

Civil Procedure

A plaintiff must sue a defendant in a civil lawsuit in order to recover for tort injuries. Civil procedure is the body of rules that govern how courts conduct civil cases. This section provides more detail on the civil trial process. One thing to keep in mind is that the laws of civil procedure vary from jurisdiction to jurisdiction. The federal and state governments all have different civil procedure rules. The description provided here is intentionally general.

NOTE

In civil procedure, the plaintiff is the party that brings the lawsuit. The defendant is the party that defends against the lawsuit. In some jurisdictions, and for some types of cases, the plaintiff could be called the petitioner. The defendant could be called the respondent.

A civil action begins when the plaintiff files a **complaint**. A complaint is a document filed with a court. A plaintiff uses a complaint to tell his or her story. The plaintiff states how he or she was injured and asks the court to make him or her whole. A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief."³⁸ It also must show that the court has jurisdiction to hear the case. The plaintiff also must specify the relief demanded. In a tort case, the plaintiff typically wishes to receive money damages. The damages compensate the plaintiff for any injuries.

The plaintiff must file a complaint within a certain period of time after the claimed injury. This time period is called the **statute of limitations**. For example, in Indiana, the statute of limitations for most tort actions is two years.³⁹ The plaintiff must sue the defendant within two years of being injured by the defendant. Not all states have the same time limits. For example, in Montana the statute of limitations for most tort actions based on negligent conduct is three years.⁴⁰

Service of process refers to the procedure that delivers the complaint and a summons to the defendant. This process makes the defendant aware that the plaintiff has filed a lawsuit. There are certain formalities that must be followed in order to serve a complaint and summons on a defendant. For the most part, the complaint and summons are delivered physically to the defendant. This is to assure the court that the defendant received proper notice of the lawsuit.

NOTE

A defendant also can raise counterclaims in his or her answer. These are the defendant's claims against the plaintiff. The defendant also can raise cross-claims. These are the defendant's claims against another party to hold that third party responsible for the plaintiff's injuries.

The defendant must respond to the complaint after receiving it. That response is called an **answer**. All jurisdictions have time limits that a defendant must follow when answering the complaint. Under the Federal Rules of Civil Procedure, a defendant must file his or her answer within 20 days after receiving the complaint.⁴¹ A court can allow a defendant more time to answer if necessary.

A defendant must respond to each claim in the plaintiff's complaint. He or she can admit to or deny the claims. The defendant must also state her or his defenses to each claim. The answer is the defendant's opportunity to tell her or his side of the story.

A defendant also can raise defenses to the plaintiff's complaint. Some of these defenses are absolute. The court must dismiss the plaintiff's lawsuit if the defendant proves the defense. For example, the defendant can question the court's jurisdiction. If the court doesn't have jurisdiction over the matter, then it must dismiss the lawsuit. A defendant also can argue that the plaintiff doesn't have a legal basis for the claim. The court must dismiss the lawsuit if there's no legal basis for the plaintiff's claim.

After the complaint and answer, the plaintiff and defendant's attorneys will begin the discovery process. This is the period of the civil lawsuit where the parties share information with one another. Unlike the criminal discovery process, there are few affirmative disclosure rules in the civil discovery process. The parties must disclose their witnesses to one another. They also must provide each other with a list of documents that they have in their possession that are related to their claims and defenses. The documents that each party must disclose include a listing of documents stored in an electronic form.

After these general disclosures, it's up to each party to ask for information that's relevant to the case. The parties use various procedural rules to ask each other for information and documents. The process can get very complicated. It also can get very expensive. Sometimes the parties will ask the court to intervene in the discovery process. This happens when the parties dispute whether some types of information must be disclosed.

For example, a defendant may not want to disclose trade secret information through the discovery process, even if it's relevant to the case. This is because documents filed in a court case become public records. This includes documents exchanged during the discovery process and then used as evidence at trial. The defendant doesn't want to lose trade secret protection. The defendant could lose that protection if the information is available to the public or if it's shared with the other party's legal team. In this instance, the defendant could ask the court to issue a protective order. This type of order requires the parties to keep certain information secret. It helps protect the defendant's trade secrets.

