OpenAccessPub

Journal of Human Psychology

ISSN: 2644-1101

DOI: 10.14302/issn.2644-1101.jhp-22-4282

Opinion Article

Freely Available Online

# The 2020 Presidential Election and Should Social Media Laws that Affect the Outcome of Intellectual Property Laws Be Dramatically Changed?

**Donald L. Buresh, Ph.D., Esq.**[1,*]

[1]Morgan State University

**Corresponding author:**

Donald L. Buresh, Ph.D., Esq. Morgan State University

**Keywords:**

2020 Presidential Election, Communications Decency Act, Intellectual Property Laws, Section 230, Social Media

**Received:** Aug 11, 2022

**Accepted:** Aug 20, 2022

**Published:** Aug 27, 2022

**Editor:**

Raul Isea, Fundación Instituto de Estudios Avanzados -IDEA

## Abstract

In light of the 2020 Presidential election, this essay asks whether social media laws that affect the outcome of intellectual property be dramatically changed. The article outlines the relationship between Section 230 of the Communications Decency Act and the various intellectual property laws, including the four privacy torts, copyright laws, trade secret laws, patent laws, trademark laws, and right of publicity laws. Intellectual property is addressed because intellectual property is typically the content of social media sites. The Communications Decency is analyzed in detail, pointing out that members of both sides of the political aisle seem to believe that the Act gives social media companies tremendous political power to make or break existing members of Congress and future candidates. The paper concludes that the answer to the above question is yes.

## Introduction

During the four years that Donald Trump was President of the United States, he used social media extensively to communicate with the American people.[1] Trump's use of Twitter and other social media was unprecedented.[2] Before him, no other President had employed social media as a communication vehicle in quite the same way.[3] For the American people, this was new, exciting, and novel. What would Trump say next? How did he feel? Was he reflecting the thoughts and feelings of his base? Were the American people getting an unfiltered view of how their President acted and reacted to the events unfolding in the United States and abroad?

Could his opposition respond in kind, or at least appropriately react?

As the four years of Donald Trump's presidency marched on to its eventual conclusion on January 20, 2021, the American people became increasingly aware of the political positions of the individuals and organizations in the mainstream media and Big Tech.[4] Many conservative individuals felt that the media were biased against them. In contrast, the political left came to feel that Trump wielded power

akin to a dictator.[5] The contrast was stark during the 2020 campaign season. Trump held rally after rally, where tens of thousands of supporters came to see him, crowded in open venues such as fields, parks, and airports.[6] When Vice-President Biden held a rally, only several hundred individuals attended, usually separated by six or more feet for fear of contracting the novel coronavirus.[7] Yet, when the presidential election was held on November 3, 2020, the first Tuesday in November, there were 81 million votes cast for Joseph Biden and 74 million for Donald Trump.[8] According to Dunn, there were 159 million votes counted in the 2020 presidential election, with 239 million Americans eligible to vote.[9] In other words, 66.7 percent of the eligible voters voted in the 2020 presidential election.[10] This was remarkable. Many conservative Americans felt that the election was illegitimate. The mainstream media and the social media platforms attributed this belief to misinformation and dedicated their efforts to eradicating this conclusion in the minds of conservative Americans by the means at their disposal.[11] [12] This was the blatant contradiction facing the country. Was the election legal? Was massive election fraud involved? Was Joseph Biden now the legitimate President of the United States? These are some of the questions Americans have been grappling with since November 3, 2020.

In particular, who was to blame if fraud was involved in the election? Were the social media companies complicit? Since the 2020 election, the social media companies have de- platformed many individuals and organizations that have questioned the election's legitimacy, fueling the belief that these companies had immense political power.[13] [14] Democrats (reluctantly) and Republicans (eagerly) have realized that social media could make or break future candidates.[15] The general feeling among many Americans was that social media possessed too much political power.[16] They asked why was it that social media was so powerful. Many answered that Section 230 of the Communications Decency Act (CDA) gave social media immunity above and beyond the apparent intentions of the law.[17] [18] The purpose of the CDA was to promote the development of the Internet, not to allow social media to dominate American political conversation.[19]

Something had to change, and it had to be done soon. It is for this purpose that this paper is dedicated. This essay asks whether social media laws that affect the outcome of intellectual property laws should be dramatically changed. The reason that intellectual property is involved is that intellectual property and information make up social media content..

**Definition of Social-Media**

According to the Merriam-Webster Dictionary, social media are "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)."[20] In other words, social media are vehicles for electronic communication. The Cambridge Dictionary defines social media as "websites and computer programs that allow people to communicate and share information on the internet using a computer or cell phone."[21] According to Investopedia, social media "refers to a computer-based technology that facilitates the sharing of ideas, thoughts, and information through virtual networks and communities."[22] Social media is based on the Internet, allowing users to quickly communicate their personal information, documents, videos, and photo-graphs. Although social media is omnipresent in the United States and Europe, Asian countries lead the planet in social media usage.[23]

**Types of Social Media Laws**

There are a variety of laws that deal with social media in one way or another. First, the four common law privacy torts have some relevance when dealing with social media. Second, copyright law should be considered when focusing on social media, particularly Section 512 (c), or the safe harbor provision. The essay proceeds to look at the effect of Section 230 of the CDA on the various privacy torts and intellectual property (IP) laws, including Copyright Law, Trade Secret Law, Patent Law, and Trademark and the Right of Publicity Law. The CDA is discussed before the Right of Publicity Law because the

CDA can be an affirmative defense to the right of publicity.

**Common-Law Privacy Torts and Social Media**

The right to privacy to information regarding one's person was clarified by Prosser when he organized the right to privacy doctrine into the following four distinct torts:

- Unreasonable intrusion upon another's seclusion;
- Public disclosure of private facts;
- False light invasion of privacy; and
- Appropriation of another's name or likeness.[24] [25]

All four torts are relevant in the context of social media. An individual may post content without consent and for-profit about another that intrudes on an individual's seclusion by employing social media. The same can happen regarding the public disclosure of private facts, a false light invasion of privacy, or the appropriation of someone's name or likeness. Although state laws allow an individual to sue when such information is used commercially, private individuals and celebrities can sue in state courts for public disclosure of private facts. In other words, much like a violation of a person's right of publicity, the unauthorized use of information about a person is an encroachment of an individual's property rights. The four privacy torts imply that individuals have property rights to their personal information, and a sovereign state's responsibility is to protect individual property rights.

When considering the four privacy torts in a social media context, the question is whether there is a federal law that immunizes a tortfeasor from being sued by a plaintiff. The four privacy torts are typically embedded in state law. The Supremacy Clause in the Constitution prohibits states from interfering with the federal government's exercise of its constitutional powers. The Supremacy Clause also prevents the states from assuming any functions that are exclusively entrusted to the federal government.[26]

**Copyright Law and Social Media**

The copyright law section consists of three subsections. The first subsection discusses copyright law in general, while the second describes the Digital Millennium Copyright Act. The final subsection addresses the safe harbor provision of Section 512(c).

***Copyright Law in General***

Copyright is a form of intellectual property that is protected by United States law.[27] The protection is available for original works of authorship that are fixed in a tangible form and can be published or unpublished.[28] Copyright laws can protect software programs and only covers the form of material expression.[29] Copyright law does not safeguard concepts, ideas, techniques, or facts that make up a particular work, which is why work must be fixed in a tangible format.[30] A classic example of a physical form would be printed books on paper or original paintings.

The main goal of copyright law is to protect the creator's creativity, time, and work effort.[31] In promoting this goal, the Copyright Act of 1976 gave the copyright owner the exclusive rights to:

- Reproduce the work;
- Prepare derivative works;
- Distribute copies of the work by sale, lease, or other transfer of ownership;
- Perform the work publicly; and
- Display the work publicly.[32]

The use of copyrighted material is not an exclusive right.[33] The copyright owner also had the right to assign their copyrights to third parties.[34] A contract typically achieved the assignment of rights even though it was not legally mandated that the transfer of rights be memorialized in a written document.[35]

An author of work can create the work in their employment. This is known as "work for hire."[36] Registration of a copyright is unnecessary, but it is advantageous to have a recorded copyright.[37] According to the Berne Convention, work created after 1989 need not have a copyright notice.[38] These are the essential features of copyrights.

***Digital Millennium Copyright Act***

On October 2, 1998, President Clinton signed The Digital Millennium Copyright Act (DMCA) into law.[39] The result was that the United States of America became a signatory to the two 1996 World Intellectual Property Organization (WIPO) treaties – the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.[40] The DMCA consists of the following five titles:

- Title I – Implements the two treaties;
- Title II – Creates limitations on the liabilities of online service providers;
- Title III – Has an exemption for making a copy of a computer program to repair;
- Title IV - contains six miscellaneous provisions that relate to the functions of the Copyright Office; and
- Title V – Creates a new form of protection for the hulls of a ship.[41]

***Section 512(c) Safe Harbor Provision***

Section 512(c), or the safe harbor provision in Title II of the DMCA, generates an exemption for Internet service providers (ISPs) against infringement liability, assuming that the following criteria are met:

- An ISP must not receive financial benefit from the infringing activity;
- An ISP should not possess actual knowledge or be aware of the circumstances regarding the hosting of the infringing material;
- When provided expressed written notice by a copyright holder, an ISP must quickly take down the infringing content;
- If an ISP subjectively knows of an infringement and a reasonably prudent person would conclude that the activity is infringing, an ISP must expeditiously remove the alleged violation.[42]

The alleged infringer may contest the removal of their content. Again, the ISP must act promptly in reviewing the counter-allegations. If the ISP obeys these rules, it is safe from legal liability.[43]

The first prong of Section 512(c) requires that the ISP not receive any financial benefit from infringement by third-party content. If the ISP analyzes the infringing content and proceeds to sell the analysis results to a customer, the first prong of Section 512(c) would not be satisfied. Suppose the effect of the analysis is a digital model, physical object, or source code that produces a pictorial, graphic, or sculptural work. The work is copyrightable by the ISP,[44] and the first prong of Section 512(c) may not apply. Suppose an analysis result is a physical object created for non-utilitarian purposes, incorporating some artistic features. In that case, the physical object is eligible for copyright protection even if the software that created the object is open-sourced.[45] [46] In *Feist,* the Supreme Court opined that a low threshold of originality invokes copyright protection,[47] even though the functional characteristics of the object are not copyrightable.[48] For example, if the ISP's analysis of the infringing contents were a coffee cup, there would be no copyright protection for the ISP, and the first prong of Section 512(c) would be violated. However, if the coffee cup contained some artistic expression, like a handle that looks like the wings of a bird, then the coffee cup handle would be copyrightable, but the rest of the coffee cup would not be copyrightable.[49] Given that the ISP made a profit on selling the coffee cup, it is likely that the ISP violated the first prong of Section 512(c).

