EMORY | LAW

Emory Law Journal

Volume 69 | Issue 4

2020

Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection

Jesse Lake

HEY, YOU STOLE MY AVATAR!: VIRTUAL REALITY AND ITS RISKS TO IDENTITY PROTECTION

ABSTRACT

Virtual reality (VR) consists of technology that injects users into a virtual world and will allow users to interact on an unprecedented level of cyber intimacy. VR technology is at a consumption tipping point as the technology is now cheaper and more accessible than ever before. Given the possible applications of VR in professional and business settings, some users will use their true name and likeness to interact with others, creating an effective extension of their person into the virtual world. By injecting their real identity into VR, these users are subject to risks of identity misappropriation—or the unauthorized use of their name and likeness by others. While identity misappropriation is already a sizeable problem in current social media interaction, VR is poised to exacerbate the issue. Unlike current social media identity misappropriations that yield only fixed media such as still photos, short videos, and written thoughts, when a VR identity is appropriated the thief can both create new content and continually interact with other people as the stolen identity. The problem is further intensified by other factors such as the real-time interaction between users, sophistication of perpetrators, and increased user investment in their virtual identity.

As it stands, the current substantive legal framework for redress of online identity misappropriation amounts to a web of inconsistent privacy laws leaving gaps in protection for the millions of users that log onto the VR servers. These inconsistencies are substantially caused by procedural barriers brought about by dated Internet laws. These procedural barriers include Internet personal jurisdiction, strong judicial preference toward protecting the anonymity of anonymous online users and sweeping immunity for Internet Service Providers (ISP). Together, these barriers leave plaintiffs without a defendant to sue: Anonymity and personal jurisdiction laws make enforcement against the appropriator virtually impossible, and ISP immunity prevents the plaintiff from suing the VR provider.

This Comment will argue for the lifting of these procedural barriers to give victims of VR identity misappropriation the opportunity to bring their claim to court. The proposed solutions include reworking personal jurisdiction precedent, adopting a plaintiff-friendly John Doe subpoena standard, and rewriting the Communications Decency Act to both reduce immunity and establish a victim compensation fund. Implementing these proposals will deter

VR identity thieves from committing future misappropriations and incentivize VR providers to police their own products.

INTRODUCTION

Increasingly, there is an augmented world growing among us. This world is virtual, created by state-of-the-art virtual reality (VR) technology that immerses users into computer-generated experiences. Users will be able to accomplish a wide range of activities, including shopping at an Amazon VR kiosk,[1] holding "face-to-face" business meetings in virtual conference rooms,[2] or watching a live NBA game from courtside seats.[3] This technology will, quite literally, add a new reality to people's everyday lives. But VR will also create new legal questions. These are questions that our legal system must answer before millions of users log onto the VR server. Without these answers, the legal landscape of VR will be governed by private user agreements that consumers will likely not even read but can substantially limit their rights in their new world.

Current laws have not been tailored to provide adequate recourse to the many transgressions that can occur in a VR world. The adoption of VR is one direct example of technology moving faster than the law, as our society is becoming transfixed by cyberspace. Particularly, identity misappropriation, while already a pervasive problem with current cyber technology,[4] will likely be a more frequent and dangerous issue in VR. Identity misappropriation occurs when someone uses the identity of another person without authorization to extract some type of benefit.

In the VR world, everyone will possess an online identity (or avatar)[5] that they will use to interact with others. A user's avatar is the virtual manifestation

---

[1] Jeremy Horwitz, *Watch Amazon's VR Kiosks Transform the Future of Shopping*, VENTURE BEAT (July 12, 2018, 7:07 AM), https://venturebeat.com/2018/07/12/watch-amazons-vr-kiosks-transform-the-future-of-shopping.

[2] DOGHEAD SIMULATIONS, https://www.dogheadsimulations.com (last visited Oct. 12, 2018).

[3] NBA, http://www.nba.com/xr (last visited Oct. 12, 2018).

[4] Jo Ling Kent & Michael Cappetta, *Fake Facebook Profiles Cause Heartbreak for Families and Colleagues*, NBC NEWS (July 26, 2018, 7:17 PM), https://www.nbcnews.com/business/consumer/fake-facebook-profiles-cause-heartbreak-families-colleagues-n895091. The article reports various instances of identity theft through Facebook, including a deceased police officer's Facebook profile created depicting "new life" in another state and an Atlanta city official finding his identity plastered across multiple fake Facebook profiles attempting to attract women. *Id*. The article also states that Facebook has disabled over 1.3 billion fake profiles. *Id*. *See also* Linda Childers, *Sextortion: How a New Breed of Predator Exploits Victims Through Their Own Computers*, ALLURE (Oct. 16, 2017), https://www.allure.com/story/online-predators-blackmail-sextortion-victims-explicit-images ("[T]his new breed of online predator is far savvier and more dangerous."); Martin Van Beyen, *'I'm Horrified': Facebook Woman Preyed on Schoolboys*, SYDNEY MORNING HERALD (Apr. 18, 2011), https://www.smh.com.au/technology/im-horrified-facebook-woman-preyed-on-schoolboys-20110418-1dkwd.html (discussing a twenty-eight-year-old woman who used several fake profiles to befriend forty high school boys, then would sometimes kill the fictitious profile using other fake profiles to break the news).

[5] An avatar is a personalized graphical illustration that represents a computer user, or a character or alter ego that represents that user. *Avatar*, TECHNOPEDIA, https://www.techopedia.com/definition/4624/avatar (last

of their actual person and will serve as their identity in VR society. From local "small-city" servers (hosting 10–20 users) to large "metropolitan" server farms (hosting millions of users), users will be known in their VR communities by the likeness and popularity[6] of their avatar. Thus, as users become incentivized to gain popularity by investing in their VR avatar, criminals will be even more apt to exploit the popularity of other avatars.

VR will further exacerbate the issue of identity misappropriation because VR enables users to interact with a level of unprecedented intimacy. These interactions will occur in real time, robbing victims of the opportunity to authenticate the validity of avatars they interact with. These interactions could occur in a virtual marketplace, nightclub, or office building, and will mimic real-world human interaction. Hence, while VR communication elevates digital communication to quasi-organic human interaction, it also creates an environment where users cannot verify exactly who (or what) they are interacting with, leaving many fraudsters undiscovered and free to dupe more victims.

Victims of these frauds manifest on both sides of the transgression. On the one hand, there will be avatars whose identities are stolen and used to defraud other VR users. And on the other hand, there are the users that are defrauded by stolen VR avatars. As with any crime, the damages of such actions depend on the circumstances of the crime. Some can be high profile, such as a thief that steals the identity of a prominent businessperson and broadcasts a "lucrative" business opportunity to his millions of followers. Or that same thief can publish the confidential conversations that the businessperson had with their partners. Other instances may be more localized but just as severe, such as stealing the identity of an ordinary person to interact with that person's lover. The possible types of these misappropriations can be endless and, if left unaddressed, would lead to a collapse of trust in the VR world.

From a substantive legal perspective, the victim's recourse depends on many different factors, including the motivation of the infringer and the popularity of the user. Some jurisdictions only recognize an action for identity

visited Oct. 24, 2018).

[6] In VR, the popularity of the avatar can be measured by a VR social credit score, following, reviews, or rankings from other users. *See* Kevin Houser, *Report: America Has A Social Credit Score System Much Like China's*, Futurism (Aug. 27, 2019), https://futurism.com/america-social-credit-system-china (Insurance companies now base premiums by the content of one's social media feed. A restaurant software company called PatronScan maintains a list of objectionable customers that restaurants can use to exclude certain people.) As The most concerning aspect of this U.S. social credit score is that it operates entirely separate from the U.S. justice system. *Id*.

misappropriation when the perpetrator derived a commercial or monetary benefit, while others have broader definitions of what constitutes a benefit.[7] Additionally, some jurisdictions permit recovery only when the victim was aware of the misappropriation, leaving victims who were unaware of the misappropriation without remedy.[8] These inconsistencies leave gaps in identity protection for the millions of eventual VR users.

The reason for these inconsistencies likely stems from the many procedural restraints brought about by dated computer and Internet laws. These restraints have limited the number of cases heard on the subject, hindering the legal evolution of identity misappropriation laws. These outdated Internet laws have produced intractable cyber jurisdictional questions, sweeping protections for anonymous cyber criminals, and broad immunity for Internet Service Providers (ISP).[9]

As an illustration, imagine two VR users whose avatars depict their true name and likeness. Then, an identify thief comes in and copies both avatars, but for different purposes. Avatar A is copied to endorse his new clothing line at his VR storefront, and Avatar B is copied purely because the thief likes the way the avatar looks and walks around a VR club interacting with others as Avatar B. While the act of misappropriation in both instances is functionally the same, the redressability for each victim will depend on a number of factors. Some of these factors include the purpose of the misappropriation, the commercial value of the user's likeness (if any), and the jurisdiction of the VR technology enabling the interaction.[10] This uneven application of identity misappropriation is worrisome for the millions who will enter the VR world, and may stifle the idealized concept[11] of a virtual world where users use their true name and likeness to interact with others if they fear that their identity can be stolen without recourse.

Accordingly, this Comment will argue that the procedural barriers brought by Internet law need to be revamped to allow the substantive identity protection

---

[7] *See infra* Part II.

[8] *See infra* Part II.

[9] *See infra* Part I.

[10] Jason Zenor, *If It's in the Game: Is There Liability for User-Generated Characters that Appropriate a Player's Likeness?*, 16 JOHN MARSHALL REV. INT. PROP. L. 291, 296 (2017).

[11] The idealized concept refers to a VR society where users use their true identity and likeness as their avatar. *Infra* notes 65–68 and accompanying text. This effectively creates a "real" world within the virtual. This preference for true identity has already been seen with popular social media platforms. *See* Chuna Mui, *Why Facebook Beat MySpace, and Why MySpace's Revised Strategy Will Probably Fail*, FORBES (Jan. 12, 2011), https://www.forbes.com/sites/chunkamui/2011/01/12/why-facebook-beat-myspace-and-why-myspaces-revised-strategy-will-probably-fail/#11043dae2c9a (Facebook allows users to connect using real images uploaded by the user to create a digital identity).

law to evolve. First, Part I will discuss the major technological developments and characteristics of VR and what makes VR ripe for identity misappropriation. Part II analyzes the current legal sources of identity protection and the shortfalls therein. Part III explains relevant Internet law and its various procedural wrinkles that have inhibited the substantive law from evolving.

