INFORMATION BRIEF
Research Department
Minnesota House of Representatives
600 State Office Building
St. Paul, MN 55155

Mary Mullen, Legislative Analyst
651-296-9253

May 2018

The Internet and Public Policy: Cybertorts and Online Property Rights

This is one of a series on public policy and the Internet, with special attention to the laws and public policies of the state of Minnesota.

This brief examines at how certain civil wrongs—or tortious conduct—occur online and the laws that have been used to address the conduct. The brief also discusses how intellectual property law and the probate law have adapted to address online property rights.

Contents

About The Internet and Public Policy Series

The Internet is a worldwide communication web created through technology, hardware and software, and human use patterns, which are shaped by mores, customs, and occasionally laws. States have their own roles within the larger national and international network that is the Internet. The challenge for policymakers is that the Internet itself is malleable, and no static definition can capture its breadth and changing uses.

This series of information briefs isolates discrete policy issues and the ways in which specific Internet issues provide choices for the Minnesota marketplace and for lawmakers. See the list at the end of this document for other titles in this series.

Introduction

Both social and commercial activity on the Internet may give rise to lawsuits aimed at repairing harm to a company or a person's reputation, economic interests, or privacy—all of these falling under the broader legal concept of torts.[1] Unlike torts that occur in the material world, cybertorts generally focus on the "financial losses, reputation injury, or emotional injury rather than personal injury or physical damage to property."[2] Information-based torts have damages that are much harder to quantify than traditional torts involving physical injuries, malpractice, or economic damages. They also tend to require the court to act to stop a company or individual from continuing an action that is causing a harm, or going to cause a harm in the future, which is called injunctive relief.

The Internet has a number of features that change how torts occur online. Because information can be accessed in new ways through online interfaces and cloud storage fraud, identity theft and hacking allow for information to be stolen or accessed without authorization. The Internet also offers people the ability to complete banking, financial transactions, and commercial activities without ever coming face to face with another person, facilitating an increase in theft, impersonation, and identity theft. Finally, the ability to self-publish online to a wide audience without moderation has caused new opportunities for harm to individuals and businesses.

These new facets of online torts have made them more difficult to pursue in the courts. Along with the unusual way torts can occur online, many interactions between consumers, users, and online companies are controlled by user agreements. Those contracts often attempt to limit the remedies available, require arbitration, and control which jurisdiction's laws will apply and the venues where lawsuits can be filed. Despite these challenges, both common law and statutory torts have been used to address tortious online activity.

This brief looks at how tortious conduct occurs online, what laws have been used to address it, and how intellectual property law and the probate law have adapted to address online property rights.

Common Law Torts Applied to Online Tortious Activity

Existing tort law has been applied to these new Internet-related torts, in some cases with success, but in some cases the existing common law did not imagine the Internet-based activities. Existing tort law that has been used to address some of these new harms include: defamation; invasion of privacy; misappropriation of trade secrets; right of publicity;[3] interference with a contract (breach of contract); intentional misrepresentation (fraud); negligent or intentional infliction of emotional distress; tort of appropriation; and breach of fiduciary duty. In Minnesota, there is a statute that allows a person to sue and recover damages for crimes that result in theft of personal property, such as identity theft where there is a financial loss.[4] In some cases, new statutory causes of action have been created where common law has failed to address new activities on the Internet that have harmed individuals and businesses.