According to the second prong of Section 512(c), an ISP must not have actual knowledge or be aware of the facts and circumstances surrounding its hosting of the infringing content. However, Section 512(c) does not apply if the ISP infringes on the copyright owner's copyrights. Section 512(c) applies if the ISP does not receive financial benefit from the infringing work and is unaware of the violation. When an ISP violates these first two prongs, the ISP must cease production or face a copyright infringement suit. If the ISP is the infringer, there is no reason to engage in a negotiation with a third-party infringer. There would be two parties, the ISP infringer and the copyright holder, rather than three parties, the third-party infringer, the ISP, and the copyright holder.

Under the third prong of Section 512(c), the ISP

must expeditiously remove the offending content when given express written notice of copyright infringement by the copyright holder of third-party content. If the notice is oral versus written and the ISP does not take down the infringing content, the question is whether the ISP is immune from legal action. The ISP should insist in its policy statement that the notice be expressly written down and sent to the ISP as soon as the copyright holder discovers the infringement. Another issue arises if the ISP is not expeditious in removing the infringing content. What constitutes a reasonable time between the time notice is given to the ISP, and the infringing content is removed? It is reasonable for the ISP to give counsel time to review the facts of the case, verify that notice has occurred, and determine the current state of the law. This can happen when the alleged infringement is covered by fair use, where the employment of fair use content is not copyright infringement. In some situations, a 24-hour period may be reasonable. However, a more extended period may be acceptable if the ISP is small and does not possess the resources to comply quickly with the third prong of Section 512(c). Hopefully, a reasonable court would consider these facts when making its determination.

Finally, in the fourth prong of Section 512(c), if the ISP has subjective knowledge of the infringing content and a reasonably prudent person would consider the content infringing, then an ISP must expeditiously take down the offending content. This means that the ISP must subjectively believe that the content is infringing, regardless of whether the content is objectively infringing. If a reasonably prudent person concludes that the content is infringing, then the ISP is obliged to remove the content even if the content is not objectively infringing. This situation puts an ISP in a precarious position, for if the content is objectively not infringing, the ISP may be over-reacting, removing content when it is not necessary. One could argue that the fourth prong allows the ISP to err on caution by taking down the content. Although possibly a reasonable thing to do, the fact that Section 512(c) permits the taking down of non-infringing content would likely annoy the content owner, sometimes even inviting a lawsuit. Potential litigation is the price that society pays for protecting copyrights when infringement is an unknown commodity.

**Trade Secret Law and Social-Media**

The first subsection addresses trade secrets in general in the following two subsections. The second subsection talks about trade secrets and social media.

***Trade Secrets in General***

The Uniform Trade Secrets Act (UTSA) is legislation created by the Uniform Law Commission (ULC), a non-profit organization.[50] The USTA defines trade secrets and describes claims related to trade secrets. Currently, 47 states and the District of Columbia have adopted the UTSA.[51] According to the UTSA, a trade secret is "information, including a formula, pattern, compilation, program, device, method, technique, or process that:

- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[52]

Before the UTSA was created, the unauthorized use or disclosure of a trade secret was traditionally a common-law tort.[53] Sections 757 and 758 of the Restatement of Torts (First) established the basic principles of trade secret law that United States courts widely employed.[54] In particular, Section 757, comment b, listed six factors to be considered in deciding whether information constituted a trade secret:

- The degree to which the information is known parties outside a claimant's business;
- The degree to which parties inside the business know the information;
- The steps that were taken by a claimant to protect the secrecy of the information;
- The value of the information inside and outside the company;

- The effort or financial cost spent by a business in developing the information; and
- The ease or difficulty of acquiring or reproducing the information.[55]

The first thing to notice about the definition is that trade secrets are broadly defined.[56] There are two requirements imposed on information to be a trade secret. First, there must be economic value to the information because the information is not publicly well-known.[57] Second, effort must be expended to ensure that the information is kept secret from the public.[58] An example of a trade secret is the formula for making Coke-Cola or the herbs and spices that Kentucky Fried Chicken uses. The result is that trade secrets are a much larger breadth of information than copyrights, patents, and trademarks.[59] Trade secrets can encompass any information developed for natural persons or companies that is not publicly well-known.[60]

*Necessity of Trade Secrets.* There are seven reasons why trade secrets are necessary, including:

- New technology;
- A changing work environment;
- The increasing value of trade secret information;
- The Uniform Trade Secrets Act;
- Flexible (and expanding) scope of trade secrets;
- The rise of international threats; and
- Interaction with patent law.[61]

First, new technology, such as computers, ensures that information can be easily misappropriated.[62] Second, although companies are loathed for acknowledging this fact, current and former employees are the entities that are most frequently sued for trade secret misuse.[63] Third, trade secrets increase in value because of the ever-expanding world economy.[64] Fourth, over the years, trade secrets and secret litigation have increased because trade secret law is maturing and becoming ubiquitous.[65] Fifth, the flexible definition of a trade secret promotes additional trade secret litigation.[66] Sixth, there is an increased threat of trade secret theft as individuals and foreign nations desire to evolve technologically, thereby leveling the economic playing field.[67] Finally, the changes in U.S. patent law have tilted the balance toward trade secrets.[68]

According to Halligan and Weyland, core competencies are entrenched in trade secrets.[69] However, core competencies are sometimes seen as static phenomena.[70] What must not be forgotten is that an organization is much more than its core competencies. An organization can also be characterized by dynamic capabilities, which are "the firm's ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments."[71]

*A World without Trade Secrets.* A world without trade secrets is hard to imagine because people seem naturally selfish. They are interested in discovering specific information but desire to profit financially from their discoveries. However, some individuals appear to be trained to be altruistic. They believe that they will grow and society will grow much faster if all share information.[72] This conflict does not appear to have a resolution. From a philosophical, selfishness and altruism are contradictory opposites, wherefrom a Hegelian perspective, one is the thesis, and the other is the antithesis. If static Aristotelian logic is employed, there is no solution.[73] One side must conquer the other. But if the logic of the Hegelian dialectic is used, a synthesis emerges from a thesis and an antithesis.[74] The problem is that this author has no idea what would be the result of this synthesis. One can only suspect and hope that the synthesis would contain the better parts of the selfish desire to profit financially and the altruistic yearning to advance as a society.

*Accomplishments of Trade Secrets.* This is an interesting question that can only be answered in a capitalist economic system. Trade secrets are economic phenomena whose value derives from the economic value of information.[75] Another reason trade secrets exist comes from the Lockean labor theory of value, where individuals own their labor.[76] These days, the problem with this justification is that the vast majority of people work for corporations that require, as a condition of employment, that they sign over the rights to their labor to the

organization. In other words, trade secrets do little to preserve an individual's rights to the results of a person's labor.

Third, from a Rawlsian perspective, where the purpose of a society is to help the least advantaged, trade secrets can promote the benefit of the least advantaged by providing these individuals income through the commercial sale or licensing of the results of the trade secret information.[77] The final justification of trade secrets is the populist image or myth that if a person works both smart and hard, they too can achieve significant economic gain through discovering valuable information, protecting it from public disclosure, and reaping the profits from its possession.[78]

***Trade Secrets and Social-Media***

On May 11, 2016, President Obama signed the Defend Trade Secrets Act (DTSA) into law.[79] [80] The DTSA is a United States federal law permits a trade secret owner to sue in federal court when its trade secrets are misappropriated.[81] The DTSA is closely aligned with the UTSA. The DTSA extended the Economic Espionage Act (EEA) of 1996, criminalizing specific trade secret misappropriations and granting legal immunity to corporate whistleblowers.[82] *Schein* was the first DTSA case where the court granted a restraining order preventing an ex-employee from soliciting the plaintiff's customers.[83]

If social media is involved in infringing on a trade secret, it will likely be a misappropriation of the secret. The four possible causes of action are unauthorized acquisition, unauthorized disclosure, unauthorized use, or knowledge acquired by mistake or accident.[84] Unauthorized acquisition occurs when an individual obtains a trade secret but does not have the authority to acquire the trade secret from the trade secret owner.[85] Unauthorized disclosure happens when an individual that the trade secret owner authorizes to know the content of a trade secret discloses the trade secret to a person who is not authorized to know the content of the trade secret.[86] Unauthorized use arises when an individual that the trade secret owner authorizes to know the content of a trade secret employs the trade secret in a manner not authorized by the trade secret owner.[87] Finally, knowledge of a trade secret that is acquired by mistake or accident implies that a trade secret was obtained when an authorized individual revealed a trade secret to a third party that had reason to know that they were receiving a trade secret.[88]

In the first two instances, under the DTSA, an ISP that stored the content of a trade secret on their website would likely be held harmless. The reason is that the ISP is passively storing the trade secret on their site. In the third possibility, they would be liable if an ISP uses a trade secret stored on their site under the DTSA. However, if Section 230 of the CDA were applied, the ISP would likely be immune from prosecution, where a defendant would argue that the DCA trumps the DTSA. If the fourth misappropriation possibility occurred, an ISP could be liable under the DTSA, but again immunity would exist provided that the ISP promptly removed the infringing content from their site. One issue that should be remembered is that the DTSA extended the EEA. An unauthorized individual that acquired, disclosed, used, or otherwise obtained a trade secret by mistake or accident could also be charged under the EEA. If the defendant is an ISP, the question arises whether the CDA trumps the DTSA or the EEA, thereby holding the ISP harmless. Based on the analysis of the CDA below, the answer appears to be yes.

The two ways an individual can obtain a trade secret and not be charged for misappropriation occur when the person reverse engineers the trade secret, independently derives the trade secret, or obtains the trade secret by any lawful means.[89] Reverse engineering, also known as back engineering, is the "[d]isassembly and examination of products that are available to the public."[90]

It is a process whereby a manufactured object is deconstructed to expose its design, architecture, or unearth knowledge from the object.[91] The process is similar to scientific research, where the difference is that scientific research concerns natural phenomena, whereas reverse engineering deals with taking apart and understanding how human-made objects work.[92]

Reverse engineering is a chemical engineering,

electrical engineering, mechanical engineering, software engineering, or systems biology methodology.[93] The beneficial reasons to reverse engineer an object include:

- Reproducing legacy products that are no longer manufactured or where there are no blueprints to manufacture them;
- Examining obsolete products that are no longer supported or manufactured;
- Analyzing the design of a product to make improvements;
- Performing a competitive analysis of a competitor's product, looking for potential patent infringement;
- Servicing or repairing a product when its documentation is not available;
- Creating an interoperable product;
- Preventing crime by reverse engineering malware; and
- Analyzing why a product failed.[94]

Reverse engineering can also be employed for illegal or unethical purposes, such as copying a copyrighted or patented product without permission or unlocking a smartphone from any cell phone provider.[95]

Suppose an ISP lawfully reverse engineers a trade secret, independently derives a trade secret, or obtains a trade secret by any lawful means. In that case, the platform is not liable under the DTSA. An ISP is liable under the DTSA if the ISP unlawfully reverse-engineered the trade secret. The CDA is likely immaterial in these three instances because either the ISP lawfully attained the trade secret or acted unlawfully in acquiring the trade secret.