After the discovery process ends, the parties either settle their lawsuits or proceed to trial. In late 2008, the U.S. Department of Justice issued a special study on civil trials in state courts. In the jurisdictions responding to the survey, only 3 percent of civil cases actually went to trial. The other 97 percent of cases are disposed of prior to trial. Either the parties settle the cases or the court dismisses them through other processes.⁴²

If a tort case goes to trial, the plaintiff must prove all the elements of his or her claim. He or she must prove the case through a preponderance of the evidence. This is a lower standard of proof than in criminal cases.

A civil trial ends with the court or jury's decision on the case. Some civil cases are tried in front of a judge alone. These are called *bench trials*. Bench trials are unusual in tort cases. The 2008 U.S. Department of Justice study on civil trials in state courts reported that juries decide 9 out of 10 tort cases.

Parties may appeal an adverse ruling at the trial court level. Either party may appeal a ruling to a higher court though a number of different procedural rules. These rules are outside of the scope of this chapter.

Electronic Discovery

For the parties in a lawsuit, electronic data can be important evidence. This is especially true since many parties and witnesses store their data in an electronic format only. The introduction of electronic-format evidence and record-keeping systems caused some problems for the legal system. These problems were acute in the discovery phase of lawsuits, where parties would engage in expensive fights over the production of electronic information.

Electronic discovery deals with information stored in an electronic format. It's also known as E-discovery. Prior to 2006, courts decided E-discovery issues on case-by-case basis under standard discovery rules. The most famous case for E-discovery issues is *Zubulake v. UBS Warburg, LLC*.⁴³ The U.S. District Court for the Southern District of New York decided this case.

There are actually several *Zubulake* decisions regarding electronic discovery. They stated the first real rules for parties to follow regarding electronic evidence. The rules related to the duty to preserve evidence, the duty to monitor compliance with preservation decisions, and costs of providing electronic data.

In 2006, the U.S. Supreme Court amended the Federal Rules of Civil Procedure to clarify how parties should handle E-discovery. These revisions were largely as a result of the *Zubulake* case. Additional amendments to the Federal Rules of Civil Procedure regarding E-discovery were proposed in August 2013. The Judicial Conference Committee on Rules of Practice and Procedure received 2,359 comments on the new rules.⁴⁴

Both the judge and plaintiff in the *Zubulake* case submitted comments on the proposed rules concerning E-discovery. If the new rules are approved, they will go into effect December 1, 2015.⁴⁵

When a lawsuit begins, parties are obligated to preserve certain types of evidence. This includes evidence stored in an electronic format. The Federal Rules of Civil Procedure call this type of evidence "electronically stored information" (ESI). The definition is broad and is meant to include any type of information that can be stored electronically.

Common Tort Law Actions in Cyberspace

Torts are wrongful acts between individuals. Lawyers and commentators have started to use the term *cybertorts* to describe torts arising from Internet communications such as e-mail.⁴⁶ Courts are applying traditional tort law principles to areas where communications and personal interactions occur electronically. This section will briefly describe some of the ways that tort law concepts have been applied to online interactions.

Defamation

Defamation is an intentional tort. Defamation occurs when one person speaks or publishes a false statement of fact about another person that injures that person's reputation. There are two types of defamation cases. They are:

- **Libel**—Written defamation
- **Slander**—Oral defamation

Parties to a lawsuit must address ESI early in the lawsuit. This is because it can be easily deleted or changed. The parties must address how discoverable ESI will be preserved. They also must address the format in which it will be shared with the other party. It can be shared in its native format, which may not be usable by the other party. It also can be shared in a reasonably useful form. If the parties don't specify how the ESI is to be shared, then a party providing ESI must notify the requesting party of the format.