Intentional Infliction of Emotional Distress

The ease of publishing content online has also increased instances of harassment, stalking, bullying, blackmail, and defamation. One common law approach to deal with these online civil harms is the intentional infliction of emotional distress. Cases of cyberbullying have risen to national attention recently, but attempts to find redress are often met with complicated legal battles and little resolution for the victims.[5] Suing for intentional infliction of emotional distress is one option, although the damages can be difficult to prove. Minnesota courts follow the four elements laid out in the Second Restatement of Torts for intentional infliction of emotional distress: "(1) the conduct must be extreme and outrageous; (2) the conduct must be intentional or reckless; (3) it must cause emotional distress; and (4) the distress must be severe."[6]

Defamation

Defamation is a common law tort used to address published materials that negatively impact a person on the Internet, especially via social media, online bulletin boards, and blog websites.[7] Defamation, invasion of privacy, and intentional infliction of emotional distress torts are all challenging actions for a plaintiff to bring, because the speech that is published (communicated to another) is often protected by the First Amendment right of free speech. There are some exceptions related to students and employees, but the court has often upheld the value of protected speech.[8]

Blogging is one area where defamation and other tortious action can come head-to-head with First Amendment rights. The Minnesota Court of Appeals found that a blogger's right to publish information about a public figure about an issue of public concern was protected First Amendment speech when the blogger believed the information to be true and therefore not defamatory.[9] Online speech has been found to have the same protections as other forms of written media.[10] YouTube, social media, and video-hosting websites no longer have the oversight of network or cable television as the content is uploaded by the users. When people are imitated or their image or likeness is used online, liability often comes down to whether the action was intended to be a freedom of expression, such as a parody or art, which is more likely to be protected by the First Amendment, or if the action was commercial speech or intended to make money.

Anti-SLAPP Laws

"Strategic lawsuits against public participation," or SLAPP lawsuits, often come as defamation cases against a person who is speaking out publically against an action he or she perceives as harmful, often related to an issue of public concern. Companies or private interests that see the speech as defamatory or problematic, file a lawsuit to "bury" the person in litigation costs and discourage his or her efforts to speak out. Anti-SLAPP legislation is the state's attempt to curb these lawsuits. The term "cyberSLAPP" has become more common as SLAPP lawsuits have been aimed at unfavorable online reviews, publications, and political commentary. Individuals are sued for defamation for posting unfavorable information about commercial activities, such as posting a public review of a doctor or criticizing the business practices of a company. More than half the states have an anti-SLAPP statute, including Minnesota, but the Minnesota law was found to be unconstitutional by the Minnesota Supreme Court in 2017.[11]

Right to Privacy

The right to privacy is an action that is recognized in 30 states, and the District of Columbia, as a common law tort. Four distinct torts have emerged under the right to privacy:[12]

- intrusion into a plaintiff's private affairs
- disclosure of private (embarrassing) facts about the plaintiff
- false light, intended to protect a plaintiff from true information that is misrepresented and casts the plaintiff in a false light
- misappropriation or right of likeness claim, where the plaintiff's likeness has been used for commercial gain without his or her permission

These torts rose in applicability during the 20th century as publication became more common, and also rose when publication became a daily activity for most people who are on the Internet. In some instances, there are statutes that protect privacy, such as a person's financial information, which is protected in statute by the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act.[13] Four states have incorporated the right to privacy into their state constitutions: Florida,[14] Alaska,[15] Montana,[16] and California;[17] this provides some additional support for privacy-based harms in those states.

While cases, and especially damages, can be difficult to prove, in some instances the tort of invasion of privacy is the only legal remedy when someone has disclosed the personal information of another online. In *Boring v. Google*, the Third Circuit Court of Appeals upheld the dismissal of the right of privacy claims brought by the plaintiffs who had sued Google for coming onto their private road and taking a picture of their property for Google's street view program. The case explains that the *publication* of the images has no bearing on the decision in an "intrusion into seclusion" privacy action, highlighting the difficulty in applying common law privacy torts to some of the new technological advancements resulting from the Internet.[18]

The tort of appropriation, which prevents a person's likeness from being used to advertise products, applies when the person appropriating the likeness is benefitting commercially. Privacy

advocates argue that it should be expanded so that individuals can use this claim to prevent the dissemination of their personal information and likeness without consent.[19]