## Patent Law and Social-Media

This paper's Patent Law and Social Media section is divided into two subsections. The first subsection talks about patents in general. The second subsection discusses patent law from a social media perspective.

### *Patents in General*

According to the United States Patent and Trademark Office, patents are "[t]echnical inventions, such as chemical compositions like pharmaceutical drugs, mechanical processes like complex machinery, or machine designs that are new, unique, and usable in some type of industry."[96] An example of a patentable invention would be an engine that runs on water, burning hydrogen and releasing oxygen into the atmosphere. To obtain a patent, a patent applicant must show that inventions must be novel, useful, and non-obvious.[97]

An invention is novel if it is generally new and unknown to the public and gives its owner a competitive advantage.[98] Novelty is essential in assessing the patentability of an invention.[99] Novelty also means new when compared to the prior state-of-the-art. An invention must be helpful or possess utility, meaning that the invention must have specific, substantial, and credible use.[100] An invention is non-o bvious when the invention is not apparent to an individual skilled in the art.[101] In contrast to novelty, non-obviousness can exist where the prior art lacks identity with the patent claims.

A statutory bar to a patent exists when either an inventor or a third party engages in activities (e.g., public use, prior printed publication, or prior patent) that disclose the invention under consideration.[102] A patent application must contain the name(s) of the actual inventor. A patent claim can be invalidated if the applicant is not the inventor but derived the patent from another individual's work.[103] In the United States, and before March 16, 2013, when there were competing inventors of an invention, the inventor who was first to invent received the patent.[104] However, after March 13, 2013, the United States became the first-to-file nation. If a patent was filed before March 13, 2013, the patent follows the first-to-invent rules.[105]

### *Patents and Social-Media*

Because an inventor may lose their ability to patent an invention if they publicly disclose the invention before filing a patent application, utmost secrecy is paramount. This means that the details of an invention will most likely never appear on social media. If an inventor decides to reveal information about a patent to a third party, the third-party should sign a non-disclosure

agreement. Inventors should be rather careful to whom they reveal information about an invention. It should be remembered that all patents begin as trade secrets, where the conditions for ensuring that trade secrets are legally protected until the patent is granted.

Social media can be employed when an individual infringes a patent. According to Section 271(a) of the United States patent law, an individual who "without authority makes, uses, offers to sell, or sells any patented invention, within the united states, or imports into the united states any patented invention during the term of the patent therefor[e], infringes the patent."[106] When without authority, a third party employs social media to use, offers to sell, or sells a patented invention, the third party is infringing on the patent owner's rights.[107] According to Section 230 of the CDA, once an ISP is made aware of the infringing conduct and offending content, the ISP is obliged to remove the content promptly. Failure to remove the offending content may invalidate the ISP's immunity from prosecution. The CDA will be discussed in greater detail in an upcoming section of this paper.

**Trademark Law and Social-Media**

This section is broken up into three subsections. The first subsection discusses trademark law in general. The second subsection deals with trademarks and domain names. The third subsection talks about trademarks and cybersquatting.

***Trademarks in General***

According to the United States Patent and Trademark Office, a trademark is a "word, phrase, design, or a combination that identifies your goods or services, distinguishes them from the goods or services of others, and indicates the source of your goods or services."[108] American trademark law originates from seventeenth-century English to nineteenth-century American case law. Trademarks are like cattle brands, where ranchers use them to identify their cattle.

Trademarks are important because they distinguish one merchant from another, helping customers decide where to take their business.

*Blanchard* was the first English decision of a claim based on the use of a trademark.[109] Here, a playing card maker sought an injunction to prevent the defendant from using the Great *Mogul* as a stamp on his cards. The case suggested that the plaintiff had the sole right to the stamp because his company was given a charter from King Charles I. The judge denied the injunction, probably because politics influenced the decision. After all, Charles I was beheaded for treason in 1642.[110]

The definition of a trademark emphasizes that a mark must be distinctive because it must identify and distinguish goods so that a customer knows the source of the goods.[111] A trademark qualifies as distinctive if either:

1) It is inherently distinctive of source; or
2) It has developed an acquired distinctiveness of source.[112]

A mark that intrinsically lacks distinctiveness can qualify as distinctive if they have acquired distinctiveness over time, otherwise known as a secondary meaning. A descriptive term may nonetheless become a trademark if the description becomes descriptive in the minds of consumers. For example, "American Airlines" is a descriptive term, yet today it is uniquely associated with the company with the same name.

The Lanham Act identifies the following five categories of terms when determining whether a term deserves trademark protection. The classes are (1) generic, (2) descriptive, (3) suggestive, (4) arbitrary, or (5) fanciful.[113] A generic term refers to the genus of a given product, which is a species. Under common law, neither generic nor descriptive terms could be valid trademarks.[114] A descriptive but not generic term is a word (or words) "that merely describes a product or its ingredient, quality, characteristic, function, feature, purpose or use."[115] An example of a descriptive mark is "Cold and Creamy" for ice cream.[116] In *Stix Products*, the court opined that a mark is suggestive if "it requires imagination, thought, and perception to conclude the nature of [the] goods."[117] A mark is arbitrary if the mark is "composed of a word or words that have a common meaning in the language of the relevant jurisdiction; however, that meaning is unrelated to the goods or services for which the mark is used."[118] Finally, a trademark is fanciful if the

zmark "consists of a combination of letters with no meaning; thus, it is an invented word."[119]

Even if a mark is distinctive, it can be denied protection if it is covered by one of the statutory bars specified in the Lanham Act. According to the Lanham Act Section 2, the registration of a mark will be barred if it consists of an immoral, deceptive, or scandalous matter.[120]

A mark can also be barred from registration if it "disparage[s] or falsely suggest[s] a connection with persons, living or dead, institutions, beliefs, or national symbols, or bring them into contempt, or disrepute."[121] A non-geographic deceptive mark can neither be registered nor protected under federal trademark law.[122] However, a non-geographic "deceptively misdescriptive" mark may be registered and protected under federal law only if the trademark owner can demonstrate that the mark has developed secondary meaning as a designation of its source.[123]

A trademark must be used in commerce, where the mark is employed in the ordinary course of trade and not made merely to reserve the right of a mark.[124] The mark must be put on a product sold or transported in commerce or used for advertising purposes.[125] By commerce, it means all commerce that Congress regulates.[126] Finally, a third party can use a trademark provided the mark is used in "good faith only to describe the goods or services of [the trademark owner] or their geographical origin."[127] This is known as the fair use of a mark.

***Trademarks and Domain Names***

The Internet is no longer a technological mystery but an integral part of everyday life. The Internet is a proven useful tool in all businesses. These days with little effort, anyone can register a domain name, allowing access to customers worldwide. Trademark law protects some domains and permits mark owners to take legal action against domains that infringe on legitimate trademark rights, just as if an illicit domain was a traditional mark that infringed on a legitimate mark. Trademark disputes over domain names can be due to good-faith disagreements among competitors over the right to use specific words, symbols, or other devices present in traditional trademark disputes. Trademark disputes can also arise over the employment of metatags or keywords to attract customers via search engines or triggers for pop-up advertising. The sale of keywords and some listings have generated potential trademark rights issues.

A domain name is a significant component of a Uniform Resource Locator (URL) used to locate a website or a web page. The Lanham Act defines a domain name as "any alphanumeric designation registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet."[128] It should be remembered that obtaining a domain name is not a substitute for securing trademark rights; in and of itself, it does not establish trademark rights by using an Internet address. A domain name has two parts, the top-level generic domain name (e.g., ".com") and the second- level domain name (e.g., "amazon" or "google"). A second-level domain name can include:

- An existing trademark and primary brand significance;
- An existing trademark with a dictionary meaning;
- A trademark with other words (e.g., "ford-parts")
- An ordinary generic word (e.g., "computers.com");
- A string of characters that are an acronym (e.g., "ibm.com"); or
- A random string of alphanumeric characters (e.g., "abc123.com").[129]

There are challenges associated with domain names. First, domain names can exist without reference to a trademark, good, or service. Second, organizations that register domain names do so on a first-come, first-served basis without considering trademark ownership. The issue is that a given domain name may not be associated with a trademark or marginally associated with a mark due to businesses focusing on trademark rights without thinking about domain name issues.[130]

An organization should probably register its trademarks and domain names with the United States Patent and Trademark Office and register with foreign

jurisdictions. If an entity performs this simple task, it is less likely that a search engine will sell corporate brands as keywords to competitors or that competitors will be able to company brands as metatags or descriptive terms on their website.[131] Because the cost of registering a domain name is essentially negligible, a firm should probably attempt to register a slew of domain names that use hyphens (e.g., "united-airlines.com") and misspellings (e.g., "unitdairlnes.com") to act as a defensive perimeter against would-be cyber squatters.[132] Part of the challenge of maintaining a defense perimeter is constant vigilance or recognizing the possibility that there are character gaps in the perimeter. Above all, entities that own domain names should post prominent notices on their websites, expressly stating their ownership of their marks and domain names.[133]

***Trademarks and Cybersquatting***

Cybersquatting is a deliberate, bad faith, and abusive registration of Internet domain names with the intent to gain financial remuneration from an entity.[134] Cybersquatting usually violates an organization's trademark rights.[135] Even so, the law secures the rights of a trademark owner because a "domain name is more than a mere address: like trademarks, second-level domain names communicate information as to source."[136]

Trademark owners can halt cyber squatters through arbitration under the Uniform Domain Name Resolution Policy (UDRP) by filing suit in the United States under the Anti- Cybersquatting Consumer Protection Act (ACPA).[137] Because the courts have upheld the constitutionality of the ACPA, a plaintiff must prove:

1) The plaintiff owns the mark, the mark being either a registered mark or a common-law mark;
2) The defendant's domain name is identical to, or confusingly similar to, the plaintiff's domain name; and
3) The defendant used, registered, or trafficked in the domain name with a bad faith intent to profit from the plaintiff's trademark.

There are nine factors that the Lanham Act provided to help courts decide when a defendant is acting in bad faith, including:

"(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names that the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection(c)(1) of section 43."[138]

Although none of the nine criteria are determinative by themselves, when based on the circumstances of the case, the nine criteria can be used to form a viable argument for bad faith.

There are various defenses to a domain name suit. A defendant could argue fair use to overcome a cybersquatting claim. A defendant could attempt to show that the mark in question is generic or descriptive without secondary meaning. In both instances, the mark would not be protected by law, so no cybersquatting would have occurred. The offending domain could be a parody or a "gripe site" (i.e., a domain name registered by a disgruntled former employee with no commercial intent) on the trademark owner's domain name, preventing a domain name suit in the future. Anyone of these defenses or others could effectively defend against a cybersquatting suit.[139]

Once a domain owner recognizes the existence of a potential cyber squatter, the owner can do nothing, monitor the use of the offending name to see if a problem arises, send a cease and desist letter, institute a UDRP proceeding, or institute a civil suit in federal court under ACPA.[140] Which option to choose depends on an organization's objectives and goals. Sometimes waiting to pursue legal action is appropriate, while other times is not. There are no easy answers here.