In some instances, it can be hard to produce ESI for various reasons. A party doesn't have to produce ESI if it's not reasonably accessible due to undue burden or costs associated with retrieving the ESI. The party claiming that it can't produce ESI for these reasons bears the burden of proving that production is overly costly or complex.

Usually a court can sanction a party if it destroys evidence during the course of a lawsuit. This is called spoliation of evidence. It occurs when evidence in a lawsuit is inappropriately changed or destroyed. Spoliation sanctions can be severe. The Federal Rules of Civil Procedure recognize that sometimes ESI that is relevant to a case may be destroyed through the normal operations of information technology systems. The Rules provide a safe harbor to parties in these situations. The Rules state that a court may not impose sanctions on a party for failing to produce ESI that is destroyed because of the good-faith operation of information technology systems.

To fall into the safe harbor, the party must show that it took steps to preserve the ESI and acted in good faith. The duty to preserve ESI arises when a party is made aware of a legal claim or is put on notice that litigation is imminent or reasonably anticipated. Sometimes the attorney for a party might issue a preservation notice or litigation hold. These notices tell the party exactly what type of information must be preserved and for how long. Sometimes attorneys for opposing parties will send these types of notices to each other or to witnesses in order to make sure that ESI is preserved.

The American Bar Association has prepared a simple "E-Discovery Survival Guide." You can read the materials at http://www.americanbar.org/content/dam/aba/publishing/young_lawyer/yl_d_tyl_may10_ediscovery_authcheckdam.pdf.

The distinction between **libel** and **slander** has diminished in recent years, with "defamation" being used generally to refer to both types of cases. Defamation cases in cyberspace involving written communications are considered libel cases.

To prove defamation, a plaintiff must show all of the following:

- That the defendant made a false statement of fact
- That the defendant published the statement to third parties
- That the defendant knew or should have known that the statement was false

The defamatory statement must be more than mere opinion. For instance, in *Hammer v. Amazon.com* (2005), the plaintiff sued Amazon.com for defamation. The plaintiff was a self-published author. An online reviewer gave the plaintiff's book a negative review. Amazon published the review. The plaintiff wanted Amazon to remove the review. Amazon refused. The court ruled that the reviewer's statements were opinion and could not support a defamation claim.⁴⁷

NOTE

The term **flaming** refers to contentious online debates. They're heated exchanges between online posters. They often occur on online discussion boards. People might be able to use these types of statements to support a defamation case.

NOTE

Traditionally, loathsome diseases were diseases such as leprosy and venereal disease. They are diseases that have great social stigma.

The defamatory statement must be published to third parties. The publication requirement is easily satisfied when information is posted on the Internet. In fact, since many people have access to the Internet and materials posted on it, it may be easier for a plaintiff to show publication in an Internet defamation case. Information posted on the Internet may reach an audience more quickly. It also could lead to greater damage to the plaintiff.

Finally, the plaintiff must show that the defendant knew, or should have known, that the statement was false. A plaintiff shows this by presenting evidence that the defendant didn't check facts or the source of a statement.

Some types of statements are so scandalous that a court automatically presumes that defamation has occurred. These types of statements are called defamation *per se*. *Per se* is a Latin phrase that means "by itself." Types of statements considered defamation *per se* include:

- Statements that a person has a loathsome disease
- Statements that a person has committed a crime
- Statements about sexual misconduct or chastity
- Statements about professional impropriety

If a defamation case involves these types of statements, the plaintiffs don't have to prove all the defamation elements. They just must prove their damages.

Defamation is considered in context. A court must consider all the facts and circumstances around a case. In a traditional defamation case, the plaintiff can sue both the original maker of the defamatory statement and anyone who republishes the statement. These lines are blurred online. It makes it especially hard to determine where a defamatory statement first appears.

Internet defamation cases continue to rise. In 2013 a cheerleader for a professional football team won an Internet defamation case. That case is currently under appeal. In 2009, a woman sued her former high school classmates for allegedly defamatory statements made on a Facebook Web page. The plaintiff also sued Facebook for publishing the statements. The court dismissed Facebook from the case in September 2009.