After laying this framework, Part IV offers proposals to overcome the various procedural hurdles and analyzes their effect on the substantive law. Some of these changes include reconsidering what amounts to personal jurisdiction for digital defendants, creating a more effective framework for allowing victims to subpoena anonymous defendants, and redrafting the Communications Decency Acts to reduce the broad grant of immunity for ISPs and to implement a victim compensation fund. This Comment concludes that these changes need to be implemented before the upcoming mass adoption of VR so that the U.S. justice system can provide adequate redressability for the many Internet crimes that could occur in VR. These changes should supply VR users with the comfort of knowing that they will be backed by the legal system of the real world.

I. VIRTUAL REALITY: A WHOLE NEW WORLD

Virtual reality presents an entirely new world of human interaction and society. This Part starts by explaining the technology behind VR and the major players and developments in the industry. Next, this Part explains the applications of VR and the many psychological effects VR technology has on its users. Lastly, this Part explains why VR technology proposes unique problems for identity misappropriation.

A. VR Technology Background

VR immerses users into a virtual world by stimulating the user's senses to generate a sense of being present in a virtual environment.[12] In 2017, "[t]he global VR market was valued at $3.13 billion … and is expected to reach $49.7

[12] *Global Virtual Reality Market Size 2018*, REUTERS PLUS (July 2, 2018, 9:45 AM), https://www.reuters.com/brandfeatures/venture-capital/article?id=40919. This is primarily done through sight and sound technology that allows users to see and hear their virtual environment. Antoni Zolciak, *Augmented Reality & Virtual Reality Trends in 2018*, IN'SANELAB (July 8, 2018), https://insanelab.com/blog/vr-ar-mr/augmented-reality-virtual-reality-trends-2018. However, there is progress being made that will involve other senses in VR. For instance, Tokyo-based Vaqso Inc. has designed an odor-emitting attachment that can emit up to three different odors. *Id*. There is also FEELREAL's multisensory VR mask that intensifies the viewer's virtual reality presence using senses like heat, water mist, vibration, and wind. *Id*.

billion by 2023," with a growth rate of 58.54%.[13] The growing trend can be seen by user adoption. In 2014, there were less than one million users, but by 2020, there will be an estimated 82 million users.[14]

This growth is spurred by a number of factors, both technological and cultural. First, computing power has grown exponentially, effectuating real-time processing of giant amounts of data on small devices.[15] Additionally, major VR hardware companies have created head-mounted display (HMD) devices that contain all the necessary processing power within the headsets, allowing the user to roam free without having to connect to special (and expensive) gaming computers, which were required in earlier VR devices.[16] Lastly, from a cultural standpoint, millennials are key consumers of technology (specifically gaming) and will become more prominent in the market, driving consumption as they age.[17]

Due to the compact nature of a virtual reality HMD device, developers can provide fantastic resolution to produce an image well in excess of what people see with a ultra-high-definition television.[18] With perfect eye-tracking technology that works to seamlessly move the visual display in accordance with where the user is looking, VR headsets can simulate advanced motion sight.[19] Users also use advanced noise-cancelling audio headsets to fully immerse their auditory system into the virtual world.[20] The most popular HMDs are Facebook's Oculus Quest, the HTC Vive, and PlayStation VR.[21] While these

---

[13] *Global Virtual Reality Market*, *supra* note 12.

[14] Tricia Dempsey, *38+ Powerful Virtual Reality Statistics to Know in 2019*, G2 LEARNING HUB (April 25, 2019), https://learn.g2.com/virtual-reality-statistics

[15] Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051, 1058 (2018).

[16] Emory Craig, *No Surprise: Prices Fall, VR Headset Market Grows*, DIGITAL BODIES (Nov. 29, 2017), https://www.digitalbodies.net/virtual-reality/prices-fall-vr-headset-market-hits-new-highs.

[17] *See* Richard Fry, *Millennials Are the Largest Generation in the U.S. Labor Force*, PEW RES. CTR. (Apr. 11, 2018), http://www.pewresearch.org/fact-tank/2018/04/11/millennials-largest-generation-us-labor-force/.

[18] CHRISTOPH ANTHES ET AL., STATE OF THE ART OF VIRTUAL REALITY TECHNOLOGY 5–6, 13 (2016).

[19] *Id.* at 6.

[20] Some headphones are built into the HMD like Oculus Go, while other users can use separate headphones, like Audio-Technica ATH-M50x or Bose QuietComfort 35 II for an advanced listening experience. *See* Hugh Langley, *Best VR Headsets 2019*, WAREABLE (May 7, 2019), https://www.wareable.com/vr/best-vr-headsets-2017.

[21] *Id*. Oculus released the revolutionary Quest in 2020. Ian Hamilton, *More Oculus Quest Developers See Strong Sales Despte Curation Frustration*, UPLOAD (Sept. 9, 2019), https://uploadvr.com/oculus-quest-sales-strong/.

The Quest combines key attributes to a complete VR system-wireless design, virtual hand controllers, and full positional tracking. *Id.* The device also allows users to walk around for longer distances in VR (despite its name, VR mobility was limited on Quest's wired predecessor, the Oculus Go). *Id.* The Quest provides its users with wireless VR mobility with the computing power of a wired HMDs. *Id.*

technologies are designed to create state-of-the-art virtual experiences, with the proper attachment, any smartphone can be transformed into a workable form of VR for as little as $15.[22] Thus, there are currently over four billion smartphone owners with potential access to VR.[23]

Increases in haptic technology will allow users to *feel* what they are interacting with in their virtual environments. Haptic technology recreates the sense of touch by applying forces, vibrations, or motions on the user.[24] Today's gamers are familiar with the rumble packs found in game controllers that provide basic haptic feedback in the form of simple vibrations.[25] These vibration motors have been updated and integrated into VR haptic gloves to recreate textures, like NeuroDigital's Glove One and Manus VR.[26] Kinesthetic feedback, like the feeling of weight, inertia, or resistance, is harder to produce, and the technology is currently in its infancy.[27] Even still, these haptic gear companies have aspirations to create a full body suit that can apply similar forces and sensations to the entire body.[28] The full body suit will enable the user to get full sensory feeling of their virtual environment, from feeling a ball in the hands to feeling a fellow VR avatar's touch on one's skin.[29] This ability to feel will further enhance the sense of real within the virtual.

The development of today's VR technology can be compared to the first mass-produced automobile, the Model T, as the industry is just getting started. CPU processing power, bandwidth limitations, and full haptic body suits will be of magnitudes more powerful, faster, and cheaper.[30] As the technology becomes more advanced, the entire user experience will become more lifelike. Joel Breton

---

[22] GOOGLE CARDBOARD, https://vr.google.com/cardboard/get-cardboard/ (last visited Nov. 3, 2018).

[23] *See Ericsson Mobility Report*, ERICSSON (June 2019), https://www.ericsson.com/en/mobility-report.

[24] *Haptic*, TECHNOPEDIA, https://www.techopedia.com/definition/3637/haptic (last visited Nov. 11, 2019).

[25] *See* XBOX, https://www.xbox.com/en-US/xbox-one/accessories/controllers/xbox-black-wireless-controller (last visited Jan. 6, 2019).

[26] Edd Gent, *How Big Is the Gap Between* 'Ready Player One' *and Current VR Tech*, SINGULARITYHUB (Apr. 9, 2018), https://singularityhub.com/2018/04/09/how-close-are-we-to-ready-player-one-level-vr/#sm.00012dnhrt11p9dpvysvtgeuoe06q. For a description of the Glove One's haptic technology, see AVATAR VR, https://www.avatarvs.es (last visited Nov. 4, 2018).

[27] Gent, *supra* note 26 ("The SenseGlove and VRgluv both rely on bulky robotic exoskeletons powered by electronic motors to exert forces on a user's fingers, which allows them to recreate the size and stiffness of virtual objects."); *see also* SENSEGLOVE, https://www.senseglove.com (last visited Nov. 7, 2018); VRGLUV, https://vrgluv.com (last visited Nov. 7, 2018).

[28] Gent, *supra* note 26.

[29] *See* TESLASUIT, https://teslasuit.io/ (last visited Jan. 6, 2019).

[30] Heather Newman, 'Ready Player One' *Versus Reality: How Close Are We?*, FORBES (Mar. 31, 2018, 3:47 PM), https://www.forbes.com/sites/hnewman/2018/03/31/ready-player-one-versus-reality-how-close-are-we/#133768f82a01.

of VR content company Vive Studios states that the true VR experience will arrive when hardware companies can implement "full-haptic feedback, 64K resolution [nearly 60 times as many pixels as a standard high-definition television], … 8G bandwidth at consumer-friendly price points."[31]

All together, these technologies combine to create stimulated experiences for VR users and will allow users to digitally interact with each other on an unprecedented scale. Thus, companies across different industries are vying to incorporate VR into their business.

B. Application of VR

Currently, the most popular use of VR is within the gaming industry. It is likely that those who are not familiar with the current gaming market would be quick to discount the potential of VR because of its apparent roots in gaming. This would be a mistake.

First, the gaming industry is evolving at an outstanding rate.[32] Studies have shown that roughly 67% of Americans, or roughly 211 million people, play video games, and average twelve hours per week of play time.[33] In a recent ABC News survey, 97% of people ages twelve to seventeen reported playing video games (99% of all boys, 94% of all girls).[34] Further, gaming is increasingly becoming mainstream. ESports, a form of competitive video gaming, has exploded in popularity and is being broadcasted by ESPN and Turner.[35] In 2014, Amazon acquired Twitch, a live streaming video platform that allows gamers to share their screen with millions of people, for $970 million.[36] Market research

---

[31] *Id*. Breton predicts that these technologies will be made commercially available in seven to ten years. *Id*.

[32] *See* Tom Wijman, *Mobile Revenues Account for More Than 50% of the Global Games Market as It Reaches $137.9 Billion in 2018*, NEWZOO (Apr. 30, 2018), https://newzoo.com/insights/articles/global-games-market-reaches-137-9-billion-in-2018-mobile-games-take-half. The report forecasts that 2.3 billion gamers will spend $137.9 billion on games in 2018, growing at 13.3% from the year before. *Id.* Smartphones will account for $56.4 billion, console gaming generating $34.6 billion, and PC another $32.9 billion. *Id*.

[33] Brian Crecente, *Nearly 70% of Americans Play Video Games, Mostly on Smartphones (Study)*, VARIETY (Sept. 11, 2018), https://variety.com/2018/gaming/news/how-many-people-play-games-in-the-u-s-1202936332. In addition, 60% of Americans play video games daily. ENTM'T SOFTWARE ASS'N, 2018 SALES, DEMOGRAPHIC, AND USAGE DATA: ESSENTIAL FACTS ABOUT THE COMPUTER AND VIDEO GAME INDUSTRY 4 (2018).

[34] *Teens, Video Games and Civics*, PEW RES. CTR. (Sept. 16, 2008), https://https://www.pewinternet.org/2008/09/16/teens-video-games-and-civics/.