**Communications Decency Act and Social-Media**

This section of this essay is divided into three parts. The first subsection discusses the CDA in general. The second subsection focuses on the debate regarding the social protections provided to social media by Section 230. The third subsection highlights the proposed legislation to limit Section 230.

***Section 230 in General***

The CDA was the first attempt by Congress to regulate pornographic material on the Internet. CDA is the short name for Title V of the Telecommunications Act (TA) of 1996.[141] First, the CDA attempted to regulate indecency on the Internet when indecency affected children and obscenity in cyberspace.[142] Second, Section 230 of Title 47 of the United States Code was interpreted by the CDA to mean that ISPs are not publishers and therefore not legally liable for the words posted by individuals that employ their services.

Section 230 of Title 47 of the United States Code was enacted as part of the CDA. It provides immunity from third-party content for organizations that offer website platforms. In particular, Section 230(c)(1) gives immunity from liability for ISPs and users of interactive computer services who publish information from third parties.[143] It says, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[144] Section 230(c)(2) provides a "Good Samaritan" safe harbor from civil suits, where an ISP removes or edits third-party material that the ISP believes to be obscene. It is irrelevant whether the Constitution protects the speech in question.[145] In 1997, the Supreme Court struck down CDA's anti-indecency provisions in *Reno,* [146] although Section 230 was severed from the rest of the CDA, remaining good law.[147] Since Reno, there have been several unsuccessful challenges to Section 230.[148]

Although Section 230 has frequently been referred to as the law that permitted the Internet to develop,[149] the protections provided by Section 230 are not unbounded. In 2018, Section 230 was amended by the Stop Enabling Sex Traffickers Act (FOSTA-SESTA), requiring ISPs to remove digital content that violated federal and state sex trafficking laws.[150] Recently, Section 230 has been scrutinized on issues relating to hate speech and ideological biases that major technology companies possess regarding political discussions, particularly during the 2020 United States presidential election.[151]

When analyzing whether Section 230 immunity is available, the courts apply the following three-prong test:

1) The defendant must provide or use an interactive computer service;
2) The cause of action must consider the defendant as a publisher or speaker of the harmful information; and
3) The defendant must not be the information content provider of the harmful information.[152]

The immunity given by Section 230 is limited. The

exceptions to Section 230 include federal criminal liability,[153] electronic privacy violations,[154] intellectual property claims,[155] and state laws consistent with the statute.[156] The immunity does not apply to content created or developed by the ISP,[157] and the CDA does not bar civil actions based on promissory estoppel.[158] For intellectual property claims, the courts are divided. For example, in *CCBill,* the Ninth Circuit opined that the exception to intellectual property law only applies to federal intellectual property claims, such as copyright infringement, trademark infringement, and patents, rather than state intellectual property claims.[159] Finally, ISPs must comply with the DMCA to ensure Section 512(c) safe harbor protections.[160]

***Debate on Protections for Social-Media***

The two early challenges to Section 230 came from *Zeran*[161] and *Roommates.com.*[162] In both cases, the courts upheld Section 230. However, in recent years, Big Tech companies like Facebook, Google, and Apple Computer were scrutinized, where it was alleged that Russian agents used websites to influence the 2016 presidential election in favor of Donald Trump. These organizations were criticized for not preventing users from engaging in hate speech and harassment on social media.[163] There has been a lively debate about how Section 230 should be changed.

*Platform Neutrality.* Senators Ted Cruz and Josh Hawley have argued that Section 230 should apply only to politically neutral ISPs. They claim that when an ISP takes a political position, it is acting as a publisher or speaker of user content, deciding what gets published and what does not get published.[164]

*Hate Speech.* Because of the shootings in El Paso, Texas,[165] and Dayton, Ohio,[166] Section 230 has been considered in establishing liability regarding online hate speech. In the El Paso shooting, the assailant posted an alleged hate speech on 8kun, where 8kun was previously called 8chan, Infinitechan, or Infinitychan, an imageboard of user-created messages. However, hate speech is usually protected under the First Amendment, and Section 230 immunizes ISPs, provided that the content of the speech is not illegal.

*Terrorism-Related Content.* With the passage of FOSTA-SESTA, legal scholars Citron and Wittes found that terrorist groups maintained social media accounts despite federal laws making it illegal to support terrorist groups.[167] The Second Circuit held that under Section 230, technology companies are not necessarily liable for civil claims predicated on terrorism-related content.[168]

*2020 Department of Justice Review.* In February 2020, the United States Department of Justice (DOJ) chaired a workshop regarding Section 230, big tech companies, and antitrust violations. Former Attorney General Barr stated that Big Tech had matured and questioned the need for Section 230.[169] The outcome of the workshop was that the DOJ issued the following four recommendations to Congress in June 2020:

1) Incentivize ISPs to address illicit content, and remove Section 230 immunity when the illicit content deals with child abuse, terrorism, and cyberstalking, particularly when courts have notified a platform of the illicit material;
2) Remove protections from civil lawsuits when the plaintiff is the federal government;
3) Disallow Section 230 protection regarding antitrust actions; and
4) Promote discourse and transparency by defining existing terms such as “otherwise objectionable” and “good faith.”[170]

***A Selection of Section 230 Cases***

*Defamation*. In the vast majority of cases, the courts have upheld Section 230. In *Blumenthal*, the court upheld AOL’s immunity to modify or remove content that an independent contractor created because it was not the information content provider.[171] In *Batzel*, immunity was upheld for an ISP that distributed an email, even though the plaintiff opined that the email was defamatory.[172] In *Barrett*, court immunity was sustained for an individual Internet user who republished defamatory statements on a listserv, an application that distributes messages to subscribers on an electronic mailing list, because the defendant was a user of interactive computer services.[173] However, in *badbusinessbureau.com*, the court rejected the

defendant's motion to dismiss due to immunity because the defendant wrote disparaging editorial messages in response to the plaintiff's belittling report titles and headings.[174]

*False Information.* In *Gentry*, the court upheld eBay's immunity for claims predicated on forged autograph sports items sold online.[175] In *Goddard*, the court sustained immunity against fraud and money laundering claims because the court believed that Google was not responsible for misleading advertising purchased from Google by a third party.[176] In *Grindr*, the Second Circuit upheld immunity for the LGBT dating app regarding the misuse of false profiles that a natural person created.[177]

*Sexually Explicit Content.* In the *City of Livermore*, the California Court of Appeals found that a public library was not responsible when a patron downloaded pornography from the library's computers, even though the computers did not restrict access by minors.[178] In *Doe,* the Fifth Circuit upheld the immunity of MySpace, a social networking site, from negligence and gross negligence for not instituting safety measures to protect minors from online sexual predators.[179] In *LLC Hoffman*, the court upheld immunity for Backpage.com, a classified advertising website, when the firm contested a Washington state law (SB6251) that made companies that provide third-party content liable for crimes related to a minor.[180]

*Miscellaneous Cases.* In *Chicago Lawyer's Committee,* the court upheld immunity for Craigslist because of the discriminatory statements in classified advertisements by third parties.[181] In *Delfino,* the California Appellate Court upheld immunity from state tort claims when an employee used their employer's email system to send threatening messages.[182] Finally, in *Force,* the Second Circuit upheld Facebook's Section 230 immunity even though the site hosted terrorism-related content. The plaintiff asserted that because Facebook hosted content that resulted in the deaths of several individuals, Facebook was liable under the United States Anti- Terrorism Act (USATA).

***Proposed Legislation to Limit Section 230***

In 2020, various bills were introduced to Congress that intended to reduce the liability protections in Section 230 afforded Internet platforms.

*EARN IT Act of 2020.* In March 2020, with bipartisan support, the Eliminating Abuse and Rampant Neglect of Interactive Technologies (EARN-IT) was introduced into the Senate. The bill had the support of the National Center on Sexual Exploitation (NCSE)[183] and the National Center for Missing and Exploited Children (NCMEC).[184] The Electronic Frontier Foundation (EFF),[185] the American Civil Liberties Union (ACLU),[186] and many other organizations criticized the bill for fear that the best practices in the bill would create backdoors for encryption.[187] The bill amended Section 230(c)(2) by allowing any state to serve an ISP with a lawsuit if it failed to address child sexual abuse on their platform or if they permitted end-to-end encryption without ensuring that law enforcement could decrypt the information. The bill passed the Senate Judiciary Committee by 22-0 on July 2, 2020,[188] and was introduced in the House on October 2, 2020.[189]

*Limiting Section 230 Immunity to Good Samaritans Act*. In June 2020, Senators Marco Rubio, Kelly Loeffler, and Kevin Cramer requested that the Federal Communications Commission (FCC) review the Section 230 protections afforded Big Tech companies, concluding that it was time to look at Section 230 anew.[190] On June 17, 2020, Senator Hawley introduced the bill in the Senate with co-sponsors, Senators Rubio, Braun, and Cotton.[191]

*Platform Accountability and Consumer Transparency (PACT) Act.* In June 2020, Senators Brian Schatz and John Thune introduced this bipartisan bill into the Senate. The bill would require Internet platforms to publish public statements on how they moderate, demonetize, and remove user content from their sites. The ISPs would also be required to publish quarterly reports with the relevant statistics, summarizing their actions for the quarter. Essentially, these quarterly reports would be similar to a 10-Q, required by the Securities Exchange Act of 1934. The bill would permit the states' Attorney Generals to enforce actions against Internet platforms.[192]

*Behavioral Advertising Decisions Are Downgrading Services (BAD ADS) Act.* Senator Hawley introduced this bill in July 2020. The bill would remove Section 230 immunity protection for large service providers that employed behavioral advertising.[193]

*Online Freedom and Viewpoint Diversity Act.* In September 2020, Senators Lindsay Graham, Roger Wicker, and Marsha Blackburn introduced this bill into the Senate. The bill proposes to remove Section 230 liability protection for a site that fails to provide a reason for moderating or restricting content, demanding that the ISP have an objective and reasonable belief that the content violated the site's terms. The bill would also replace the vague term "objectionable" with a specific definition.[194]

*Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH) Act.* In February 2021, Senators Mark Warner, Mazie Hirono, and Amy Klobuchar introduced this bill into the Senate. The bill makes multiple changes to Section 230. First, the bill would change Section 230(c)(1) to cover speech but not information, ensuring that ISPs are liable for illegal speech. Second, the bill would remove Good Samaritan immunity regarding federal and state civil rights laws, antitrust laws, cyberstalking laws, human rights laws, or wrongful death suits. Third, the bill would eliminate immunity for commercial speech, such as advertising or marketplace listings. Finally, the bill would require ISPs to comply with court orders regarding removing the content listed above.[195]

*Executive Order 13925.* On May 28, 2020, President Donald Trump the Executive Order on Preventing Online Censorship (EO 13925).[196] The Executive Order opined that media companies that edit content, except when restricting posts that are violent, obscene, or harassing, are "engaged in editorial conduct" and thus lose their immunity under Section 230(c)(1).[197] However, the courts have interpreted the phrase "in good faith" based on its plain meaning, EO 13925 specified conditions where good faith could be revoked. The FCC, the Commerce Department, the National Telecommunications and Information Administration (NTIA), and the Attorney General would determine whether an ISP was biased. According to the executive order, the Federal Trade Commission (FTC) would decide if a federal lawsuit was warranted.[198] Although there was a great deal of controversy regarding EO 213925, on May 14, 2021, President Joseph Biden rescinded the executive order.[199]

*Health Misinformation Act.* In July 2021, Senators Amy Klobuchar and Ren Ray Luján introduced into the Senate a bill that would make ISPs liable for publishing health misinformation during a public health emergency as determined by the Department of Health and Human Services (DHHS).[200]

*Justice Against Malicious Algorithms Act.* In October 2021, Representatives Anna Eshoo, Frank Pallone Jr., Mike Doyle, and Jan Schakowsky introduced this bill into the House. The bill would remove Section 230 protections that dealt with personalized recommendation algorithms that provide users with content that knowingly or recklessly furthers physical or severe emotional injury.[201]

**Right of Publicity Law and Social Media**

This section contains two subsections. The first subsection addresses the right of publicity in general. The second subsection talks about the right of publicity and social media.