The court stated that Facebook was immune from liability under a federal law that protects internet service providers (ISPs) from statements made by users of its services. As this was written, the case was still pending against the former classmates. Information about the case, including the plaintiff's complaint, can be viewed at <http://www.citmedialaw.org/threats/finkel-v-facebook#description>.

The defendant can raise some defenses to a defamation allegation. Truth is an absolute defense to a defamation allegation. A court can't hold a defendant responsible for defamatory statements if the statements were truthful. Another defense is that the defendant acted in good faith. Statements that a defendant makes in connection with judicial or legislative proceedings have immunity from a defamation action. These types of statements are called *privileged* statements.

Internet Service Provider Liability for Torts

Congress enacted the Communications Decency Act in 1996. The U.S. Supreme Court declared many portions of this Act unconstitutional. This is because they infringed on free speech rights. One part of the Act that's still in effect is Section 230.⁴⁸

Section 230 protects interactive computer service providers from liability for the actions of content providers. The act recognizes that "[t]he rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens."⁴⁹ It also recognized that Americans rely on interactive media for educational and entertainment information. In enacting the policy, Congress sought "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services."⁵⁰

Under the law, an interactive computer service is any electronic information service or system. It specifically includes a service or system that provides access to the Internet. Courts interpret this definition as broadly as possible. The act states that an interactive computer service provider may not be treated as the "publisher" or "speaker" of content posted by service users. This is a safe harbor for interactive computer service providers. It protects them from legal liability for the actions of service users.

Courts have applied this provision quite broadly to many companies who offer services over the Internet such as social networking or bulletin board posting services. For instance, courts have found that America Online, Facebook, and Craigslist are interactive service providers who fall under the section's protection.

ISPs rely on this law to insulate themselves from the actions of their customers. Section 230 specifically preempts state or local laws that would hold ISPs responsible for the acts of content providers.

One problem for online defamation cases is that it's sometimes difficult for a plaintiff to discover the identity of an online poster. This is particularly true if an anonymous poster makes defamatory statements in an online forum. Plaintiffs often have to go to court to get an ISP to turn over identifying information about an anonymous online poster.

A final item to remember is that online tort cases often involve jurisdictional issues as well. State courts can hold out-of-state defendants responsible for their actions only in limited circumstances. Most states have complicated tests for when they can exercise jurisdiction over an out-of-state defendant. These are called "long arm jurisdiction" tests. Lawyers and courts use this term because it describes situations where the "long arm of the law" can pull a defendant into a certain jurisdiction. This is the same type of problem that was discussed in the criminal law section of this chapter. These types of jurisdiction issues sometimes mean that a plaintiff must litigate a case in a state other than the state where she or he lives.

Intentional Infliction of Emotional Distress

Intentional infliction of emotional distress (IIED) is known as the *tort of outrage*. This is because it's used to address conduct that is so offensive that a reasonable person would say "Outrageous!" To prove this tort, a plaintiff must show:

NOTE

Many states also recognize the tort of negligent infliction of emotional distress. This tort can be harder to prove because one of the elements is that the defendant owed the plaintiff a duty to act in a certain way. There's no duty requirement in IIED cases.

- That the defendant acted intentionally or recklessly
- That the defendant's conduct was extreme and outrageous
- That the defendant's conduct caused the plaintiff severe emotional distress

The *Restatement (Second) of the Law of Torts* notes that extreme and outrageous conduct is "beyond all possible bounds of decency and to be regarded as atrocious, and utterly intolerable in a civilized community."⁵¹ Courts have recognized that people have the right to be free from this type of behavior. Even though courts recognize this cause of action, they have held that the defendant's conduct truly must be extreme and outrageous given the circumstances. Mere bad or boorish behavior isn't enough under this tort.

