or her own injuries. If the defendant proves contributory negligence, he or she has no liability to the plaintiff. Only a few jurisdictions follow this rule, because it's very harsh.
- **Comparative Negligence**—The plaintiff should recover only a *pro rata* share of damages because his or her own actions also contributed to his or her injuries. In most jurisdictions, a plaintiff less than 50 percent at fault can recover a *pro rata* share of damages based on the defendant's level of fault.

Intentional Torts

Intentional torts occur when the defendant intended to commit the tort. Intentional torts often share many common elements with a crime. It helps to remember that civil actions address torts and criminal actions address crimes.

In a lawsuit for a tort, the person who was harmed seeks compensation from the wrongdoer. In a criminal trial, society is punishing the wrongdoer for the crimes committed. The same action can be both a wrong against society (a crime) and a wrong against an individual (a tort). It's entirely possible in a criminal action that the victim of a crime won't be compensated for injuries. The victim can then bring a lawsuit against the wrongdoer for the underlying tort and recover damages.

The classic example of an intentional tort is battery. Battery is harmful or offensive contact with another person. The battery tort occurs when the defendant intentionally causes harmful contact with the plaintiff.

The most common defense to an intentional tort is that the plaintiff consented to the wrongful action. A defendant must prove that the plaintiff consented. A defendant can use the plaintiff's words or actions as evidence to prove consent.

Most of the torts associated with computers and cyberspace are intentional torts. These occur when the defendant uses a computer or takes some action involving a computer, intentionally to harm the plaintiff.