***Right of Publicity in General***

The right of publicity is an intellectual property right recognized in just over 50 percent of the states.[202] It is a branch of unfair competition law. The right of publicity protects individuals against the unauthorized commercial use of a person's identity, including their name, likeness, or image.[203] The impact of the right of publicity has expanded due to the national and international growth of the Internet. Individuals possess previously unheard-of technology to market and exploit themselves and their identities contractually in life and after death regarding the sale of goods and services.[204] Violations of the right of publicity frequently occur in unfair competition cases or in suits where a person's identity also serves as a trademark where there is a possibility for confusion or dilution.[205] The scope of the right of publicity differs by state. Foreign nations have

laws that are similar to state right of publicity laws. Currently, there is no federal right of publicity law.[206]

Under most state laws, to prove a violation of the right of privacy, a plaintiff must prove that:

1) The use of an individual's identity (whether living or dead) identifies the individual;
2) The use of a person's identity is employed in commerce, harming the person's right of publicity interest; and
3) The individual has the standing to bring the right of publicity suit, either on their own or as an exclusive licensee, heir, etc.[207]

It is common for a right of publicity claim to arise in conjunction with a violation of the Lanham Act because the Act covers trademark law, unfair competition, and false advertising.[208] Trademark laws protect a plaintiff's identity when there is potential confusion with the defendant's use of that identity. The laws regarding the right of publicity are possibly broader than trademark laws because there is no need to show the likelihood of confusion.[209] Sections 2(a) and 2(c) of the Lanham Act are similar to the right of publicity. After all, the sections prevent a defendant from registering a mark in some situations.[210] Finally, there is federal protection against the unauthorized use of a person's name as a domain name. The Intellectual Property and Communications Omnibus Reform Act of 1999 generated a civil action against a defendant that uses a plaintiff's name as a domain name, intending to sell the domain name back to the plaintiff or a third party.[211] According to the Third Circuit, the Act applies if the domain name was registered before November 29, 1999, and later reregistered to another entity.[212] In contrast, the Ninth Circuit opined that the original registration would apply even if the registration were before November 29, 1999.[213]

There are various defenses to a right of publicity action, including copyright preemption, where a state right of publicity law is preempted by federal copyright law where the individual's identity is fixed within a tangible medium such as a photograph or voice recording.[214] The right of publicity may also be preempted by the First Amendment based on the right of freedom of expression.[215] Artistic expression,[216] parody,[217] politically, newsworthy, or factually based speech,[218] anti-SLAPP statutes,[219] and the CDA[220] are all First Amendment defenses to the right of publicity. Other defenses in a right of publicity claim include the first sale doctrine,[221] the statute of limitations,[222] the single publication rule,[223] and abandonment.[224]

***Right of Publicity and Social Media***

A presence on the Web has dramatically increased individuals' ability to exploit others' identity rights for commercial gain, particularly when people are putting their personal information or photographs of themselves and others on social media websites such as Facebook. Because sites have terms of service agreements that prevent individuals from violating the intellectual property rights of others, YouTube, Twitter, and Facebook have policies that prevent infringement, particularly copyright piracy, which at times overlaps with the right of publicity.[225] Websites that stream live broadcasts are difficult to police for violations of the right to publicity because of a broadcast's spontaneity.[226] Also, startup organizations without extensive financing may be unwilling or unable to police their sites for infringing activity.[227]

With the presence of multiplayer online games, there is a question of the scope of the right of publicity laws.[228] In multiplayer games, players use animated characters or avatars who buy and sell goods and services in a virtual marketplace. In virtual reality, players could believe their avatars are a proxy for themselves and their identity, where a player possesses the right to control their avatars under the right of publicity. Avatars may also appear in other games and may be subject to a right of publicity contract when a game involves celebrities.[229] The contract in the real world may likely govern publicity rights in the virtual world. If a contract does not determine publicity rights or the scope of a contract is exceeded, the rights of publicity laws in the real world would determine the outcome of a case, including First Amendment defenses.[230] Because the Internet provides

dynamic content, it is possible that secondary liability could exist.[231] Secondary liability is where one party is liable for infringement where the party aids in linking sites that infringe on a plaintiff's rights of publicity. The defendant is not sued for a direct infringement but as a party that aided and abetted an infringement from another party.

## Conclusion

Should social media laws that affect the outcome of intellectual property laws be dramatically changed? The answer to this question is a resounding yes. The common-law privacy torts, copyright laws, trade secret laws, patent laws, trademark laws, and right of publicity laws are all intellectual property laws whose outcome may be affected by applying Section 230 of the Communications Decency Act to a given set of circumstances. On their face, the intellectual property laws do not warrant being changed. However, the CDA is a horse of a different color. This article has attempted to show that the CDA can affect the outcome of IP laws because it provides an ISP with immunity from prosecution when specific conditions occur.

The more general question is whether the CDA can trump any laws. In other words, is there a current law on the books that supersedes the CDA? If so, what is the law? If not, then does the CDA make ISPs omnipotent because there are no laws that can eclipse the CDA? From a practical perspective, many people believe that ISPs and their platforms have the power to dictate the behavior of the American people, mainly if one is a politically conservative American, even when violent speech and violence in other countries have all been ignored.[232] [233] After all, Facebook, Twitter, and YouTube have permanently banned President Trump from their sites. It seems that the President of the United States was the most powerful political leader on the planet, but apparently, no more. If Facebook, Twitter, and YouTube can de-platform a United States President, does not that action imply that these organizations are more powerful than the President of the United States? The answer to this question again appears to be yes.[234]

One does not have to be a political conservative to appreciate that when another possesses tremendous political power. This can be readily seen by the number of bills that have been presented to the House and Senate in an attempt to curtail the power granted to ISPs by Section 230. Members of both sides of the aisle have proposed a seemingly kaleidoscopic of bills whose sole purpose is to rein in ISPs by limiting their immunity granted by Section 230. Based on the sampling of cases outlined in this article, it is apparent the federal and state judiciary favor the continuance of Section 230.

*Wormwood, from The Screwtape Letters*, written by C. S. Lewis, presented various options to Screwtape on how to torment Patient. Wormwood asked Screwtape which option he should select. Screwtape told Wormwood to implement all of them.[235] Perhaps the best solution is to combine the various bills that want to limit the scope of Section 230 into one comprehensive bill, curtailing the scope of Section 230 immunity. Both sides of the aisle should remember Lord Acton's famous remark that power corrupts and absolute power corrupts absolutely.[236] No one is immune when a party yields absolute or near-absolute power. It is time to let the penny drop and evaluate Section 230 anew. The time appears to be correct, but will Congress act? That is the question.

## Miscellaneous Considerations

## Author Contributions

The author has read and agreed to the published version of the manuscript.

## Funding

This research received no external funding.

## Institutional Review Board Statement

Not applicable.

## Informed Consent Statement

Not applicable.

## Conflicts of Interest

The author declares no conflict of interest.

## Acknowledgments

I thank Jeffery K. Hardin for our many discussions on the technical aspects of obtaining a patent. His insights, lively humor, perspective on the state of the world are invaluable to me.

## Abbreviations

The following abbreviations are used in this manuscript:

ACLU : American Civil Liberties Union

ACPA : Anti-Cybersquatting Consumer Protection Act

BAD ADS : Behavioral Advertising Decisions Are Downgrading Services Act

CDA : Communications Decency Act

DHHS : Department of Health and Human Services

DMCA : Digital Millennium Copyright Act

DOJ : United States Department of Justice

DTSA : Defend Trade Secrets Act

EARN-IT : Eliminating Abuse and Rampant Neglect of Interactive Technologies

EEA : Economic Espionage Act

EFF : Electronic Frontier Foundation

EO 13925 : Executive Order on Preventing Online Censorship

EONA : Existence, Ownership, Notice, and Access

FCC : Federal Communications Commission

FOSTA-SESTA : Stop Enabling Sex Traffickers Act

FTC : Federal Trade Commission

IP : Intellectual Property

ISP : Internet Service Provider

NCMEC : National Center for Missing and Exploited Children

NCSE : National Center on Sexual Exploitation

NTIA : National Telecommunications and Information Administration

PACT : Platform Accountability and Consumer Transparency Act

SAFE TECH : Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act

SLAPP : Strategic Lawsuits Against Public Participation

TA : Telecommunications Act

UDRP : Uniform Domain Name Resolution Policy

ULC : Uniform Law Commission

URL : Uniform Resource Locator

USATA : United States Anti-Terrorism Act

UTSA : Uniform Trade Secrets Act

WIPO : World Intellectual Property Organization

## Endnotes

1. Frank Newprot, *Deconstructing Trump's Use of Twitter*, Gallup (May 16, 2018), *available at* https://news.gallup.com/poll/234509/deconstructing-trump-twitter.aspx.
2. *Id.*
3. *Id.*
4. Monica Anderson, *Most Americans Say Social Media Companies Have too Much Power, Influence in Politics*, Pew Research Center (Jul. 22, 2020), *available at* https://www.pewresearch.org/fact-tank/2020/07/22/most- americans-say-social-media-companies-have-too-much-power-influence-in-politics/.
5. *Id.*
6. *As an example, see*, Daniela Flamini, *Trump's Opa-Locka Rally Draws Thousands, Raising COVID Concerns*, Nbc South Florida (Nov. 1, 2020), *available at* https://www.nbcmiami.com/news/politics/decision-2020/trump- to-host-evening-rally-in-opa-locka/2314852/.
7. *As an example, see*, Reuters Staff, *Fact check: Biden's Bristol, PA Rally Did Not Have Only 25 People in Attendance*, Reuters (Oct. 27, 2020), *available at* https://www.reuters.com/article/uk-factcheck-biden-bristol-rally- 25-peop/fact-check-bidens-bristol-pa-rally-did-not-have-only-25-people-in-attendance-idUSKBN27C2RO.
8. Adrienne Dunn, *Fact Check: Over 159 Million People Voted in the US General Election*, USA Today

(Dec. 20, 2020), *available at* https://www.usatoday.com/story/news/factcheck/2020/12/30/fact-check-fals-president-than- were-registered-u-s/4010087001/.