Trespass and Conversion

Trespass seems like an odd tort to consider in the context of Internet law or online activities, however, trespass has been used to recover damages in civil actions where a computer or computer system has been damaged by a "trespass" such as a virus, spam, bots, or spyware.[20] Similar to the concept of trespass to personal property, conversion or taking personal property, could occur through online crimes when personal property, such as a computer, is interfered with to the point that it is equivalent to taking the property.[21]

Negligence

There have been very few, if any, successful negligence claims brought related to tortious activity online. However, recent data breaches have prompted large class actions against Yahoo and Experian, alleging negligence for failing to protect consumer information.[22] Some policy experts have warned that creating a liability for negligence in data breaches could be harmful because companies will be less likely to disclose data breaches to the public.[23]

Immunity Under the Communications and Decency Act

Section 230 of the Communications and Decency Act (CDA) adds to the difficulty of applying common law torts to online activity. This federal law prevents liability from extending to any provider or user of an interactive computer service for information provided by another.[24] Section 230 of the CDA has been used to limit liability to ISPs and websites that host forums where individuals can use their venue to post content that may be tortious. The immunity does not extend to federal criminal liability but generally is found to shield the ISPs, internet hosting companies, search engines, and online message boards from liability when the information or content that is harmful is provided by another, and the interactive computer service is not involved in the creation of the content and does not edit the content.[25]

This immunity provision has been a source of controversy as cases proceed with little or no redress for harmed plaintiffs, who cannot find the individual who posted the harmful content or the person who posted the harmful content does not have any money to pay the damages. Law professor Daniel J. Solove argues that Section 230 of the CDA has gone too far and that the protections for ISPs allow irresponsible Internet use; he writes that this furthers tortious behavior by facilitating defamation and the invasion of privacy.[26] Solove argues for a notice-and-take-down system similar to what is in the current Digital Millennium Copyright Act, which could be used to assist people in removing potentially tortious information from the Internet.[27]

Statutory Civil Remedies

Civil remedies are provided in a number of federal statutes, both statutes of general application and statutes specifically written to address Internet-based torts and crimes. States have also followed suit, creating new causes of action and statutory remedies to address torts and online property rights. The federal laws discussed below are a few examples of situations where Congress felt the need to create a civil liability for individual harms that were difficult to address using state tort law.

There are also state laws emerging to address some consumer and commercial harms online, such as patent trolling[28] and revenge porn. In a number of cases, immunity from liability shields ISPs and websites from liability. In other situations, companies handling consumers' private personal information or financial information are not required to maintain the data with any imposed duty of care, which has prevented negligence from being applied to many cybertorts and data leaks. These areas may be remedied by the courts or they may be addressed by federal or state legislation looking to create more remedies for users and consumers online.

The Digital Millennium Copyright Act

The Digital Millennium Copyright Act updated the U.S. copyright law to incorporate international agreements on the use of copyrighted material online.[29] The act creates civil liability for the infringement of a copyright, including a damage award of the amount of damages suffered by the copyright owner, or the benefit to the infringing party, or for statutory damages in an amount set by the court.[30] One of the major changes under that legislation was the creation of the Online Copyright Infringement Liability Act.

The Online Copyright Infringement Liability Act

The Online Copyright Infringement Liability Act (OCILA) was passed to address the technological advances that allowed art, music, writing, and video to be shared and duplicated online. The OCILA created a more timely system for artists or the owner of a copyright to take down work that was not authorized by the copyright owner. It also created immunity from liability for the infringement of copyright laws for ISPs and other online intermediaries when the website or ISP does not know that the copyright is being infringed, does not profit from the infringed work, and removes the work "expeditiously."[31] This law also created liability limits for search engines that offer links to infringed materials and incidental storage of infringed materials by search engines, websites, and ISPs.