[35] *Why Competitive Video Gaming Will Soon Become a Billion Dollar Opportunity*, BUS. INSIDER (Mar. 15, 2017, 1:40 PM), https://www.businessinsider.com/esports-market-growth-ready-for-mainstream-2017-3.

[36] *Id*. In 2015, more people tuned into the watch the championships of the *League of Legends* (a popular video game) tournament than watched the last game of the NBA finals. David Segal, *Behind League of Legends*,

firm Newzoo values eSports at $138 billion in 2018 and expects it to grow at 22% annually.[37] These figures demonstrate the mainstream popularity of the industry, and the fact that younger generations that have grown up with video games will likely continue their consumption into adulthood.[38]

While it is clear that the growing popularity of gaming provides a solid baseline for VR consumption, the reach of VR is not confined to gaming. One of the more prominent uses of VR is in the medical industry. In 2017, the VR healthcare market was valued at $976 million and is expected to reach $5.1 billion by 2025.[39] Uses of medical VR include medical training and education,[40] as well as simulated surgeries.[41] Patient rehabilitation is also benefitting from VR. According to a 2017 study, patients who received VR therapy reported a 24% drop in pain scores, compared to other patients watching calming two-dimensional video who experienced just a 13.2% pain decrease.[42]

VR also has tremendous business and professional development implications. Innovative businesses are moving their headquarters to VR.[43] One

---

E-Sports's Main Attraction, N.Y. TIMES (Oct. 10, 2014), https://www.nytimes.com/2014/10/12/technology/riot-games-league-of-legends-main-attraction-esports.html. In September 2019, Activision hosted its Grand Finals for its *Overwatch* game and sold out the Barclays Center in Brooklyn. Shoshanna Delventhal, *Booming eSports Industry to Hit $138B in 2018*, INVESTOPEDIA, https://www.investopedia.com/news/booming-esports-industry-hit-138b-2018/(last updated Sept. 22, 2019).

[37] Delventhal, *supra* note 36.

[38] For an interesting article on the impact of video games on younger generations, see Daniel Raphael, *The Impact of Video Games on This Generation*, HUFFPOST (Nov. 7, 2013), https://www.huffingtonpost.com/daniel-raphael/the-impact-of-video-games_b_4227617.html.

[39] Jennifer Kite-Powell, *See How This Company Uses Virtual Reality to Change Patient Healthcare*, FORBES (Sept. 30, 2018, 11:06 AM), https://www.forbes.com/sites/jenniferhicks/2018/09/30/see-how-this-company-uses-virtual-reality-to-change-patient-healthcare/#2a7b4a2455ea.

[40] Rebecca Smith, *First Operation Streamed Live with Surgeon Wearing Google Glass*, TELEGRAPH (May 23, 2014), https://www.telegraph.co.uk/news/health/news/10851116/First-operation-streamed-live-with-surgeon-wearing-Google-glass.html (noting that in 2014, 13,000 medical students tuned in to watch the first cancer surgery broadcasted in augmented reality).

[41] Laura Mueller, *Virtual Reality Is the Future of Surgical Training*, CHI. HEALTH (Oct. 16, 2017), https://chicagohealthonline.com/virtual-reality-surgical-training/. "VR simulators can map individual patient's anatomical structures and recreate them … [so that] [s]urgeons can then virtually practice on these images," and, with the use of artificial intelligence, "mak[e] informed decisions on best practices." *Id*. Further, the surgeon can take unlimited risks on the simulations without fearing actual repercussions, which can lead to a more aggressive yet calculated surgery. *See id*.

[42] Soshea Leibler, *Cedars-Sinai Study Finds Virtual Reality Therapy Helps Decrease Pain in Hospitalized Patients*, CEDARS-SINAI (Mar. 29, 2017), https://www.cedars-sinai.org/newsroom/cedars-sinai-study-finds-virtual-reality-therapy-helps-decrease-pain-in-hospitalized-patients; *see also* Henry Lo et al., *Virtual Farm Game to Help Young Cancer Patients Deal with Treatment*, SIMON FRASER U. (May 19, 2016), https://www.sfu.ca/university-communications/media-releases/2016/virtual-farm-game-to-help-young-cancer-patients-deal-with-treatm.html (explaining that VR helps cancer patients cope with chemotherapy).

[43] Aaron Frank, *Inside a $1 Billion Real Estate Company Operating Entirely in VR*, SINGULARITYHUB (July 8, 2018), https://singularityhub.com/2018/07/08/inside-a-1-billion-real-estate-company-operating-entirely-in-

company, eXp Realty, is a billion-dollar publicly traded real estate brokerage company that operates its entire business in VR.[44] The company has been able to double their number of real estate agents in just seven months.[45] Company leaders attribute the growth in part to its VR campus.[46] The company's growth is unencumbered by geographical constraints because the company can hire whoever (and from wherever) they want since employees only need access to the Internet.[47] Additionally, businesses can now use VR video conferencing applications, such as Bigscreen, to engage in business meetings in VR, further evidencing VR's growing presence in the business world.[48]

Other commercial applications of VR include revolutionizing how consumers shop online through initiatives like Amazon's virtual kiosks,[49] conducting business meetings "face-to-face" in VR,[50] and virtual live music products, like NextVR, that allow fans to be on stage at a concert with their favorite artist.[51] Big businesses are already investing millions into visualization tools like VR to show off more products in less space.[52]

Due to the immaturity of the industry, more VR applications are certainly to be coming down the pike. The ever-expanding size and scope of applications for VR technology show that VR will become pervasive and will likely fundamentally change the way people interact with others.

---

vr/#sm.00012dnhrt11p9dpvysvtgeuoe06q.

[44] *Id*.

[45] *Id*.

[46] *Id*. Every employee, contractor, and thousands of agents show up team meetings, training seminars, and onboarding sessions all inside a virtual reality campus designed by California VR content company, VirBELA. *Id*. Scott Petronis, eXp Realty CTO, states that "[t]he virtual campus is a big part of our growth engine. If we were to have the constraints of a physical office, the growth we've had simply wouldn't be possible." *Id*.

[47] *Id.* ("The executive management team … operates business from remote corners of the US: the CEO is in Washington, the COO is in Scottsdale, Arizona … [and the CTO] is in upstate New York.").

[48] BIGSCREEN, https://bigscreenvr.com/about/ (last visited Jan. 2, 2019).

[49] Horwitz, *supra* note 1.

[50] Cat Zakrzewski, *Virtual Reality Takes on the Videoconference*, WALL ST. J. (Sept. 18, 2016; 10:06 PM), https://www.wsj.com/articles/virtual-reality-takes-on-the-videoconference-1474250761.

[51] NEXTVR, https://www.nextvr.com/live-nation (last visited Nov. 5, 2018).

[52] *See* Alice Bonasio, *Retailers Exploring New VR and AR Concepts to Drive Sales in 2019*, UPLOAD (Nov. 20, 2018), https://uploadvr.com/is-2019-the-year-of-v-commerce ("Amazon, IKEA, and Wayfair are all using these technologies to bring together the advantages of online shopping with brick and mortar retailing … . Macy's virtual reality furniture experience … allows people to design their own living spaces, populating [a scan of their living room] with items from Macy's catalog of products…."). Walmart, one of the leaders of commercial VR applications, uses VR to train its staff on a large variety of topics, to streamline its warehouse operations, and creating a virtual showroom for customers to try on clothing. *Id*.

C. VR's Effect on the User

To understand the potential impact of VR, it is necessary to note the psychological effects VR creates for its users. One concept, known as the Cone of Learning, describes the phenomena that humans learn and recall roughly 10–20% of what they hear and read, but retain approximately 90% of what they experience.[53] Thus, VR-driven experiences can create significant impressions on users. Hence, learning through VR, where users can simulate real life experiences, should be significantly more effective than the traditional textbook-based form of learning.[54]

In light of this, it is no surprise that VR has been proven to alter the real-life identities and perceptions of its users. Virtual embodiment is the idea that users quickly absorb their virtual bodies as their own.[55] This body ownership illusion produces astonishing changes in user's real-life attitudes, beliefs, and behaviors.[56] Consequently, there are major personality and perception changes from the user associating or aligning with their virtual identity.[57]

This has both positive and negative consequences. For example, taking on the body of Albert Einstein was shown to increase a person's cognitive task performance and was particularly effective for people with low self-esteem.[58] Additionally, VR users who used an avatar of a different race than their own reduced their unconscious racial bias.[59] Further, when adult participants inhabited the body of a small child, they began to self-identify with more child-

---

[53] Beverly Davis & Michele Summers, *Applying Dale's Cone of Experience to Increase Learning and Retention: A Study of Student Learning in a Foundational Leadership Course*, 6 QSCIENCE PROCEEDINGS 1, 2–4 (2015). This phenomenon can be attributed to the fact that people's visual system, while the richest sense, is extremely poor at collecting data. Stephen L. Macknik, *A Virtual Trick to Remove Racial Bias*, SCIENTIFIC AMERICAN (June 14, 2017), https://blogs.scientificamerican.com/illusion-chasers/a-virtual-trick-to-remove-racial-bias/. If you hold your thumb out at arm's length and focus on it, your visual field consists of about the size of your thumbnail, about 0.1% of your visual field. *Id.* Your eye must move to make up the difference, yet can only make an average of one to three movements per second. *Id.* Thus, when one wakes up in the morning, one only sees about 1% of the bedroom by the time one walks to the door. *Id.* As for the remaining 99%, the brain invents it, continuously and in real-time based on the person's previous models and presumptions about the world. *Id.*

[54] *See* CLASSVR, http://www.classvr.com/virtual-reality-in-education/ (last visited Jan 6. 2018).

[55] Aaron Frank, *How Virtual Reality Can Transform Who You Are*, SINGULARITYHUB (Nov. 1, 2018), https://singularityhub.com/2018/11/01/how-virtual-reality-can-transform-who-you-are/#sm.00012dnhrt11p9dpvysvtgeuoe06q.

[56] *Id*.

[57] *Id*.

[58] Domna Banakou et al., *Virtually Being Einstein Results in an Improvement in Cognitive Task Performance and a Decrease in Age Bias*, 9 FRONTIERS IN PSYCHOL. 1, 1 (2018), https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00917/full.

[59] Macknik, *supra* note 53.

like attributes than other participants in an adult body condition.[60] Experts also believe that VR can be used to decrease the number of violent incidents by giving users the perspective of a victim in a VR simulation, reasoning that identifying with the feeling of the victim will trigger empathy in potential aggressors.[61] On the other hand, it is unclear how taking on the body of the violent persona might impact the personality of the user.[62]

Nevertheless, across the many studies involving virtual embodiment, people consistently demonstrated a capacity to absorb their new identities instinctively and quickly.[63] Those new identities then had a powerful effect by immediately altering their perceptions about the real world.[64]

These studies beg the question: If one's identity and perception can be so malleable, what makes someone who they really are? More importantly, if VR identities can produce consistent and desirable results on people's actual identities and perceptions, then VR identities will quickly become more valuable (perhaps even commodity-like) and increase the incentive to steal the likeness of other "desirable" VR identities.