9. *Id.*

10. *Id.*

11. Darrell M. West, *How to Combat Fake News and Disinformation*, Brookings Institute (Dec. 18, 2017), *available at* https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

12. Emily Gersema, *How Americans Can Help Stop Fake News*, Usc News (Dec. 1, 2020), *available at* https://news.usc.edu/179176/how-to-help-stop-fake-news-misinformation-usc-experts/.

13. Monica Anderson, *supra*, note 4.

14. Shirin Gafferey, *Does Banning Extremists Online Work? It Depends.*, Vox (Feb. 3, 2022), *available at* https://www.vox.com/recode/22913046/deplatforming-extremists-ban-qanon-proud-boys-boogaloo-oathkeepers- three-percenters-trump.

15. Mark Jurkowitz, & Amy Mitchell, *An Oasis of Bipartisanship: Republicans and Democrats Distrust Social Media Sites for Political and Election News*, Pew Research Center (Jan. 29, 2020), *available at* https://www.pewresearch.org/journalism/2020/01/29/an-oasis-of-bipartisanship-republicans-and-democrats-distrust- social-media-sites-for-political-and-election-news/.

16. Monica Anderson, *supra*, note 4.

17. Jordan Doll, *Section 230 Immunity and Being Cancelled: A Cause of Action Against Twitter*, Cardozo Arts & Ent. L. J. (Aug.& Ent. L. J. (Aug.1, 2021), *available at* https://cardozoaelj.com/2021/08/30/section-230-immunity- and-being-cancelled-a-cause-of-action-against-twitter/.

18. Michael D. Smith, & Marshall Van Alstyne, *It's Time to Update Section 230*, Harvard Business Review (Aug. 12, 2021), *available at* https://hbr.org/2021/08/its-time-to-update-section-230.

19. Sara L. Ziegler, *Communications Decency Act of 1996 (1996)*, The First Amendment Encyclopedia (2009), *available at* https://www.mtsu.edu/first-amendment/article/1070/communications-decency-act-of-1996.

20. *Social Media*, Merriam-Webster Dictionary (n.d.), *available at* https://www.merriam- webster.com/dictionary/social%20media.

21. *Social Media*, Cambridge Dictionary (n.d.), *available at* https://dictionary.cambridge.org/us/dictionary/english/social-media.

22. Maya Dollarhide, *Social Media,* Investopedia (Aug. 31, 2021), available at https://www.investopedia.com/terms/s/social-media.asp.

23. Digital Marketing Institute, *Social Media: What Countries Use It Most & What Are They Using?*, Digital Marketing Institute (Nov. 2, 2021), *available at* https://digitalmarketinginstitute.com/blog/social-media-what- countries-use-it-most-and-what-are-they-using.

24. William L. Prosser, *Privacy*, 48 Calif. L. Rev.3 (Aug. 1960), *available at* DOI: 10.15779/Z383J3C.

25. *See generally*, Richard A. Posner, *The Right of Privacy*, 12 Geo. L. Rev. 12, 393-422 (Spring 1978), *available at* https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?arti-cle=1021&context=lectures_pre_arch_lectures_sibley.

26. U.S. Const., Art. IV, Para. 2.

27. *What Is a Copyright?*, Findlaw (n.d.), *available at* http://smallbusiness.findlaw.com/intellectual-property/what- is-copyright.html.

28. *Id.*

29. *Id.*

30. *Id.*

31. *United States Copyright Office*, A Brief Introduction and History (n.d.), *available at* https://www.copyright.gov/circs/circ1a.html.

32. *What is a Copyright?*, *supra*, note 27.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *United States Copyright Office Summary*, The Digital Millennium Copyright Act of 1998 (Dec. 1998), *available at* https://www.copyright.gov/legislation/dmca.pdf.

40. *Id.*

41. *Id.*

42. See 17 U.S. Code § 512 - Limitations on liability relating to material online. Section 512(c) is concerned with what conditions ensure that an ISP is exempt from liability.

43. *Id.*

44. See 17 U.S.C. § 102(a) of the Copyright Act.

45. *Esquire, Inc.. v. Ringer*, 591 F.2d 796, 804 (D.C. Cir. Aug. 14, 1978), *available at* https://casetext.com/case/esquire-inc-v-ringer-2.

46. Nicole Martinez, *Does Copyright and Trademark Law Protect 3D Printing?*, ART Law Journal (April 28, 2016), *available at* https://alj.artrepreneur.com/does-copyright-and-trademark-law-protect-3d-printing/.\

47. *Feist Publications, Inc. v. Rural Telephone Service Company, Inc.,* 499 U.S. 340, 362 (1991) (the Supreme Court ruled that originality is not a stringent standard in the sense that the work need only be independently created. It need not be novel or original), *available at* https://supreme.justia.com/cases/federal/us/499/340/#tab-opinion- 1958569.

48. *Kieselstein-Cord v. Accessories by Pearl, Inc.*, 632 F.2d 989, 993 (2nd Cir. 1980). (The case was decided on the grounds of conceptual separability.), *available at* https://casetext.com/case/kieselstein-cord-v-accessories-by-pearl- inc.

49. *Id.*

50. *Trade Secret*, Legal Information Institute (n.d.), *available at* https://www.law.cornell.edu/wex/trade_secret.

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. R. Mark Halligan & Richard F. Weyland, Trade Secret Asset Management 2018: A Guide to Information Asset Management Including Rico And Blockchain (Weyland Associates, Inc. 2018).

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 Berkeley Tech. L. J. 2 (Fall 2012), *available at* https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1958&context=btlj.

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. Halligan & Weyland, *supra*, note 56.

70. *What Is a Competency?*, National Competence Assessment System (n.d.), *available at* https://en.mycompetence.bg/static/9.

71. David J. Teece, Gary Pisano, & Amy Shuen, *Dynamic Capabilities and Strategic Management*, 18 Strategic Mgt. J. 7, 509-533 (Aug. 1997), *available at* https://www.business.illinois.edu/josephm/BA545_Fall%202015/Teece,%20Pisano%20and%20Shuen%20(1997).p df.

72. Robin Smith, *Aristotle's Logic*, Stanford Encyclopedia of Philosophy (2017), *available at* https://plato.stanford.edu/entries/aristotle-logic/.

73. Julie E. Maybee, *Hegel's Dialectics*, Stanford Encyclopedia of Philosophy (2016), *available at* https://plato.stanford.edu/entries/hegel-dialectics/.

74. *Id.*

75. Michael Risch, *Why Do We Have Trade Secrets?*, 11 Marquette Intel.Prop. L. Rev. 1 (2007), *available at* https://scholarship.law.marquette.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article= 1089&context=iplr;Why.

76. *Id.*

77. *Id.*

78. *Id.*

79. Pub.L. 114–153; 18 U.S.C. § 1836

80. Gregory Korte, *Obama Signs Trade Secrets Bill, Allowing Companies to Sue*, USA Today (May 11, 2016), *available at* https://www.usatoday.com/story/news/politics/2016/05/11/obama-signs-trade-secrets-bill-allowing- companies-sue/84244258/.

81. *Id.*

82. Eric Goldman, The New 'Defend Trade Secrets Act' Is the Biggest IP Development in Years, Forbes (Apr.28, 2016), available at https://www.forbes.com/sites/ericgoldman/2016/04/28/the-new-defend-trade-secrets-act-is-the- biggest-ip-development-in-years/?sh=2cde6c154261.

83. *Henry Schein, Inc. v. Cook*, 191 F. Supp. 3d 1072 (N.D. Cal. 2016), *available at* https://casetext.com/case/henry- schein-inc-v-cook-4.

84. *Trade Secret Infringement*, Justia (Oct. 2021), *available at* https://www.justia.com/intellectual-property/trade- secrets/infringement/.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Defend Trade Secrets Act of 2016*, Pub. L. 114-153 (May 11, 2016), *available at* https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf.

90. *Reverse Engineering*, Nolo dictionary (n.d.), *available at* https://www.nolo.com/dictionary/reverse-engineering-term.html.

91. Eldad Eilam, Reversing: Secrets of Revers Eengineering, (John Wiley & Sons 2005).

92. *Id.*

93. Alejandro F. Villaverde & Julio R. Banga, *Reverse Engineering and Identification in Systems Biology: Strategies, Perspectives and Challenges*, 11 J. of the Royal Soc. 91 (Feb. 06, 2014), *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3869153/.

94. Ken Thayer, *supra*, note 93.

95. *Id.*

96. *Trademark, Patent, or Copyright*, United States Panent and Trademark Office (n.d.), *available at* https://

www.uspto.gov/trademarks/basics/trademark-patent-copyright.

97. Amy L. Landers, Undertanding Patent Law (LexisNesis 3rd ed. 2017).

98. *Id.* See 35 U.S.C. § 102.

*99. Id.*

*100.Id.*

*101.Id.*

*102.Id.*

*103.Id.*

*104.Id.*

*105.Id.*

106.35 U.S. Code § 271(a).

*107.Id.*

108.*Trademark, Patent, or Copyright*, *supra*, note 97.

109.*Blanchard v. Hill*, 2 Atk. 484 (Ch.), 26 Eng. Rep. 692 (1742).

110.Blair Worden, *The Execution of Charles I*, History Today (Feb. 2, 2009), *available at* https://www.historytoday.com/archive/execution-charles-i.

111.Barton Beebe, Trademark Law: An Open-Source Casebook 37 (Creative Commons Summer 2019).

112.*Wal-Mart Stores, Inc. v. Samara Bros. Inc*., 529 U.S. 205, 201 (2000), *available at* https://supreme.justia.com/cases/federal/us/529/205/.

113.Barton Beebe, *supra*, note 112 at 39.

*114.Id.*

115.*Trademark Strength*, International Trademark Association (Nov. 5, 2020), *available at* https://www.inta.org/fact-sheets/trademark-strength/.

*116.Id.*

117.*Stix Products, Inc. v. United Merchants and Manufacturer, Inc*., 295 F. Supp. 479, 488 (S.D.N.Y. 1968), *available at* https://law.justia.com/cases/federal/district-courts/FSupp/295/479/2081140/.

118.*Trademark Strength*, *supra*, note 116.

*119.Id.*

120.Lanham Act Section 2; 15 U.S.C. § 1052.