The OCILA also created a "take-down notice" process where the ISP or website informs the user that the work is being taken down and provides an opportunity to object. This system is much less expensive than filing a lawsuit to enforce the copyright. The process does not shield the user from liability if the user continues to post the work after the take-down notice is received. The user will not have violated the copyright if the user has a license for the copyrighted material, the copyright has expired and the work is in the public domain, or if the user is posting the work under a "fair use" exception to the copyright act.[32] However, determining when an artistic work

is being infringed can be tricky; for example, a number of cases have emerged from the video-hosting website YouTube.[33]

Trademarks

Similar to the updated copyright laws, the federal trademark law was updated to account for a variety of new online activities. The act creates a civil liability when there is an infringement on a registered mark, including the copying or imitation of registered marks, such as domain names, website names, "app" names, and icons.[34] Related federal laws emerged to create civil liability for similar activities that confused consumers with similar or nearly identical marketing to existing companies and trademarks.[35]

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act created a private cause of action for losses that are incurred by violations of the act. This provision of the law includes damages for the loss of use of the computer or computer system, physical injury, and damage to the computer.[36] A plaintiff can bring an action requesting actual damages, damages for the amount the defendant profited, and punitive damages when the violation was willful or intentional.[37] The law also provides that in no case shall a person recover less than $1,000; that has been interpreted to mean there is a statutory minimum of $1,000 per violation.

State Laws: Civil Liability and Online Property Rights

State laws creating new civil causes of action, regulating consumer interactions with websites and ISPs, and establishing online property rights, have become more prevalent. Congressional action on bills designed to address a variety of online conduct has been slow, and without any action at the federal level, states have begun to pass legislation in these areas, particularly where there is widespread support and grassroots campaigns.

Revenge Porn

A phenomenon known as revenge porn, or nonconsensual pornography, emerged with the widespread use of the Internet for pornography. The term "revenge porn" is often used as a catchall to describe the distribution of a photo or video taken either with the subject's permission or without (by a hidden camera, for example) and then distributed without the subject's consent, often to a wide audience, via an Internet site. The public at large, criminal prosecutors, women's rights advocates, and politicians generally agree on the social harms brought about by the nonconsensual distribution of images and videos, but there are few answers to the problem in existing law. In interviews, victims of nonconsensual pornography report fearing imminent harm and harassment from their sexual images and personal identifying information (name, address, telephone number, Facebook account details) available online. Legal scholars argue that revenge porn is an extension of domestic violence and sexual harassment.[38]

Many young women have lost their court battles by using common law and statutory torts, like invasion of privacy, defamation, slander, intentional infliction of emotional distress, stalking, harassment, right of publicity,[39] interference with a contract, intentional misrepresentation (fraud), and identity theft. In addition, local prosecutors—who were often sympathetic to victims' stories—cited a lack of a crime committed under existing statutes. These dynamics resulted in a widespread call for legislative action.

Between 2014 and 2017, 38 states and the District of Columbia passed revenge porn legislation that makes it a crime to disseminate nonconsensual pornography. Approximately ten of those states also passed laws that provide a civil action to individuals who are harmed.[40]

In Minnesota, the legislature enacted a law in 2016 to address revenge porn. The act allows a person to sue for damages when another person has shared private images; the act also creates certain exceptions for when sharing a private sexual image is allowed. Under Minnesota Statutes, sections 604.30 to 604.31, it is unlawful to:

- disseminate, post, or publish a photo or video if the subject of the photo or video did not consent to the post or publication, and the photo or video shows the person nude, partially nude, or engaged in a sexual act; and
- solicit sexual invitations for another person when that person has not consented to the solicitation.

The law also:

- provides for damages, including special and general damages, damages in the amount of profits the defendant may have earned, and a civil penalty up to $10,000;
- allows for confidential filings when approved by the court; and
- provides express exemptions for parents or legal guardians distributing pictures of their children, law enforcement officers, or prosecutors attempting to prosecute a crime, newsworthy events or photos and videos of public importance, and immunity to ISPs consistent with Section 230 of the CDA.[41]

Search engines and websites have recognized the issue, as well. Facebook has changed its take-down policies to accommodate revenge porn, while search engines like Google have offered to remove the offending websites from search results.[42] Even if state laws prohibiting revenge porn are overturned, the crime's costs may be mitigated by the commercial response of the tech industry.