D. The Risk of Identity Misappropriation in the VR World

Aside from the mind-altering effects VR identities can produce on its users' actual identities, there are other reasons why VR poses significant risks to the identity protection of present and future VR users.

First, given the business and professional applications of VR, it is reasonable to expect (and studies have shown) that users would prefer to use their actual likeness for their avatars in these situations.[65] Further, users are going to want to present different appearances for different situations. For example, users on a VR job interview would likely prefer to use realistic identities to portray who

---

[60] Domna Banakou et al., *Illusory Ownership of a Virtual Child Body Causes Overestimation of Object Sizes and Implicit Attitude Changes*, 110 PROC. NAT'L ACAD. SCI. 12,846, 12,846 (2013).

[61] S. Seinfeld et al., *Offenders Become the Victim in Virtual Reality: Impact of Changing Perspective in Domestic Violence*, 8 SCI. REP. 1, 1 (2018), https://www.nature.com/articles/s41598-018-19987-7.

[62] Studies linked to existing non-immersive video games have proven that violent games produce violent behaviors. *See, e.g.*, Mike Snider, *Study Confirms Link Between Violent Video Games and Physical Aggression*, USA TODAY (Oct. 1, 2018), https://www.usatoday.com/story/tech/news/2018/10/01/violent-video-games-tie-physical-aggression-confirmed-study/1486188002/ ("[I]t is clear that violent video game play is associated with subsequent increases in physical aggression.").

[63] *See supra* notes 58–61 and accompanying text.

[64] *Id.*

[65] *See, e.g.*, Jennifer Wu, *Choosing My Avatar & the Psychology of Virtual Worlds: What Matters?*, 11 KALEIDOSCOPE 1, 1 (2014), (finding that persons had preferences for a "realistic female avatar in a job interview scenario," as opposed to other non-realistic avatars).

they really are in an effort make a professional impression on their interviewer.[66] Users can use machine learning and artificial intelligence to create realistic animations of their true likeness.[67] Thus, when cyber criminals infringe on these forms of avatars it will be an incredibly intimate form of identity infringement. This type of infringement will be far more intimate than the theft of a still image or a static fake Facebook profile. Rather, the identity will be a quasi-living identity that can interact with others.

Second, interactions will occur in real-time, hindering the user's ability to authenticate the true identity of avatars with whom they are interacting. Imagine that a user is standing in a virtual bar and is approached by an avatar.[68] This user will not have the time to analyze whether this approaching person really is who they claim to be. This fluid cyber engagement is unprecedented and gives fraudsters the ability to interact with millions of people, unencumbered by self-mitigating practices of the people they aim to defraud.[69]

Third, VR will also include a form of currency (probably a form of cryptocurrency) that can be exchanged in real time.[70] VRT World, a VR platform developer, is releasing a blockchain-based marketplace that will facilitate the VR economy by allowing users to exchange cryptocurrency.[71] This frictionless exchange of currency, while providing for a new area of growth for e-commerce,[72] will allow fraudulent actors to demand money from their victims instantaneously. The instant ability to cure the harm will incentivize the victim

---

[66] *Id.*

[67] For a company that specializes in creating life-like virtual avatars, see OBEN, https://www.oben.me (last visited Nov. 8, 2018). For a possible application of such technology, see Mike Scialom, *ObEN's PAI Avatar Impresses at Bradfield Health Event*, CAMBRIDGE INDEP. (Oct. 25, 2018), https://www.cambridgeindependent.co.uk/business/oben-s-pai-avatar-impresses-at-bradfield-healthcare-event-9050005/ (discussing the ways in which personalized artificial intelligence can be used in the healthcare sector).

[68] Now this can be a quasi-virtual bar like Revery: VR Bar which currently operates in Atlanta and supplies VR headsets for their patrons. REVERY: VR BAR, reveryvrbar.com (last visited Nov. 7, 2018). Or the bar could be a truly virtual bar where users independently enter the bar from their homes and interact with other VR bar hoppers. *See* Dean Takashi, *High Fidelity Takes Us Dancing in a Virtual Reality Club*, UPLOADVR (Feb. 21, 2018), https://uploadvr.com/high-fidelity-takes-us-dancing-virtual-reality-club/, for a reporter's description of his experience in such a VR bar.

[69] VR will also present users with incredible accessibility with one another by utilizing software applications like OpenSimulator. OPENSIMULATOR, http://opensimulator.org/wiki/Main_Page (last visited Oct. 12, 2018). Such applications will allow users to connect with multiple virtual environments over the Internet and virtually teleport from one world to another in seconds. *Id.*

[70] Snezhana Kazachenko, *Virtual Reality and Virtual Currency*, MEDIUM: WORLD VRT (Apr. 10, 2018), https://medium.com/vrtoken/virtual-reality-and-virtual-currency-7a20490205f.

[71] *Id.*

[72] For a discussion of the potential economic effects of VR, see Sonal Anand, *Virtual Reality in E-Commerce: Future Is Here*, MEDIUM: FRULIX (Apr. 20, 2018), https://medium.com/frulix/virtual-reality-in-e-commerce-future-is-here-a16683a00a62.

to quickly pay up to halt the misappropriation, rather than proceeding through the slow-moving legal system.[73] By the time an attorney could even draft the complaint, the infringer could defraud hundreds of users with the stolen identity. And, as shown with current cyber criminals, the first payment is usually never the only payment, as criminals often demand more when they realize the victim's willingness to pay. This phenomenon can be paralleled to ransomware, in which malicious computer software prevents users from accessing their system or personal data and demands payment to regain access.[74] Some victims of ransomware quickly pay to regain acess to their data with no guarantee that the criminal will not demand more.[75]

Most telling, identity theft of online identities is already occurring. Deepfakes are "manipulated videos, or other digital representations produced by sophisticated artificial intelligence, that yield fabricated images and sounds that appear real."[76] "Deepfakes can be the perfect weapon for purveyors of fake news" and could be used to harm the reputation of people by making the person appear to say or do something they never said or did.[77] In fact, Deepfakes have already been used to create fake messages with terrifying consequences. Some of which include a fake Barack Obama insulting Donald Trump,[78] a rather troubling video of a fake Ali Bongo, President of the country of Gabon, "confessing" his good health (despite documented health complications) which eventually started a military coup,[79] and a fake Amazon CEO Jeff Bezos announcing retirement which caused a stock decline.[80] Further, digital graphic designers are increasingly creating and selling avatars of real people on virtual marketplaces. Most of the reported uses for these avatars are sexual in nature and are allowing people to have sex with avatars of celebrities and ex-partners in VR without consent.[81] Without doubt, these alarming trends will continue,

---

[73] *See infra* notes 74–75 and accompanying text.

[74] *See* James A. Sherer, *Ransomware—Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 RICH. J.L. & TECH. 1, 1 (2017).

[75] *Id.* at 26–28.

[76] Grace Shao, *What 'Deepfakes' Are and How They May Be Dangerous*, CNBC (Oct. 13, 2019), https://www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html.

[77] *Id*.

[78] Kaylee Fagan, *A Viral Video that Appeared to Show Obama Calling Trump a 'Dips—-' Shows a Disturbing New Trend Called 'Deepfakes'*, BUSINESS INSIDER (Apr. 17, 2018), https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4.

[79] Ali Breland, *The Bizarre and Terrifying Case of the "Deepfake" Video that Helped Bring an African Nation to the Brink*, MOTHER JONES (Mar. 19, 2019), https://www.motherjones.com/politics/2019/03/deepfake-gabon-ali-bongo/.

[80] *Id*.

[81] *See* Samantha Cole & Emanuel Maiberg, *'They Can't Stop Us:' People are Having Sex With 3D Avatars of Their Exes and Celebrities*, VICE (Nov. 19, 2019), https://www.vice.com/en_us/article/j5yzpk/they-

and they attest to the current magnitude of identity misappropriation in current digital society.

In sum, VR offers real-time interaction that creates a powerful avenue for fraudsters to misappropriate the identities of millions of users. While the interactions occur in real-time and are extraordinarily realistic, the U.S. legal system will treat these interactions (and thus, crimes among them) no different than any other current computer interaction unless there is change. Treating these interactions as common computer interactions will vastly limit the ability of plaintiffs to seek redress due to the substantial procedural barriers that current Internet law creates.

II. SOURCES OF IDENTITY LAWS

As is apparent, the potential hazards in the virtual world are many and there must be a way for victims to find some recourse. Currently, the main avenue for victims of identity misappropriation to receive redressability is through identity protection laws, which this Part analyzes.

The particular source of identity protection available to a victim depends on the type of avatar deployed by the user. Avatars can take the shape of anything the user desires, which could range from a user's actual likeness, where the avatar is a carbon copy of the what the user looks like in real life,[82] to a fictitious three-headed dragon that shares no characteristics with the user's real identity.

The essential question is whether the avatar shares characteristics with the user's actual identity. If the avatar does not share any characteristics with the user, then it could be protected through trademark or copyright law, similar to any character like Mickey Mouse or Bugs Bunny.[83] However, if the avatar is akin to the identity of the user, then the user's likeness would be protected by the right of privacy and accompanying derivative privacy law rights, such as the right of publicity.[84] This Comment will focus on the latter form of avatar, where

---

cant-stop-us-people-are-having-sex-with-3d-avatars-of-their-exes-and-celebrities. The article found that users are using real features of real people (eyebrows, faces, penises, breasts, etc.) and created virtual avatars to have sex with in VR. *Id*. *See also* Christopher Cameron, *Pervy Trend Sees People Creating 3D Avatars of Celebs and Exes for VR Sex*, N.Y. POST (Nov. 20, 2019), https://nypost.com/2019/11/20/pervy-trend-sees-people-creating-3d-avatars-of-celebs-and-exes-for-vr-sex/.

[82] ObEN, *supra* note 67.

[83] Trademark and copyright law are already well-established in legal academia and are beyond the scope of this Comment. For an interesting read on issues at the intersection of trademark law, copyright law, and VR, see Sharon Lowry, *Property Rights in Virtual Reality: All's Fair in Life and Warcraft*, 15 TEX. WESLEYAN L. REV. 109 (2008).

[84] *See infra* Part II.A–B.

the user adopts his own image as his avatar. Given the business and professional applications of VR, it is entirely likely that users would want to use their real image when conducting business or meeting new people as something about "CEO Mickey" or some other animated character doesn't command the same respect that a CEO would prefer.[85]

The two laws that govern the unauthorized use of someone's name or likeness are the right of privacy and its derivative, the right of publicity.[86] However, these laws remain substantially incomplete and fail to provide adequate redress to the many victims of identity misappropriation.