The landmark case recognizing this tort happened in California. In this case, the defendant won a contract for trash collection. A State Rubbish Collectors Association member previously held that contract. The defendant was not a member of the association. The association intimidated the defendant into signing a membership agreement. The members threatened to hurt him and destroy his garbage truck. The plaintiffs then sued the defendant to collect on the membership agreement. The defendant argued that he was not liable under the agreement because the association had threatened him and he signed the agreement under duress. He also argued that the plaintiff's actions caused him to become severely ill and miss work.

In ruling on the case, the court said that a person has the right to live his life without "serious, intentional, and unprivileged invasions of emotional and mental tranquility."⁵² The court found that the defendant could recover on his IIED claim.

IIED cases can arise through e-mail, comments made on social networking sites, and instant messaging. Since IIED cases involve interactions between a plaintiff and defendant, evidence proving the contents of the electronic communications can be very important. Like defamation cases, in most instances ISPs aren't liable for the actions of content providers that cause an IIED.

Often IIED cases involve situations where a person is using a work e-mail account or Internet access to commit the tortious activity. There are times when employers might be liable for the bad acts of employees. Employers can be liable for their employees' actions when those actions take place within the scope of the employee's job. An employer also must have knowledge of the employee's tortious acts. Courts have been reluctant to hold employers responsible for the cybertorts of employees unless the employer had knowledge of its employee's actions and didn't take steps to stop them.

IIED claims also can involve claims of harassment. Some states recognize harassment as a tort, while most consider it criminal behavior. Some states also have included cyberstalking or online harassment in their criminal harassment laws. For example, Oklahoma and New York have anti-stalking laws that include online harassment as a prohibited activity.⁵³

Harassment is similar to IIED in that the harasser intends to cause the plaintiff emotional distress. Harassment can include continuing to communicate with a person when she or he has asked that the harasser no longer talk to them. It also can include threats made against a person or that person's loved ones. Harassment also can include offensive sexual remarks and remarks based on characteristics such as race, national origin, religion, and gender.

Like IIED, harassment can very easily take place in the online environment. It can occur via e-mail, postings on social networking Web pages, and postings on other Web pages.

Trespass Torts

Common law recognizes trespass torts. In common law, there are two types of trespass cases: trespass on land and trespass to chattels. *Chattels* means personal property. A trespass to chattels is intentionally interfering with a person's use or possession of personal property. The defendant's use of the plaintiff's personal property must cause an injury or damage. Often this happens when the defendant harms the personal property in some way.

Courts have extended trespass to chattels cases to online situations, such as spam e-mail. The first court case holding spammers responsible for trespass to chattels was in 1997. In that case, an ISP sued a defendant for bypassing the ISP's spam-blocking controls to send spam e-mails to the ISP's customers. The defendant had changed the header information on its spam e-mails so that they could get past the filters. The ISP argued that the spam e-mails imposed a burden on its system. It also argued that the defendant's spam messages were an intrusion to the ISP's system since they bypassed filtering controls. The U.S. District Court for the Southern District of Ohio found that the defendant's spamming activities did indeed constitute a trespass of that system.⁵⁴

In a trespass to chattels case, the plaintiff must be able to prove that he or she was injured or harmed. This is the most difficult element to show in online cases. In 2003, the Intel Corporation sued an ex-employee for sending spam e-mails to over 30,000 Intel employees on multiple occasions. The California Supreme Court rejected Intel's trespass claim because it was unable to prove any damages. Intel was not able to show that the thousands of e-mails slowed its servers or caused some sort of adverse effect on its computer systems.⁵⁵

Privacy Violations

The four privacy torts are:

- Intrusion into seclusion
- Portrayal in a false light
- Appropriation of likeness or identity
- Public disclosure of private facts

Courts are beginning to recognize that people have a right of privacy in their electronic equipment and electronic communications. The intrusion into seclusion privacy tort is used most often in this context. For example, a plaintiff may be able to sue a defendant for accessing the plaintiff's private electronic blog without permission. However, the rise of the Internet as a communications and entertainment medium may mean that other privacy torts, such as portrayal in a false light, may grow as well.