Digital Assets

The information age has changed the nature of valued assets from tangible goods to digital content, information, and even money. What was once left behind—papers, letters, photographs, movies, music, books, even artistic creations—are no longer always in a physical format. The nature of the ownership over that information has changed as well. For example, the Internet allows people to "lease" a space to hold music and lease the music itself. Some music downloads allow a person to own the file—and pass it on when that person dies—others do not. Website

policies about who owns the content on a site and whether or not the contractual agreement in the terms of service continue after a user dies, were not anticipated when estate planning laws were enacted hundreds of years ago; those laws have rarely been updated to account for changing technology. For example, can people leave Bitcoins to their children? Can a video game player pass on a video game persona to a friend? What should happen with digital films, cloud photo accounts, and personal records?

Digital assets include Facebook accounts, e-mail accounts, photos, personal records and data, career information, entertainment including films and music, gaming persona and assets, and the harder-to-define online persona. The property may be virtual, held by a company based in California or on a server located in Singapore, but the asset may need to be distributed through a probate in Oklahoma. The distribution of these assets, or perhaps more appropriately, the access of these assets by the heirs to an estate, or a fiduciary like a trustee or guardian, is a legal grey area. Practically speaking, most people do not make a will or plan for the distribution of their assets at death, so the most basic aspect of estate planning for digital assets—leaving behind a list of online accounts and passwords—rarely occurs in the first place, let alone the legal authorization to access the accounts or to make sure no one can access them, if that is what the user intends.

The Revised Uniform Fiduciary Access to Digital Access Act (UFADAA) was enacted to address the hole in common law and state legislation; it gives users a path to deal with "digital assets" at the time of a person's death. Wills, trusts, health care directives, and other fiduciary instruments did not contemplate that a person's computer, music, photographs, e-mails, and other assets may exist in the virtual world—creating "digital assets" just like tangible assets but that were difficult to access (due to their location and password protection) and unaccounted for in a typical estate distribution.

The original model statute was proposed by the Uniform Laws Commission, the American group that drafts model uniform legislation, and was released as a draft in 2014. Delaware quickly passed this version in 2014, but other states waited until an official model law was circulated in 2015. By then, the tech companies had mounted a lobbying effort to point out issues with the legislation, and the 2015 UFADAA did not pass in any states. The bill ignored a number of issues when it was drafted. The tech companies that opposed the UFADAA proposed their own model statute, the Privacy Expectations Afterlife and Choice Act (PEAC Act), which passed in Virginia in 2015. Since the Revised UFADAA passed in ten states in 2016 and was introduced in another 14 states, it is likely Virginia and Delaware will pass the Revised UFADAA to replace their current laws.

In Minnesota, the Revised UFADAA is codified as Minnesota Statutes, chapter 521A:

- allows a fiduciary (a personal representative, trustee, power of attorney, or guardian) to access a person's e-mail and websites where a person may have digital assets with a form of written consent through the fiduciary document or through a previous user agreement or terms of service agreement with the website;
- provides a legal process to get to digital assets where a website or tech company may not want to disclose because it is trying to protect the privacy of the user;

- provides for some direction as to how to disclose assets when the document creating the fiduciary relationship is silent on the issue;
- provides limited liability for companies attempting to comply with good-faith requests; and
- directs how the disclosure of information or use of a computer interacts with federal criminal laws that prohibit computer access and e-mail access by an unauthorized user.

The original UFADAA did not take into consideration the contract that users agree to when downloading software, buying hardware, and using websites and programs. In fact, it made those terms of service contracts and user agreements void. Websites argued for the validity of these contracts—terms of service agreements, user agreements, and website settings chosen by the user.