A. The Right to Privacy

The right to privacy is central to protecting one's real world identity and is thus relevant to the VR world of the future. The right consists of the freedom from "unwarranted appropriation or exploitation of one's personality, the publicizing of one's private affairs … or the wrongful intrusion into one's private activities, in such a manner as to cause mental suffering, shame, or humiliation to a person of ordinary sensibilities."[87] The right to privacy that governs intrusions from private parties is a tort, whereas the right to privacy that governs intrusions from the government is constitutional.[88]

The origin of the right of privacy is found in a *Harvard Law Review* article written by Samuel Warren and Louis Brandeis, aptly titled *The Right to Privacy*.[89] Voicing their concern with the advent of "instantaneous photographs" and late-19th century newspaper enterprises invading the privacy of people, the authors argued that a legal right to privacy was not only desirable, but absolutely necessary to protect individuals from the dangers of mass media publication.[90] One cannot help but analogize the threat of photography and mass publication to privacy with the oncoming adoption of VR and its current threat to privacy.

---

[85] *See supra* note 65–66 and accompanying text.

[86] *See infra* Part II.A–B.

[87] R.T. Kimbrough, Annotation, *Right of Privacy*, 138 A.L.R 22, 25 (1942); *accord* R.T. Kimbrough, Annotation, *Right of Privacy*, 168 A.L.R 446, 448; W.E. Shipley, Annotation, *Right of Privacy*, 14 A.L.R.2d 750, 755 (1950).

[88] Rosenberg v. Martin, 478 F.2d 520, 524 (2d Cir. 1973) ("The constitutional right to privacy is not to be equated with the statutory right accorded by New York … and other states."); *infra* note 96 and accompanying text; *see, e.g.*, ERWIN CHEMERINSKY, CONSTITUTIONAL LAW, PRINCIPLES AND POLICIES 849–50 (5th ed. 2015) (discussing the constitutional right to privacy in the context of an individual's right to purchase and use contraceptives).

[89] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[90] *See id.* at 195–96 ("[W]hat is whispered in the closet shall [not] be claimed from the house-tops").

"The Warren and Brandeis article had a tremendous and lasting impact on the law."[91]

State adoption of the right of privacy soon followed. In response to a 1902 court denial of privacy rights,[92] "the New York legislature passed the first 'privacy' statute, forbidding the unpermitted use of name or likeness for advertising or trade purposes."[93] Similarly, in *Pavesich v. New England Life Ins. Co.*, the Supreme Court of Georgia enthusiastically adopted a right of privacy into its common law.[94] "[B]y the 1940s, … [m]ost of the courts accepting the *Pavesich* view emphasized that the right was … a 'personal tort' in the classic sense [with] 'damages … exclusively those of mental anguish.'"[95]

In his influential 1960 article, William Prosser divided the right of privacy into four torts: intrusion, disclosure, false light, and appropriation.[96] Intrusion and disclosure do not pertain to identity misappropriation in VR and are beyond the scope of this Comment—even though they have significant VR consequences elsewhere.[97] However, false light and, to a greater extent, appropriation strike at the issue of identity misappropriation in VR.

False light, or injurious falsehood, occurs when a defendant publicly presents the plaintiff in a "false light."[98] This can occur when a "defendant publicly and falsely attributes to [the] plaintiff some [controversial] opinion or statement."[99] A circumstance that could occur in VR is when an avatar is depicted to support a controversial issue, such as drug use, prostitution, or racism. Thus, if a VR identity thief steals an avatar and associates that avatar with controversial or offensive behavior, the thief would be conducting the tort

---

[91] J. THOMAS MCCARTHY, 1 THE RIGHTS OF PUBLICITY AND PRIVACY, § 1:14 (2016). "Over 100 years after its publication, the California Supreme Court … commenced its opinion about privacy rights by citing" the article. *Id.* (citing Shulman v. Group W Productions, Inc., 955 P.2d 469, 473 (Cal. 1998)).

[92] Roberson v. Rochester Folding Box Co. 64 N.E. 442, (N.Y. 1902).

[93] MCCARTHY, supra note 91, § 1:15.

[94] Pavesich v. New England Life Ins. Co., 50 S.E. 68, 71 (Ga. 1905); MCCARTHY, *supra* note 91, § 1:17.

[95] MCCARTHY, *supra* note 91, § 1.18 (quoting Eick v. Perk Dog Food Co., 106 N.E.2d 742, 756 (Ill. App. Ct. 1952)).

[96] William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). "The tremendous impact of Prosser's" classification is tellingly shown by the fact that the *Restatement (Second) of Torts* adopts, in whole, the four parts "as an accurate restatement of the law." MCCARTHY, *supra* note 91, § 1.24 (citing RESTATEMENT (SECOND) OF TORTS, § 652A–652I (AM. LAW. INST. 1977)). The *Restatement* presents Prosser's four torts in an order different from the one Prosser employed, listing them as follows: intrusion, appropriation, disclosure and false light. RESTATEMENT (SECOND) OF TORTS, § 652A.

[97] *See* Lemley & Volokh, *supra* note 15, at 1080 (noting that VR will present hackers with opportunities to spy on users in both private and public affairs, pertaining to the tort of intrusion).

[98] Prosser, *supra* note 95, at 398.

[99] MCCARTHY, *supra* note 91, § 1:22.

of false light. The damages associated with false light pertain to the mental suffering of the plaintiff rather than the injury to his reputation.[100] However, if the identity thief does not engage in such controversial behavior with the stolen identity, the thief will not be subject to false light.[101] Accordingly, victims of VR identity theft whose avatars are not associated with controversial behavior cannot sue under false light.

Invasion of privacy by appropriation usually involves a person's "unpermitted use of a plaintiff's identity … with damage to the plaintiff's dignitary interests and peace of mind."[102] "Although in most cases, the infringer makes a commercial use of the plaintiff's identity, in some cases, a non-commercial use, such as forgery of plaintiff's name, will also constitute the tort of invasion of privacy by appropriation."[103] This type of privacy protection was the immediate historical precursor to the right of publicity which focuses on economic interests associated with one's identity (discussed in detail below).[104] Essentially, the tort of appropriation compensates plaintiffs for their mental suffering caused by the unauthorized use of their identity, but only if the infringer used the identity to their advantage.[105] Everyone can assert the action of invasion of privacy by appropriation, as damages are calculated on the mental suffering resulting from the defendant's use (rather on the commercial value of their identity).[106]

Thus, victims that are unaware of the unauthorized use of their identity or those who cannot experience the requisite mental suffering (like children and mentally handicapped) are unable to assert this claim and seek redress.[107] Additionally, if the infringer does not use the stolen identity or does not use the identity to his advantage (e.g., storing for future use), then the victim cannot assert invasion of privacy by appropriation.[108] These shortcomings become important in VR, as users that are unaware of the infringer's fraud or users with

---

100 *Id.*

101 *See, e.g.*, Welling v. Weinfeld, 866 N.E.2d 1051 (Ohio 2007) (adopting the tort of false light and recognizing that the tort would not occur if one did not give "publicity to a matter concerning another that places the other before the public in a false light").

102 MCCARTHY, *supra* note 91, § 1:23.

103 *Id.* § 5:62.

104 *Id.* § 1:23.

105 *Id.*

106 *Id.*

107 *See, e.g.*, Slocum v. Sears Roebuck & Co., 542 So.2d 777, 779 (La. Ct. App. 1989). A baby's photo was used without permission in an advertisement. *Id.* at 778. The privacy claim was dismissed because the baby suffered no actual damage. *Id.* at 779.

108 MCCARTHY, *supra* note 91, § 1:23.

unused stolen identities will not be able to recover under this tort, despite injuries they might be suffering.

B. The Right of Publicity

To address the shortcomings of false light and misappropriation privacy laws, in the mid-twentieth century courts began to use a new source of identity protection called the right of publicity.[109] The right of publicity developed from the invasion of privacy by appropriation tort, "which focused on the indignity and mental trauma incurred when one's identity was widely disseminated in an unpermitted commercial use."[110] But, "[w]hen celebrities began to claim invasion of privacy by misappropriation, … many courts rejected the [argument that] use of the celebrity's identity was an invasion of privacy [because] the plaintiff, by virtue of his celebrity, was already well known" and in the public domain.[111] The "privacy" label, in the sense of a right to be "left alone," seemed to run counter to the fact that famous people, who have voluntarily sacrificed their right of privacy in exchange for fame, are enforcing their privacy rights on the theory that they want to be "left alone."[112]

To counter this hurdle, courts established the right of publicity as a property right "to protect the commercial value of celebrities' identities, rather than their privacy interest[s]".[113] While privacy rights protect against any mental distress that accompanies undesired publicity, "the right to publicity protects pecuniary, not emotional, interests."[114]

---

[109] *Id.* § 1.4.

[110] Alicia M. Hunt, *Everyone Wants to Be a Star: Extensive Publicity Rights for Noncelebrities Unduly Restrict Commercial Speech*, 95 NW. U. L. REV. 1605, 1606 (2001) (quoting MCCARTHY, *supra* note 91, §§ 4:14–4:20).

[111] *Id.*

[112] *Id.* at 1605–06.

[113] *Id.* at 1605. In 1953, Judge Jerome Frank of the U.S. Court of Appeals for the Second Circuit "was … the first to coin the term 'right of publicity.'" MCCARTHY, *supra* note 91, § 1:26. He "used [the term] to denote a property right in a person's identity … [which] is infringed by the unpermitted use of a person's identity in a commercial setting, … capable of being assigned and licensed." *Id*. *See also* Haelen Labs., Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953) ("[W]e think that in addition to and independent that of [the] right of privacy (which New York derives from statute), a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture … [f]or it is common knowledge that many prominent persons … would feel sorely deprived if they no longer received money for authorizing advertisements, popularizing their countenances, displayed in newspapers, magazines, buses, trains and subways.").

[114] Ventura v. Titan Sports, Inc., 65 F.3d 725, 730 (8th Cir. 1995) ("[T]he right of publicity differs substantially from the right to privacy.").