A question that is yet to be resolved is whether people have a true right of privacy in their use of the Internet, independent of any tortious or criminal activity. A person's privacy on the Internet is somewhat limited by the logging mechanisms that ISPs and Web pages employ to make sure that systems are operating correctly. Programs used by service providers to track activity for advertising purposes also are threats to privacy.

Tort cases are firmly rooted in state laws. There may be other tort actions that a plaintiff can use to seek redress for harmful activities in cyberspace. If a plaintiff is harmed by actions in cyberspace, and has damages and injuries that he or she can prove, the plaintiff will need to review state laws and court cases for appropriate causes of action.

Case Studies and Examples

The following case studies and examples show how the concepts discussed in this chapter are used. These case studies are real-world examples of criminal and tort law issues in cyberspace.

CAN-SPAM Act

The U.S. government first brought criminal charges under the CAN-SPAM Act in April 2004. The U.S. Postal Inspection Service, U.S. Attorneys' office, and Federal Trade Commission were involved in investigating the case.

In this case, the federal government charged the defendants with sending spam messages to sell phony diet products. The defendants operated under the name Phoenix Avatar, LLC. The defendants hid their identities in spam messages by using corporate and government computer systems and spoofing third party e-mail addresses. They used computers belonging to Ford Motor Company, computers used by the U.S. court system, and the Unisys Corporation to hide their identities. Spam that was undeliverable bounced back to the innocent third party e-mail addresses. Phoenix Avatar sent millions of spam messages this way.

One of the defendants in the case, Daniel Lin, pleaded guilty to violations of the CAN-SPAM Act in January 2006. In June 2006, the court sentenced him to three years in federal prison.

The Federal Trade Commission filed a civil enforcement action against Phoenix Avatar. The FTC brought the action for violations of both the FTC Act and the CAN-SPAM Act. The FTC Act violations were related to the defendant's sale of the phony diet products.

In March 2005, the FTC settled civil charges against Phoenix Avatar. As part of the settlement, the defendants agreed to pay a \$20,000 penalty. They also agreed not to violate the CAN-SPAM Act.

NOTE

You can read the FTC enforcement action documents at <http://www.ftc.gov/os/caselist/0423084/0423084.shtm>.

Defamation

The Internet has a number of anonymous gossip Web sites. Juicy Campus was one of the first popular sites. It started in 2007 and closed down in February 2009. It allowed students to post anonymous gossip about events and people at their campuses. Juicy Campus had separate Web pages for different colleges.

Juicy Campus billed itself as a way to promote free speech on college campuses. Among its features, anonymous users could post gossip about other students, read gossip posted by other users, and vote on the "juiciest" pieces of gossip. Students ridiculed or insulted on Juicy Campus had little recourse, as the postings were anonymous. As an ISP, Juicy Campus didn't share the identities of its online posters without a court order.

Since Juicy Campus closed down, other online campus gossip Web sites have grown in popularity. One of the sites that opened when Juicy Campus shut down is CollegeACB. In its own press release, the owner of the Web site wrote: "The College ACB or College Anonymous Confession Board seeks to give students a place to vent, rant, and talk to college peers in an environment free from social constraints and about subjects that might otherwise be taboo." College ACB closed down in 2011.⁵⁶

AutoAdmit is a similar site. It's an online law school discussion board. As on similar gossip Web sites, posts in that forum sometimes can be insulting and offensive. In 2007, two Yale Law School students sued anonymous AutoAdmit posters for defamation. The parties settled the case in 2009. The terms of the settlement were confidential. You can learn more about that case on the Citizen Media Law project Web page at <http://www.citmedialaw.org/threats/autoadmit#description>.

Think about these types of Web sites. How do they promote free speech? Are there occasions on these Web sites where one person's right to free speech infringes upon another person's right to live peacefully?