*121.Id.*

122.*Id.* at § 1052(a).

123.Lanham Act §§ 2(e)(1) and 2(f); 15 U.S.C. §§ 1052(e ) (1) and 2(f).

124.Lanham Act § 45; 15 U.S.C. § 1127.

*125.Id.*

*126.Id.*

127.Lanham Act § 33(b)(4); 15 U.S.C. §§ 1115(b)(4).

128.15 U.S.C. § 1127.

129.Jonathan S. Jennings, & J. Michael Monahan, Trademarks and Unfair Competition, 2-5 (Law Journal Press 2014).

130.*Id.* at 2-6.

131.*Id.* at 2-9.

132.*Id.* at 2-10.

133.*Id.* at 2-12.

134.*Id.* at 2-13.

*135.Id.*

136.*Brookfield Communications, Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036, 1055 (9th Cir. 1999), *available at* https://law.resource.org/pub/us/case/reporter/F3/174/174.F3d.1036.98-56918.html.

137.Jonathan S. Jennings, & J. Michael Monahan, *supra*, note 130 at 2-13.

138.15 U.S.C. § 1125(d)(1)(B)(i).

139.Jonathan S. Jennings, & J. Michael Monahan, *supra*, note 130 at 2-20 to 2-22.

140.*Id.* at 2-31.

141.*Telecommunications Act of 1996,* Pub. L. 104-104, *available at* https://www.congress.gov/104/plaws/publ104/PLAW-104publ104.htm.

*142.Id.*

143.*47 U.S. Code § 230 - Protection for Private Blocking and Screening of Offensive Material*, Legal Information Institute (n.d.), *available at* https://www.law.cornell.edu/uscode/text/47/230.

*144.Id.*

*145.Id.*

*146.Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997), *available at* https://supreme.justia.com/cases/federal/us/521/844/#tab-opinion-1960201.

*147.*Id.

148.Anna Salvatore, *Supreme Court Declines to Review Case on Section 230 (For Now)*, Lawfare (Oct. 14, 2020), *available at* https://www.lawfareblog.com/supreme-court-declines-review-section-230-for-now.

149.Anshu Siripurapu, *Trump and Section 230: What to Know*, Council on Foreign Relations (Dec. 2, 2020), available at https://www.cfr.org/in-brief/trump-and-section-230-what-know.

150.*Stop Enabling Sex Traffickers Act*, Pub. L. 115-164 (The law makes it illegal to knowingly assist, facilitate, or support sex trafficking. The law also amended the Section 230 safe harbors by excluding enforcement of federal or state sex trafficking laws from its immunity), *available at* https://www.congress.gov/115/plaws/publ164/PLAW- 115publ164.pdf.

151.David Morar, & Chris Riley, *A Guide for Conceptualizing the Debate over Section 230*, Brookings Institute: Tech Stream (Aug. 9, 2021), *available at* https://www.brookings.edu/techstream/a-guide-for-conceptualizing-the- debate-over-section-230/.

152.Kathleen Ann Ruane, *How Broad A Shield? A Brief Overview of Section 230 of the Communications Decency Act*, Congressional Research Service (Feb. 21, 2018), *available at* https://fas.org/sgp/crs/misc/LSB10082.pdf. See Section 230(e)(1).

153.See Section 230(e)(1).

154.See Section 230(e)(4).

155.See Section 230(e)(2).

156.See Section 230(e)(3).

157.*Anthony v. Yahoo! Inc.*, 421 F. Supp.2d 1257 (N.D. Cal. 2006), *available at* https://casetext.com/case/anthony-v- yahoo-inc-2.

158.*Barnes v. Yahoo! Inc.*, 570 F.3d 1096 (9th Cir. 2009), *available at* https://casetext.com/case/barnes-v-yahoo-inc- 3.

159.*Perfect 10, Inc. v. CCBill*, LLC, 488 F.2d 1102, 1118 (9th Cir. 2007), *available at* https://casetext.com/case/perfect-10-inc-v-ccbill-llc.

160.TechDirt, *Explainer: How Letting Platforms Decide What Content to Facilitate Is What Makes Section 230 Work*, ABOVE THE LAW (Jun. 21, 2019), *available at* https://abovethelaw.com/2019/06/explainer-how-letting- platforms-decide-what-content-to-facilitate-is-what-makes-section-230-work/.

161.*Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997),[2] cert. denied, 524 U.S. 937 (1998) (The Fourth Circuit held that Section 230 "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."), *available at* https://casetext.com/case/zeran-v-america-online.

162.*Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (The Ninth Circuit sitting *en banc* held that immunity under Section 230 did not apply to an interactive online operator whose questionnaire violated the Fair Housing Act.), *available at* https://casetext.com/case/fair-v-roommates.

163.Niam Yaraghi, *How Should Social Media*

*Platforms Combat Misinformation and Hate Speech?*, Brookings Institute (Apr. 9, 2019), *available at* https://www.brookings.edu/blog/techtank/2019/04/09/how-should-social-media-platforms-combat-misinformation-and-hate-speech/.

164. Mike Masnick, *Ted Cruz Demands a Return of the Fairness Doctrine, Which He Has Mocked in the Past, Due to Misunderstanding CDA 230*, Techdirt (Apr. 13, 2018), *available at* https://www.techdirt.com/articles/20180412/23230639618/ted-cruz-demands-return-fairness-doctrine-which-he-has- mocked-past-due-to-misunderstanding-cda-230.shtml.

165.Craig Huber, *El Paso Marks 2 Years Since Deadly Mass Shooting: 'Our Hearts Remain Broken'*, Spectrum News (Aug. 3, 2021), *available at* https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2021/08/03/el-paso- marks-2-years-since-deadly-mass-shooting---our-hearts-remain-broken-

166.Paul P. Murphy, Konstantin Toropin, Drew Griffin, Scott Bronstein, & Eric Levenson, *Dayton Shooter Had An Obsession With Violence and Mass Shootings, Police Say*, Cable News Network (CNN) (Aug. 7, 2019), *available at* https://www.cnn.com/2019/08/05/us/connor-betts-dayton-shooting-profile/index.html.

167.Danielle K. Citron, & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, Scholarly Commons at Boston University School of Law (Jul. 2017), *available at* https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1616&context=faculty_scholarship.

168.Jeffrey D. Neuburger, *Facebook Shielded by CDA Immunity against Federal Claims for Allowing Use of Its Platform by Terrorists*, National Law Review (Aug. 9, 2019), *available at* https://www.natlawreview.com/article/facebook-shielded-cda-immunity-against-federal-claims-allowing-use-its- platform.

169.Lauren Feiner, *AG Barr Takes Aim at a Key Legal Protection for Big Tech Companies*, CNBC (Feb. 19, 2020), *available at* https://www.cnbc.com/2020/02/19/ag-barr-takes-aim-at-section-230-a-key-protection-for-tech- firms.html.

170.Brent Kendall, & John D. McKinnon, *Justice Department Proposes Limiting Internet Companies' Protections*, The Wall Street Journal (Jun. 17, 2020), *available at* https://www.wsj.com/articles/justice-department-to- propose-limiting-internet-firms-protections-11592391602?mod=djemalertNEWS.

171. *Blumenthal v. Drudge*, 992 F. Supp. 44, 49–53 (D.D.C. 1998), *available at* https://law.justia.com/cases/federal/district-courts/FSupp/992/44/1456770/.

172.*Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), *available at* https://casetext.com/case/batzel-v-smith-2.

173.*Barrett v. Rosenthal*, 40 Cal. 4th 33 (2006), *available at* https://casetext.com/case/barrett-v-rosenthal.

174.*MCW, Inc. v. badbusinessbureau.com(RipOff Report/ Ed Magedson/XCENTRIC Ventures LLC)* 2004 WL 833595, No. Civ.A.3, *available at* https://h2o.law.harvard.edu/cases/4517.

175.*Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816, 830 (2002), *available at* https://law.justia.com/cases/california/court- of-appeal/4th/99/816.html.

176.*Goddard v. Google, Inc.*, C 08-2738 JF (PVT), 2008 WL 5245490, 2008 U.S. Dist. LEXIS 101890 (N.D. Cal. December 17, 2008), *available at* https://casetext.com/case/goddard-v-google.

*177.Herrick v. Grindr*, 765 F. App'x 586 (2nd Cir. 2019), *available at* https://casetext.com/case/herrick-v-grindr-llc- 3.

178.*Kathleen R. v. City of Livermore*, 87 Cal. App. 4th 684, 692 (2001), *available at* https://law.justia.com/cases/california/court-of-appeal/4th/87/684.html.

179.*Doe v. MySpace*, 528 F.3d 413 (5th Cir. 2008), *available at* https://casetext.com/case/doe-v-myspace-4.

180.*Backpage.com LLC v Hoffman et al.*, Civil Action No.

13-cv-03952 (DMC) (JAD), *available at* https://www.eff.org/files/2014/01/28/d.n.j._2-13-cv-03952_36.pdf.

*181.Chicago Lawyers' Committee For Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008), *available at* https://caselaw.findlaw.com/us-7th-circuit/1046308.html.

182.*Delfino v. Agilent Technologies*, 145 Cal. App. 4th 790 (2006), cert denied, 128 S. Ct. 98 (2007), *available at* https://casetext.com/case/delfino-v-agilent-tech.

183.*STATEMENT – National Center on Sexual Exploitation Supports EARN IT Act,* National Center On Sexual Exploitation (Mar. 5, 2020), *available at* https://endsexualexploitation.org/articles/statement-national-center-on- sexual-exploitation-supports-earn-it-act/.

184.*NCMEC Supports New Legislation to Protect Children*, National Center for Missing and Exploited Children (Mar. 5, 2020), *available at* https://www.missingkids.org/blog/2020/earn-it-act-2020.

185.Elliot Harmon, *Congress Must Stop the Graham-Blumenthal Anti-Security Bill*, Electronic Frontier Foundation (Jan. 31, 2020), available at https://www.eff.org/deeplinks/2020/01/congress-must-stop-graham- blumenthal-anti-security-bill.

186.Ronald Newman, Neema Singh Guliani, Kate Ruane, & Ian Thompson, *ACLU Letter of Opposition to EARN IT Act Manager's Amendment*, American Civil Liberties Union (Jul. 1, 2020), *available at* https://www.aclu.org/letter/aclu-letter-opposition-earn-it-act-managers-amendment.

187.Adi Robertson, *Congress Proposes Anti-Child Abuse Rules to Punish Web Platforms — And Raises Fears about Encryption*, The Verge (Mar. 5, 2020), *available at* https://www.theverge.com/2020/3/5/21162983/congress- senate-earn-it-act-lindsey-graham-richard-blumenthal-section-230-encryption-bill-proposed.

188.C. Fisher, *EARN IT Act Amendments Transfer the Fight over Section 230 to the States*, Engadget (Jul. 2, 2020), *available at* https://www.engadget.com/earn-it-act-amendments-pass-senate-judiciary-committee-165030518.html.