"The right of publicity is a state law created intellectual property right."[115] "While it bears some family resemblances to… [other areas of intellectual property rights]… the right of publicity has its own unique legal dimensions" and justifications.[116]

To prevail on a prima facie case for liability of infringement of the right of publicity, a plaintiff must prove validity and infringement.[117] That is, that the "[p]laintiff owns an enforceable right in [their] identity" and the defendant infringed on that right by using the identity to their benefit.[118] However, the threshold for what constitutes a benefit to the defendant differs among jurisdictions.[119] Some jurisdictions require that a plaintiff must show that the defendant has made money of the use of the plaintiff's likeness.[120] Other jurisdictions require only a tangible benefit, irrespective of any monetary benefit.[121] The remedy for infringement can be an injunction or damages.[122]

Unfortunately, not everyone can bring an action under the right of publicity. The right of publicity was created for celebrities to collect on the commercial value of their identity, and thus, it is well established that celebrities can seek enforcement for infringements of this right.[123] And understandably so—celebrity endorsements have frequently been used by marketers to effectively advertise their products and celebrities should be able to recover the economic value associated with their name.[124] However, courts have split on the issue of

---

115 MCCARTHY, *supra* note 91, § 3:1.

116 *Id.*

117 *Id.* § 3:2.

118 *Id.*

119 *See* Henley v. Dillard Dep't Stores, 46 F. Supp. 2d 587, 597 (N.D. Tex. 1999) ("[T]he plaintiff in a right to publicity action is not required to show that the defendant made money off the commercial use of the name or likeness … [Defendant] should be held liable because it received a benefit by getting use a celebrity's name for free in its advertising. Whether or not the advertisement worked … is wholly irrelevant."); *infra* notes 120–21 and accompanying text.

120 *See* Haelen Labs v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953); Palmer v. Schonhorn Enter., Inc., 232 A.2d 458, 462 (N.J. Super. Ct. Ch. Div. 1967) ("[A]lthough the publication of biographical data of a well-known figure does not per se constitute an invasion of privacy, the use of that same data for the purpose of capitalizing upon the name … in connection with a commercial project other than the dissemination of news or articles or biographies does.").

121 Newton v. Thomason, 22 F.3d 1455, 1460 n.4 (9th Cir. 2005) (defining the right of publicity as an "appropriation of plaintiff's name or likeness to defendant's advantage, commercially or *otherwise*" (emphasis added)).

122 Thomas Phillip Boggess, *Cause of Action for an Infringement of the Right of Publicity*, *in* 31 CAUSES OF ACTION, 121, 124 (Clark Kimball & Mark Pickering eds., 2006).

123 *See supra* note 110 and accompanying text.

124 *See* Michael E. Jones, *Celebrity Endorsements: A Case for Alarm and Concern for the Future*, 15 NEW ENG. L. REV. 521, 525 (1980) (showing endorsement makes larger impression on target audience). In *Fraley v. Facebook, Inc.*, Facebook CEO Mark Zuckerberg stated that "[a] trusted referral influences people more than

whether non-celebrities should be able to recover under the right of publicity.[125] The majority view is that the right of publicity should extend to everyone, and the less famous the plaintiff, the fewer the commercial damages.[126] The minority view, in contrast, is that the right is solely a celebrity's right, and non-celebrities should not be able to recover unless they demonstrate a significant commercial value of their identity.[127]

Critics of the minority view argue that the right of publicity should not draw a critical line between "celebrities" and "non-celebrities" as the distinction is too ephemeral—after all, "[o]ne person's celebrity is another person's 'who's that?'"[128] Further, defamation law has shown us that defining fame is incredibly challenging.[129] Instead, critics of the minority position argue that celebrity status should only be factored into the economic value calculation of the plaintiff's identity.[130] Nevertheless, this split creates barriers for "regular joe" VR identity misappropriation victims that are not celebrities and cannot assert false light or invasion of privacy by misappropriation due to the specific facts of their case.[131]

---

the best broadcast message. A trusted referral is the Holy Grail of advertising." 830 F. Supp. 2d 785, 799 (N.D. Cal. 2011).

[125] *See* Alicia M. Hunt, Comment, *Everyone Wants to Be A Star: Extensive Publicity Rights for Noncelebrities Unduly Restrict Commercial Speech*, 95 NW. U. L. REV. 1605, 1658 (2001) ("The view adopted by the minority of states is that the right of publicity should only apply to individuals who can show value in identity….").

[126] *See*, *e.g.*, Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 825 (9th Cir. 1974) ("We conclude that the California appellate courts would … afford legal protection to an individual's proprietary interest in his own identity."); Tellado v. Time-Life Books, Inc., 643 F. Supp. 904, 909 (D.N.J. 1986) ("I do not find that New Jersey law limits the cause of action of misappropriation to famous individuals."); Dora v. Frontline Video, Inc., 18 Cal. Rptr. 2d 790, 792 n.2 (Ct. App. 1993) ("There is a split of opinion among jurisdictions as to whether a "non-celebrity" should have the right to sue for the commercial value of unpermitted use of personal identity.").

[127] Martin Luther King, Jr. Ctr. for Soc. Change, Inc. v. Am. Heritage Prods., Inc., 296 S.E.2d 697, 703 (Ga. 1982) (concluding that the right of publicity extends only to celebrities, while the right of privacy extends to everyone).

[128] MCCARTHY, *supra* note 91, §4:2.

[129] *Id.*; *see*, *e.g.*, Wolston v. Reader's Digest Ass'n, Inc., 443 U.S. 157, 164–65, 168 (1979) (categorizing fame between "all purposes" public figures who achieve pervasive fame and "limited purpose" public figures who qualify for only a "limited range of issues")*; see also* Rosanova v. Playboy Enters., Inc., 411 F. Supp. 440, 443 (S.D. Ga. 1976) (defining a public figure is "like trying to nail a jellyfish to the wall").

[130] Motschenbacher, 498 F.2d at 824–25 n.11 ("Generally, the greater the fame or notoriety of the identity appropriated, the greater will be the extent of the economic injury suffered. However, it is quite possible that the appropriation of the identity of a celebrity may induce humiliation, embarrassment and mental distress, while the appropriation of the identity of a relatively unknown person may result in economic injury or may itself create economic value in what was previously valueless.").

[131] These plaintiffs may not be able to assert those rights due to lack of appreciation of the misappropriation or from lack of use from the infringer.

"Under by either statute or common law, the right of publicity is recognized as the law of thirty-three states."[132] Although the right may be recognized in a slight majority of states, it has been treated differently throughout them.[133] Along with differing on whether the right should extend to non-celebrities, states also differ on whether the right is transferable or descendible.[134] Also, states are inconsistent in applying remedies.[135] Depending on the state, remedies in a right of publicity action can include preliminary injunction, injunction, pecuniary and nonpecuniary damages, punitive damages, and attorney's costs and fees.[136]

This nationwide disparity of the right of publicity and the varying approaches to the right has led to calls by both academics and practitioners for a federal statute to unify protections nationwide.[137] The Intellectual Property Law Section (IPLS) of the American Bar Association is drafting a proposed federal right of publicity statute that would classify the right as a property right that would extend to all individuals, regardless of whether their identity has a demonstrable commercial value.[138] The IPLS proposes allowing for a statutory damages ($500) for individuals that cannot prove commercial value in their name.[139] Additionally, the International Trademark Association has called for an

---

[132] MCCARTHY, *supra* note 91, §6:2. These states are "Alabama, Arizona, Arkansas, California, Connecticut, Indiana, Florida, Georgia, Hawaii, Illinois, Kentucky, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee Texas, Utah, Virginia, Washington, West Virginia and Wisconsin." *Id.*

[133] *See generally* Eric J. Goodman, *A National Identity Crisis: The Need for a Federal Right of Publicity Statute*, 9 DEPAUL-LCA J. ART. & ENT. L. & POL'Y 227, 257–64 (1999) (describing variations among the states on the right of publicity, the duration of the right after death, and remedies for violations of publicity rights).

[134] *Id*. *Compare* Hillerich & Bradsby Co. v. Christian Bros., Inc., 943 F. Supp. 1136, 1142 (D. Minn. 1996) (granting an injunction after conducting a balancing test due to the use of plaintiff's likeness without permission), *with* Weinstein Design Group, Inc. v. Fielder, 884 So. 2d 990, 1003 (Fla. Dist. Ct. App. 2004) (remanding for a new trial in favor of a company that used plaintiff's likeness without permission after examining precedent and statutes).

[135] Goodman, *supra* note 133, at 261–64.

[136] *Id*. at 261–62.

[137] *See* A.B.A. SECTION OF INTELL. PROP. L., 1999-2000 ANNUAL REPORT 108–10 (Mark K. Dickson & James A. Forstner eds., 2000); J. Eugene Salmon, Jr., Note, *The Right of Publicity Run Riot: The Case for a Federal Statute*, 60 S. CAL. L. REV. 1179, 1179 (1987) (exploring the current incongruent state regulatory regimes and proposing a new uniform federal statute).

[138] A.B.A. SECTION OF INTELL. PROP. L., *supra* note 137, at 109 ("The rights under this Act are property rights that are freely transferable in whole or in part to any person either by written transfer…." The Section's proposed statute is in working-draft form and has not yet been formally proposed or adopted by the ABA.).

[139] Kevin L. Vick & Jean Paul-Jassey, *Why a Federal Right of Publicity Is Necessary*, 28 COMMC'NS LAWYER 14, 19 (2011) ("The federal right of publicity statute should provide for statutory damages that permit an individual to vindicate his rights and dignity in the absence of demonstrable economic damages. But statutory damages should be modest, for example, $500….").

amendment to the Lanham Act to further codify and formally establish the right of publicity.[140]

Nevertheless, these calls for federal unity for the right of publicity are just that—calls. And currently, there are many gaps in identity protections for Americans nationwide. With different approaches to standing and remedies, many people will enter the VR world unprotected from the oncoming threat of identity misappropriation that VR will certainly pose. Until these inconsistences are resolved, many VR users will refuse to use their real name and likeness out of fear of theft without recourse, which will stifle the idealized concept of VR society.

III. INTERNET LAW'S IMPACT ON IDENTITY PROTECTION

It may seem incredible that even after twenty years of mass communication through the Internet and roughly twenty years of social media, these substantive legal inconsistencies are still prevalent. This is especially true in light of the increase in identity theft over the same period.[141] Nevertheless, the substantive laws concerning identity protection remain wholly inadequate, fragmented, and incomplete. The reason for this lies in significant part with dated Internet laws that have produced substantial procedural barriers that prevent Internet disputes from getting into the courthouse and, thus, prevent precedent from forming and identity protection laws from evolving.

VR will take place on the Internet, which means that VR identity misappropriation disputes will touch on Internet law. Internet law has created many procedural wrinkles that make an already complicated problem more complicated. These procedural hurdles have substantially limited victims' ability to even get their claim into the courthouse, which explains why the substantive identity protection laws discussed in Part II remain so inconsistent. First, decentralized Internet servers, and cyber interactions among them, have forced courts to reconsider what amounts to personal jurisdiction, making regulation and enforcement difficult.[142] Second, strict John Doe subpoena standards grant too much protection to the online anonymity of defendants and make it extremely difficult, if not impossible, to identify online cyber-criminals.[143] Third, Section 230 of the Communications Decency Act grants

---

[140] *See* INT'L TRADEMARK ASS'N, BD. RESOLUTIONS: U.S. FED. RIGHT OF PUBLICITY (1998).