The Revised UFADAA took these contracts into consideration and allowed the terms of service agreement to control when the terms of service agreement is able to be modified. In these situations, the terms of service agreement controls over general directions in a will or other fiduciary arrangement. This allows the user to change the instructions online if needed, otherwise the will or other fiduciary instrument will govern. Finally, if the user has provided no directive in a will or other fiduciary arrangement, the terms of service agreement will govern. This approach is consistent with the prevailing law in this area, which is that while terms of service contracts and user agreements are boilerplate, often ignored by consumers, and sometimes difficult to locate, they have generally been upheld by the courts unless they are so one-sided as to be unconscionable or impossible to locate on a website.

One of the major issues the tech companies raised was that fiduciaries would have access to a user's e-mail accounts—and all archived e-mails—and that this was the default position. They were imagining how a fiduciary operates in the brick-and-mortar world, where a person's power of attorney or personal representative can open a person's mail and look at it. But e-mail is different because of the automated nature of archiving. Now a person's personal representative can see every piece of mail ever received over the course of a person's life. On top of that, federal law governing e-mail communication privacy likely prevents a default rule granting access to a fiduciary without explicit consent. This provision was one of the major changes to the revised act.

The changes to UFADAA largely reflect tech companies' concerns over a law that viewed digital assets the same as physical assets and which failed to recognize the legal framework that already existed between the user and the website. The Revised UFADAA has now been passed in ten states, and a handful of other states have passed other digital access laws that govern in this area. The Revised UFADAA keeps estate planning and probate at the state level. It also facilitated a nationwide conversation on digital assets between state legislatures, the courts, and big tech companies. The shift in viewing digital assets as an important part of a person's estate has occurred, as has a better understanding of the nature of the relationship between a consumer or user and the websites they interact with.

Other Works in the Series

This series of information briefs isolates discreet policy issues and the ways in which specific Internet issues provide choices for the Minnesota marketplace and for lawmakers. The following publications are part of the Internet and Public Policy series:

- Challenges and policy consideration for state regulation
- Privacy and consumer protection
- Criminal activity on the Internet
- Federal Internet laws
- Jurisdiction and procedures in Internet law cases
- State and federal accessibility laws

There may be more topics added, as needed. A special attempt will be made to keep all of these pieces up to date, but the pace of change may prove challenging.

ENDNOTES

[1] Michael L. Rustad, *Global Internet Law* (St. Paul: West Academic Publishing, 2014), 378.

[2] Rustad, *Global Internet*, 112.

[3] Unlike the identity theft, the right of publicity is a tort that involves someone using the commercial value of another's likeness without permission (Rustad, 420).

[4] Minn. Stat. § 604.14.

[5] *U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), a criminal action was brought under the Computer Fraud and Abuse Act against a woman who harassed a 13-year-old online who then committed suicide; *State v. Ravi*, 447 N.J.Super. 261 (N.J. 2016), charges were brought under state hate crime law against Ravi for cyberbullying another man related to his sexual orientation.

[6] *Hubbard v. United Press Intern, Inc.*, 330 N.W.2d 428, 438-439 (Minn. 1983).

[7] Along with defamation, the common law tort of libel is untrue written communication to a third party that is unfavorable, and slander is the same action when the communication is oral.

[8] *Tatro v. University of Minnesota* 816 N.W.2d 509 (Minn. 2012); *Sagehorn v. Indep. Sch. Dist. No. 728*, 122 F. Supp. 3d 842, 850 (D. Minn. 2015); *Murdock v. L.A. Fitness*, (D. Minn. 2012).

[9] *Moore v. Hoff*, 821 N.W.2d 591 (Minn. Ct. App. 2012), reversing Hoff's award for tortious interference with employment because the statements published about the plaintiff were believed to be true, about a public official, and relating to a matter of public concern. The court found that the tortious actions were too entangled in the defendant's right to free speech and if liability was found, the defendant's First Amendment rights would be infringed.