189.Joe Mullin, Urgent: *EARN IT Act Introduced in House of Representatives*, Electronic Frontier Foundation (Oct. 2, 2020), *available at* https://www.eff.org/deeplinks/2020/10/urgent-earn-it-act-introduced-house- representatives.

190.Tobias Hoonhunt, GO*P Senators Ask FCC to 'Clearly Define' Section 230 Protections for Big Tech*, National Review (Jun. 9, 2020), *available at* https://www.nationalreview.com/news/gop-senators-ask-fcc-to-clearly-define- section-230-protections-for-big-tech/.

191.Russell Brandom, *Senate Republicans Want to Make It Easier to Sue Tech Companies for Bias*, The Verge (Jun. 17, 2020), *available at* https://www.theverge.com/2020/6/17/21294032/section-230-hawley-rubio-conservative- bias-lawsuit-good-faith.

192.Makena Kelly, *The PACT Act Would Force Platforms to Disclose Shadowbans and Demonetizations*, The Verge (Jun. 24, 2020), *available at* https://www.theverge.com/2020/6/24/21302170/facebook-google-brian-schatz- john-thune-section-230-content-moderation.

193.Adi Robertson, *Sen. Josh Hawley Wants to Strip Legal Protections from Sites with Targeted Ads*, The Verge (Jul. 28, 2020), *available at* https://www.theverge.com/2020/7/28/21344894/josh-hawley-bad-ads-act-behavioral- advertising-bill-section-230.

194. Makena Kelly, *Republicans Pressure Platforms with New 230 Bill*, The Verge (Sep. 8, 2020), *available at* https://www.theverge.com/2020/9/8/21428079/republicans-pressure-platforms-230-bill-liability-protection- blackburn-lindsey-graham-wicker.

195. Emily Birnbau, & Issie Lapowsky, *This Is the Democrats' Plan to Limit Section 230*, Protocol (Feb. 5, 2021), *available at* https://www.protocol.com/policy/democrats-plan-section-230.

196.Donald J. Trump, *Executive Order on Preventing Online Censorship*, The White House (May 28, 2020),

*available at* https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-preventing-online-censorship/.

197.Sam Dean, *The Facts about Section 230, the Internet Speech Law Trump Wants to Change*, The Los Angeles Times (May 28, 2020), *available at* https://www.latimes.com/business/technology/story/2020-05-28/the-facts-about- section-230-the-internet-speech-law-trump-wants-to-change.

198.Bobby Allyn, *Stung By Twitter, Trump Signs Executive Order To Weaken Social Media Companies*, National Public Radio (May 28, 2020), *available at* https://www.npr.org/2020/05/28/863932758/stung-by-twitter-trump- signs-executive-order-to-weaken-social-media-companies.

199.Kim Lyons, *Biden Revokes Trump Executive Order thatTargeted Section 230*, The Verge (May 15, 2021), *available at* https://www.theverge.com/2021/5/15/22437627/biden-revokes-trump-executive-order-section-230- twitter-facebook-google.

200.Makena Kelly, *Senators Target Section 230 to Fight COVID-19 Vaccine Misinformation*, THE VERGE (Jul. 22, 2021), *available at* https://www.theverge.com/2021/7/22/22588903/covid19-misinformation-section-230-facebook- joe-biden-white-house.

201.Adi Robertson, *Lawmakers Want to Strip Legal Protections from the Facebook News Feed*, The Verge (Oct. 14, 2021), *available at* https://www.theverge.com/2021/10/14/22726290/malicious-algorithms-section-230-bill-eshoo- pallone-doyle-schakowsky-facebook-whistleblower.

*202.* Jonathan S. Jennings, & J. Michael Monahan, *supra*, note 230 at 5-2

*203.Id.*

*204.Id.*

205.*Id.*

206.*Id.* at 5-3.

207.*Id.* at 5-10.

208.*Id.* at 5-17.

209.*Id.* at 5-18.

210.U.S.C. §§ 2(a) and 2(c). In *Buffett v. Chi-Chi's, Inc.*, 226, U.S.P.Q. 428 (T.T.A.B. 1985), an individual obtains a protectable interest in a name or its equivalent under Section 2(a), where the appropriated name uniquely identifies an individual. Also in *Ross v. Analytical Technology, Inc.*, 51 U.S.P.Q.2d 1269, 1275-76 n. 14 (T.T.,A.B. 1999), if Section 2(c) is viewed as a right of publicity, it should be construed as the right of an individual to control the commercial use of their identity, including the use of a person's identity via social media.

*211.*See 15 U.S.C. § 8131.

212.*Schmidheimy v. Weber*, 319 F.3d 581, 582-83 (3rd Cir. 2003), *available at* https://casetext.com/case/schmidheiny-v-weber-4.

213.*GoPets. Ltd. V. Hise*, 657 F3d 1024, 1031-33 (9th Cir. 2011), *available at* https://casetext.com/case/gopets-ltd-v- hise.

214.Jonathan S. Jennings, & J. Michael Monahan, *supra*, note 130 at 5-20,

215.*Id.* at 5-23.

216.*Comedy III Productions. Inc. v. Gary Saderup, Inc.*, 21 P.3d 797, 810 (2001). (The California Supreme Court created a balancing test between the First Amendment and the right of publicity predicated on whether the work added significant creative elements that trans-formed into something more than a just celebrity likeness or imitation.), *available at* https://caselaw.findlaw.com/ca-court-of-appeal/1288836.html.

217.*Cardtoons, L.C. v. Major League Baseball Players Association*, 95 F.3d 959 (10th Cir. 1996). (The sale of parody trading cards that featured the names or likenesses of major league baseball players was held to be protected speech under the First Amendment.), *available at* https://casetext.com/case/cardtoons-lc-v-mlbpa.

218.For example, see: -
*1) Carson v. Here's Johnny Portable Toilets, Inc.*, 698 F.2d 831, 836-37 (6th Cir. 1983), *available at* https://law.justia.com/cases/federal/district-courts/FSupp/498/71/1652758/.
*2) Cardtoons, L.C. v. Major League Baseball Players Association*, 95 F.3d 959 (10th Cir. 1996), *available at* https://law.justia.com/cases/federal/district-courts/FSupp/838/1501/2255031/,
*3) Paulsen v. Personality Posters, Inc.,* 59 Misc.2d 244 (1968), *available at* https://casetext.com/case/paulsen-v-personality-posters.
*4) Friends of Phil Gramm v. Americans for Phil Gramm in '84*, 587 F. Supp. 769 (E.D. Va. 1984), *available at* https://law.justia.com/cases/federal/district-courts/FSupp/587/769/1753000/.

219.SLAPP is an acronym for "Strategic Lawsuits Against Public Participation." The purpose of these statutes are to dismiss right of publicity cases that are filed with a state court to suppress free speech and are without merit.

220.The Communications Decency Act states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." See *Perfect 10, Inc. v. CCBill*, LLC, 488 F.2d 1102, 1118 (9th Cir. 2007) (citing 47 U.S.C. §§ 230 (c)(1), (e)(3)), *available at* https://casetext.com/case/perfect-10-inc-v-ccbill-llc.

221.*Allison v. Vintage Sports Plaques*, 136 F.3d 1443, 1448 (11th Cir. 1998). (The Eleventh Circuit decided that when a product is sold a second time, an individual's right of publicity no longer held.), *available at* https://casetext.com/case/allison-v-vintage-sports-plaques.

222.*Blair v. Nevada Lanning Partnership*, 369 Ill. App.3d 318 (2006) (The court held that the common law statute of limitations was one year, even though the Illinois Right of Publicity Act did not specify a statutory time limit.), *available at* https://casetext.com/case/blair-v-nevada-landing-partnership.

223.The single publication rule limits the number of times a plaintiff may object to multiple copies of something referencing the identity right in question. For example, see the California Uniform Single Publication Act, Cal. Civ. Code § 3425.3.

224.*Negri v. Schering Corp*., 333 F. Supp.101, 104-05 (S.D.N.Y. 1971) (The plaintiff changed their appearance so much that no identification was possible.), *available at* https://law.justia.com/cases/federal/district- courts/FSupp/333/101/1606328/.

225.Jonathan S. Jennings, *Right of Publicity Law Meets Social Media*, American Bar Association: Section of Intellectual Property Law (Aug. 5, 2012), *available at* https://www.pattishall.com/pdf/JSJ- ABA%20Right%20of%20Publicity%20Law%20Meets%20Social%20Media.pdf.

*226.*Ian C. Ballon, Paul W. Garrity, & Jennifer L. Barry, *Trademark Threat @ Facebook, Twitter and Other Social Networking Websites*, Strafford (Oct. 28, 2010), *available at* http://media.straffordpub.com/products/trademark-threat-facebook-twitter-and-other-social-networking-websites-2010-10-28/presentation.pdf.

227.Brad Stone, *Young Turn to Web Sites Without Rules*, The New York Times (Jan. 2, 2007), *available at* https://www.nytimes.com/2007/01/02/technology/02net.html.

*228.*Youjeong Kim, & S. Shyam Sundar, *Me, Myself, and My Avatar in* Virtual Social Identity and Consumer (Routledge 2009).

229.*No Doubt v. Activision Publishing, Inc.*, 702 F. Supp.2d 1139, 1140 (C.D. Cal. 2010), *available at* https://scholar.google.com/scholar_case?case=8975777450937949912&hl=en&as_sdt=6&as_vis=1&oi=scholarr.

230.*Id.*

231.*Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1183-84 (C.D. Cal. 2002) (The court relied the joint liability principle in the Restatement (Second) of Torts § 876.), *available at* https://casetext.com/case/perfect- 10-inc-v-cybernet-ventures-inc.

232.Jessica Guyenn, *'You're the Ultimate Editor,' Twitter's Jack Dorsey and Facebook's Mark Zuckerberg Accused of*

*Censoring Conservatives*, USA Today (Nov. 17, 2020), *available at* https://www.usatoday.com/story/tech/2020/11/17/facebook-twitter-dorsey-zuckerberg-donald-trump-conservative- bias-antitrust/6317585002/,

233.Adam Satariano, *After Barring Trump, Facebook and Twitter Face Scrutiny About Inaction Abroad*, The New York Times (Jan. 17, 2021), *available at* https://www.nytimes.com/2021/01/14/technology/trump-facebook- twitter.html.

234.Shirin Ghaffary, & Rani Molla, *Here's Just How Much People Have Stopped Talking about Trump on Facebook and Twitter*, Vox (May 6, 2021), *available at* https://www.vox.com/recode/22421396/donald-trump-social-media- ban-facebook-twitter-decrease-drop-impact-youtube.

235.CS. Lewis, The Screwtape Letters (Samizdat University Press May 2, 1941).

236.*Absolute Power Corrupts Absolutely*, Literary Devices (n.d.), *available at* https://literarydevices.net/absolute-power-corrupts-absolutely/.