[141] Shareen Irshad & Tariq Rahim Soomro, *Identity Theft and Social Media*, INT'L J. OF COMPUT. SCI. & NETWORK SEC. 43, 43 (2018).

[142] *See* Lewicki, *infra* note 150.

[143] *See* Miller, *infra* note 174.

broad immunity to ISPs which further limits plaintiff's ability to seek compensation and effectively disincentivizes ISPs to regulate their own products.[144]

This Part will explain these procedural hurdles caused by Internet law. First, Section A explains the Internet's effect on personal jurisdiction law and what amounts to digital minimum contacts. Second, Section B explains the five different John Doe subpoena standards for anonymous cyber defendants and the challenges it presents for victims of VR identity misappropriation. Lastly, Section C analyzes the Communications Decency Act's broad grant of immunity for ISPs and its relationship to identity misappropriation.

A. Internet and Personal Jurisdiction: Digital Minimum Contacts

The Internet has brought new concerns to personal jurisdiction. Because the Internet lacks any central location, the notion that a particular forum can seize authority over an Internet transaction seems peculiar. This is troublesome for VR identity misappropriation victims who wish to bring an action against their perpetrator.

To find personal jurisdiction, courts start with a state's long arm statute, which determines whether a state court has personal jurisdiction over a non-resident defendant.[145] If personal jurisdiction is proper under the state's long-arm statute, courts then determine whether the exercise of personal jurisdiction would satisfy "fair play and substantial justice" required by constitutional due process.[146] At the core of this determination is the question of whether the defendant has minimum contacts with that state that would lead the defendant to "reasonably anticipate" being summoned to a court in that state.[147]

There are two types of personal jurisdiction: general and specific.[148] Irrespective of the dispute or controversy, a court will always have general jurisdiction over a defendant at their domicile (on the rationale that the defendant has "continuous and systemic" contacts with that forum).[149] In the context of an

---

144 *See* H.R. REP. No. 104-458, at 194 (1996) (Conf. Rep.).

145 *See* World-Wide Volkswagen Corp. v. Woodsen, 444 U.S. 286, 289–90 (1980).

146 *Id*. at 292 (quoting Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)).

147 *Id*. at 297*; see also* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 470 (1985) (describing the lower court's evaluation of "reasonable notice").

148 *See Burger King Corp*., 471 U.S. at 473 n.15.

149 *Int'l Shoe Co.*, 326 U.S. at 317. For a corporation, the place of residence is their state of incorporation and state of their principal place of business (usually the headquarters). Daimler AG v. Bauman, 571 U.S. 117, 137 (2014). The headquarters is the "nerve-center" or where the corporation's officers, "direct, control, and coordinate the corporation's activities." Hertz. Corp. v. Friend, 599 U.S. 77, 92–93 (2010).

Internet dispute, courts have limited general jurisdiction only to the defendant's domicile because allowing the computer interaction via the Internet to be defined as "continuous and systematic contacts" would render personal jurisdiction obsolete (as the Internet consists of millions of cyber connections per second).[150]

On the other hand, "specific jurisdiction permits a court to exercise jurisdiction when the cause of action arises directly from the defendant's contacts with the forum state."[151] These contacts must reach a certain minimum threshold, or "minimum contacts," to satisfy personal jurisdiction.[152] While courts have yet to provide a definitive answer as to what level of Internet contacts would be sufficient to establish minimum contacts for purposes of specific jurisdiction,[153] they have identified three levels, or types, of Internet contacts for a court to reference when determining if minimum contacts, and therefore specific personal jurisdiction, exists.[154]

The first level of Internet contact recognized by the courts occurs when a defendant clearly does business over the Internet, sometimes called an "active website."[155] "An active website is one where the parties can interact back and forth, make purchases, enter into contracts, and conduct other activities that involve the participation of both parties."[156] The seminal case involving active websites and personal jurisdiction is *CompuServe, Inc. v. Patterson*.[157] The court found that the defendant operated an active website, and was therefore subject to personal jurisdiction because the website had contracts with various individuals and could reasonably anticipate litigation in the states in which they

---

[150] Lora J. Lewicki, Note, *Internet Jurisdiction and Minimum Contacts*, 76 N. D. L. REV. 911, 918–19 (2001) (quoting Millennium Enters., Inc. v. Millennium Music, LP, 33 F. Supp. 2d 907, 910 (D. Or. 1999)).

[151] *Id*. *See also Int'l Shoe Co.*, 326 U.S. at 316. A court may exercise specific jurisdiction over a party when that party has "minimum contacts" with the state or forum where the cause of action took place. *Id*.

[152] *Id*.

[153] Lewicki, *supra* note 150, at 918.

[154] *Id*. at 922.

[155] *Id*.; *see also* CompuServ, Inc. v. Patterson, 89 F.3d 1257, 1264 (6th Cir. 1996) (explaining that a company can do business in a state without being "physically present in the forum"); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) ("At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper.").

[156] *See Compuserv*, 89 F.3d at 1263–65 (concluding that entering into contracts and emailing is evidence of the plaintiff making "a connection" with a different state).

[157] Lewicki, *supra* note 150, at 922.

contracted with.[158] Thus, active sites generally are subject to personal jurisdiction in every forum they conduct business in.[159]

The second level of Internet contacts, called passive websites, occurs when a user-plaintiff in the forum state exchanges information with the defendant through the defendant's website.[160] In these instances, jurisdiction is determined by assessing the level of interactivity between the defendant and user-plaintiff and the commercial nature of the exchange that occurs through the website.[161] While a minority of courts find that merely advertising over the Internet is enough to assert jurisdiction,[162] later decisions have declined this reasoning because such reasoning subjects these websites to nationwide service of process.[163]

The third level of Internet contact occurs when a website is not necessarily conducting business but functions as more than a mere information bank.[164] These sites are called "intermediate websites."[165] Most websites fall into this category. And, it is likely that VR fits this definition—as plaintiffs and defendants are both users on a common VR application.[166]

Courts have used broad discretion to determine on a case-by-case basis whether the level of interactivity and commercial nature of the information is such that the exercise of personal jurisdiction is warranted.[167] Finding the level of interactivity is difficult because there often are not enough contacts between

---

158 *Compuserv*, 89 F.3d at 1264–65 ("There can be no doubt that Patterson purposefully transacted business in Ohio.").

159 *Id.*; Lewicki, *supra* note 150, at 922 ("In cases dealing with active web sites, the court will usually find that there is personal jurisdiction if the Internet activity involves doing business over the Internet."); *see Compuserv*, 89 F.3d at 1266–67 (holding that purposefully availing oneself "of the privilege of doing business" in a state subjects a company to personal jurisdiction in that state); *see also* Maritz Inc. v Cybergold, 947 F. Supp. 1328, 1333 (E.D. Mo. 1996) (holding that a website that allows people to sign up for a mailing list has an "intent to reach all internet users" and therefore qualifies as a business subject to personal jurisdiction in a foreign state).

160 Lewicki, *supra* note 150, at 930 ("Passive web sites, at the other end of the sliding scale, are sites that serve as mere advertisements or simply provide information.").

161 *Id*. at 930–36 (discussing how courts have decided passive websites cases).

162 *See* TELCO Commc'ns v. An Apple A Day, 977 F. Supp. 404, 408 (E.D. Va. 1997) (holding that putting a press release online is enough to assert personal jurisdiction in any state it caused harm).

163 *See* Barrett v. Catacombs Press, 44 F. Supp. 2d 717, 725 (E.D. Pa. 1999) ("Another line of cases has rejected the holding that advertisement Web sites are merely passive.").

164 PurCo Fleet Servs., Inc. v. Towers, 38 F. Supp. 2d 1320, 1324–25 (D. Utah 1999) (explaining that the company used its website to solicit business outside the state); *see also Barrett*, 44 F. Supp. 2d at 726–27 (describing the third category as "difficult to classify").

165 Lewicki, *supra* note 150, at 936.

166 *See id.*

167 *See id.* ("In this category, there are often other factors considered by the court in order to determine whether or not there is jurisdiction.").

the defendant and the particular forum in question.[168] For this, courts will look to non-Internet factors (such as travel, telephone, or mail contacts) made to that forum to determine whether the defendant could have reasonably anticipated being summoned in the forum.[169] Generally, absent a non-Internet contact with the forum, jurisdiction will not exist because exercising jurisdiction over these types of websites would create nationwide jurisdiction for any individual or business that uses the website.[170]

This is problematic because VR identity infringers typically do not avail themselves to the forum of their victim. They likely do not know who the actual person is behind the avatar they steal, let alone where that person resides. Thus, it is virtually impossible for Internet defendants to prove the requisite amount of non-Internet contacts needed to avail themselves to the plaintiff's forum—making enforcement and redressability impracticable.

Because of this extreme difficulty with suing Internet defendant in the plaintiff's forum, plaintiffs are left with suing in the defendant's resident state. However, this is extremely difficult given our legal system's strong preference for protecting the anonymity of Internet users.

B. Anonymity of Users

Authors have a First Amendment right to remain anonymous.[171] The Supreme Court extended this right of anonymity to online speech.[172] The Court found that while the broadcast industry presents consumers with unabated content and thus the producer of the content should be identified (like a TV program or commercial), Internet users do not usually encounter content "by accident" and normally must perform an affirmative action to be exposed to indecent content (like entering a website or opening a program).[173] For these constitutional considerations, courts have been careful in compelling ISPs to unmask the identity of their users.[174] This judicial caution has led to inconsistent

---

168 *Id*. ("These types of cases are often more difficult to classify….").

169 *Barrett*, 44 F. Supp. 2d at 726–27 ("By examining the current case law on the Internet, we find that many courts have exercised personal jurisdiction when a defendant has posted a Web page and participated in other non-Internet related contact with the forum.").

170 *Id*. at 727.

171 McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (holding that a state law prohibition against the distribution of anonymous campaign literature violated First Amendment). The Court further stated that "[a]nonymity … provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent." *Id*.