[10] See *Reno v. ACLU*, 521 U.S. 844 (1997), the U.S. Supreme Court held that speech on the Internet was afforded the full protection of the First Amendment and not the diminished protections provided to radio and television.

[11] *Leiendecker, et al. v. Asian Women United of Minnesota*, 895 N.W.2d 623 (Minn. 2017).

[12] William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383 (1960).

[13] 15 U.S.C. §§ 1681; 6801, 6805.

[14] Florida Const. art., § 23.

[15] Alaska Const. art. I, § 22.

[16] Montana Const. art. 2, §10.

[17] California Const. art. 1, §1.

[18] *Boring v. Google, Inc.*, No. 09-2350, 2010 U.S. App. LEXIS 1891 (3rd Cir. 2010).

[19] Daniel J. Solove, "Speech, Privacy, and Reputation on the Internet" at 23. Saul Levmore and Martha C. Nussbaum, editors. *The Offensive Internet: Privacy, Speech, and Reputation* (Cambridge: Harvard University Press, 2010).

[20] Rustad, *Global Internet*, 289.

[21] Rustad, *Global Internet*, 396.

[22] Molly Mosendz, "Equifax Faces Multibillion-Dollar Lawsuit Over Hack," *Bloomberg*, September 8, 2017; Ethan Baron, "Yahoo data-breach class-action lawsuits joined together in San Jose federal court," *Siliconbeat*, December 8, 2016, http://www.siliconbeat.com/2016/12/08/yahoo-data-breach-class-action-suits-joined-together-in-san-jose-federal-court/.

[23] Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255 (2005).

[24] 47 U.S.C. § 230 (c)(1).

[25] *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

[26] Solove, "Speech, Privacy," 24.

[27] Solove, "Speech, Privacy," 25.

[28] National Conference of State Legislatures, "Patent Troll Legislation," July 12, 2016, http://www.ncsl.org/research/financial-services-and-commerce/2016-patent-troll-legislation.aspx.

[29] 17 U.S.C. §§ 101, 104, 104A, 108, 112, 114, 117, 512, 701, 1201-1205, 1301-1332; and 28 U.S.C. § 4001.

[30] 17 U.S.C. § 504.

[31] 17 U.S.C. § 512.

[32] 17 U.S.C. §§ 101-801; fair use has been found to includes criticism, comment, new reporting, teaching, scholarship, research, and parody.

[33] *Lenz v. Universal Music Corp*., 801 F.3d 1126 (9th Cir. Ct. App. 2015), holding that the copyright owner must consider if there is a fair use exception before sending a "take-down notice." The video that was the subject of the lawsuit was of a family dancing to a song that was playing in the background.

[34] Federal Lanham Act of 1946, 15 U.S.C. §§ 1125; 1114(1).

[35] See Anti-Cybersquatting Act (ACPA 1999), 15 U.S.C. § 1125(d); Trademark Dilution Revision Act (2005); 15 U.S.C. § 1125.

[36] 18 U.S.C. § 1030 (E)(11). [37]

18 U.S.C. § 2707.

[38] Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn," *Wake Forest Law Review*, vol. 49 (2014), 345-391.

[39] Unlike the identity theft, the right of publicity is a tort that involves someone using the commercial value of another's likeness without permission.

[40] California, Florida, North Carolina, North Dakota, Pennsylvania, Texas, Vermont, Washington, Wisconsin, and Minnesota.

[41] Section 230 of the Communications and Decency Act protects website providers by providing immunity

from lawsuits against them for the content posted on their sites. This allows the liability to remain with the person speaking or producing the material and gives the site immunity. The provision is often considered controversial because it allows website operators to ignore criminal and offensive behavior, instead of controlling or patrolling the website.

[42] Amit Singhal, " 'Revenge porn' and Search" *Google Policy Blog*, June 19, 2015.