172 Reno v. ACLU, 521 U.S. 844, 868 (1997).

173 *Id*. at 869 (quoting the lower court's decision, ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

174 *See* Jason C. Miller, *Who's Exposing John Doe? Distinguishing Between Public and Private Figure*

standards for issuing John Doe subpoenas that require the ISP to reveal the identity of an anonymous poster.[175]

Under the Federal Rules of Civil Procedure, a plaintiff must identify a defendant before they can proceed with a suit.[176] However, when the defendant is an anonymous computer user (John Doe), this requirement is nearly impossible to meet as written. For this, plaintiffs must file an ex parte motion seeking a subpoena to compel the ISP to disclose the defendant's identity.[177] This motion is necessary because an ISP cannot disclose a user's identity without a court order, as prescribed by Section 47 of the Telecommunications Act.[178] If the plaintiff fails to identify and serve the John Doe within ninety days of the commencement of the action, the anonymous defendant will be dismissed.[179]

The subpoena process is grueling. A plaintiff who wishes to subpoena an anonymous user must first submit an order to the court to show cause for unmasking the defendant.[180] Then, assuming no pushback from the ISP (ISPs frequently fight these subpoenas), the ISP will inform the defendant of the subpoena and their right to fight the order anonymously.[181] "Eventually, a hearing will be held to determine whether the identity of a particular defendant must be disclosed so that the discovery process can proceed."[182]

There are five prevailing standards for assessing whether an anonymous defendant's identity should be disclosed by the ISP. The first and second standards are relatively plaintiff-friendly as they are easier to satisfy than the other standards. The third, fourth, and fifth standards are defendant-friendly and

---

Plaintiffs in Subpoenas and ISPs in Anonymous Online Defamation Suits, 13 J. TECH. L. & POL'Y 299, 245–46 (2008) (describing the procedural difficulties in unveiling anonymous website contributors).

175 *Id*. at 245 (describing differences in notice requirements); *see also* Ryan M. Martin, *Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits*, 75 U. CIN. L. REV. 1217, 1227 (2007).

176 FED. R. CIV. P. 4(m) ("If a defendant is not served within 90 days after the complaint is filed, the court—on motion or on its own after notice to the plaintiff—must dismiss the action without prejudice against that defendant or order that service be made within a specified time.").

177 *See, e.g.*, McMann v. Doe, 460 F. Supp. 2d 259, 262–63 (D. Mass. 2006).

178 47 U.S.C. § 551(c)(2)(B) (2012).

179 Redd v. Dougherty, 578 F. Supp. 2d 1042, 1049 (N.D. Ill. 2008) ("More than 120 days have passed since the filing of the Plaintiff's complaint…. Accordingly, these defendants are dismissed without prejudice…."); Church of Universal Love and Music v. Fayette College, 892 F. Supp. 2d 736, 748–49 (W.D. Pa. 2012) ("[U]se of John Doe defendants is permissible in certain situations until reasonable discovery permits the true defendants to be identified… If reasonable discovery does not unveil the proper identities, however, the John Doe defendants must be dismissed." (quoting Blakeslee v. Clinton County, 336 Fed. Appx. 248, 250 (3d Cir. 2009))).

180 Martin, *supra* note 175, at 1227.

181 *Id*.

182 *Id*.

essentially require that the plaintiff survive a motion for summary judgment without knowing the identity of the defendant, which is incredibly difficult.

The first standard was created in *Columbia Insurance Co. v. Seescandy.com* in which the court considered the balancing interests of requiring the disclosure of an anonymous online content provider.[183] The court created a fairly weak standard to govern the disclosure of the defendant's identity.[184] The court required that the plaintiff (1) "identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court," (2) "identify all previous steps he had taken to locate the defendant," and (3) "establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss."[185] Thus, as long as the plaintiff can survive a motion to dismiss and has made some efforts to identify the plaintiff without a court order, the court will likely issue the subpoena.

The second standard is known as the "good faith" standard and it is the most favorable to plaintiffs. In *In re Subpoena Duces Tecum to America Online, Inc.*, a company sued five John Does for allegedly publishing defamatory content on an America Online chat room.[186] AOL refused to comply with the order.[187] In balancing the right to communicate anonymously with the need "to assure that those persons who choose to abuse [the right],"[188] the court held that the identity of the John Doe defendant should be disclosed because the company had a "legitimate, good faith basis" to allege a cause of action against the defendants.[189]

While the above cases were deferential to plaintiffs, in *Rocker Management LLC v. John Does 1–20*, the Northern District of California applied a third, less deferential standard that favored anonymity.[190] Rocker Management sued fifteen anonymous defendants and served Yahoo with a subpoena demanding the disclosure of the identity of two of the defendants.[191] The court found that, given the totality of the circumstances, the anonymous defendant's identity should not

183 185 F.R.D. 573, 578 (N.D. Cal. 1999).
184 *See id.*
185 *Id.*
186 52 Va. Cir. 26, 26–27 (Cir. Ct. 2000).
187 *Id* at 27.
188 *Id.* at 34–35.
189 *Id* at 37.
190 No. 03-MC-33, 2003 WL 22149380, at *3 (N.D. Cal. 2003).
191 *Id.* at *1.

be disclosed because the plaintiff could not be successful on a libel claim.[192] The court determined that a reasonable viewer would not interpret the posts to be factual assertions and thus, the claim for libel could not be successful on the merits.[193] Accordingly, the defendant's identity should not be disclosed.[194] This standard is tougher on plaintiffs because it requires the court to analyze the merits of the plaintiff's claim (without knowing the identity of the defendants), rather than deferring to the plaintiff's "good faith basis" for identifying the defendant.

The fourth standard includes a balancing test and a notice requirement which, in effect, greatly favors the right of anonymity of defendants. In *Dendrite International Inc. v. Doe No. 3*, a company brought a defamation action against John Doe defendants.[195] The Superior Court of New Jersey hoped to strike the proper balance between the defendant's First Amendment right to anonymous speech and the plaintiff's interest in protecting its reputation.[196] In doing so, the *Dendrite* standard requires the plaintiff: (1) give notice to the anonymous poster that they are the subject of a subpoena;[197] (2) identify the exact statements that "allegedly constitute actionable speech;"[198] and (3) "produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant."[199] Moreover, if all the above requirements are met, the court must then balance the necessity of the disclosure, measured by the strength of the prima facie case presented by the plaintiff, with the First Amendment right of the defendant to speak anonymously.[200] In applying this standard, the court found that although the statements were false and potentially defaming, the company failed to establish sufficient evidence to prove that the statements caused injury to the company's reputation.[201] Thus, the court affirmed the lower court's denial of the plaintiff's motion to conduct discovery to identify the defendant.[202] In applying

---

192 *Id.* at *2–3 (highlighting the "grammar and spelling errors" on the forum and a warning message on the forum indicating that the thread consisted of users' opinions).

193 *Id*. at *3.

194 *Id*.

195 775 A.2d 756, 756–57 (N.J. Super. Ct. App. Div. 2001).

196 *Id*. at 760.

197 *Id*.

198 *Id*.

199 *Id*.

200 *Id*. at 760–61.

201 *Id*. at 771–72.

202 *Id*. at 760.

the *Dendrite* standard, subsequent courts have used it to allow and disallow the disclosure of the identity of an anonymous Internet poster.[203]

The fifth standard is another that favors the defendant's First Amendment right to anonymity. In *Doe v. Cahill*, the Supreme Court of Delaware explicitly refused to adopt the standards found in *Seescandy* or *America Online*, finding that those standards were "too easily satisfied" to adequately protect anonymous speech.[204] Rather, the court went in the direction of *Dendrite*, but created a two-part test.[205] The first part is a notice requirement similar to that in *Dendrite*, and the second part requires the plaintiff submit sufficient evidence to withstand a motion for summary judgement for each element of their claim.[206] While the court made an exception for prima facie elements that would be impossible to prove without disclosing the defendant's identity (such as the malicious intent element),[207] the standard weighs heavily in favor of protecting anonymous posters because of the extremely high burden on the plaintiff to survive summary judgment without knowing the identity of the defendant.[208]

"Most courts have adopted a John Doe subpoena standard that is balanced heavily in favor of the anonymous online speaker," such as the *Dendrite* or *Cahill* standard.[209] Some courts have created hybrids of the *Cahill* and *Dendrite* standard.[210] Others have added to the good faith standard by requiring the plaintiff to prove that the information requested cannot be obtained from another other source.[211]

While the applied standards of courts are split, the balancing factors that the court must assess remain the same—the plaintiff's right to redressability for defamatory speech versus the defendant's First Amendment right to free speech

---

[203] *Compare* Immunomedics, Inc. v. Doe, 775 A.2d 773, 777 (N.J. Super. App. Div. 2001) (holding that the plaintiff provided sufficient evidence to prove that the anonymous defendant was an employee of the company and that he violated a confidentiality agreement and allowed the subpoena), *with* Highfields Capital Mgmt. L.P. v. Doe, 385 F. Supp. 2d 969, 970–71 (N.D. Cal. 2005) (concluding that plaintiff did not show that there was a "real evidentiary basis" for surmising that the defendant engaged in "wrongful conduct" that caused real harm to the plaintiff).

[204] 884 A.2d 451, 458 (Del. 2005). For other courts that have adopted this stricter standard, see *SaleHoo Group, Ltd. v. ABC Co.*, 722 F. Supp. 2d 1210, 1216 (W.D. Wash. 2010); *Mobilisa, Inc. v. Doe*, 170 P.3d 712, 720 (Ariz. Ct. App. 2007).

[205] *Cahill*, 884 A.2d at 461.

[206] *Id*. at 460, 463.

[207] *Id*. at 464.

[208] *Id*. at 459.

[209] Wesley Burrell, *I Am He as You Are He as You Are Me: Being Able To Be Yourself, Protecting the Integrity of Identity Online*, 44 LOY. L.A. L. REV. 705, 729 (2011).

[210] *See* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 1154, 1171–72 (Ct. App. 2008).

[211] *See* Enterline v. Pocono Med. Ctr., 751 F. Supp. 2d 782, 789 (M.D. Pa. 2008).

and anonymity. There is a direct trade-off for a court siding with a particular factor. Weak protections for anonymity may give plaintiffs "extra-judicial self-help remedies."[212] Alternatively, giving anonymity "too much deference will immunize online harassers and defamers, eliminate deterrence, and leave plaintiffs powerless."[213] Different facts result in different analyses.[214]

However, these courts' reluctance to encourage "extra-judicial" remedies come at the expense of cybercrime victims. These courts do not appreciate the fact that if a plaintiff spends the time and resources to pursue action in court, they likely do have a good faith reason to. Further, by subjecting plaintiffs to survive summary judgment without knowing the identity of their perpetrator creates a tantamount blockage to the courthouse (as the motion will likely be dismissed).[215]

In particular, courts should not expect a victim of identity theft to prove that the defendant benefitted from the misappropriation (an essential element of the right of publicity) if they do not know the person responsible for the misappropriation. Further, courts cannot analyze the severity of misappropriation (i.e., history of previous infringements) without knowing who the infringer is. Nonetheless, courts with strict John Doe subpoena standards are shielding potential cyber criminals and preventing victims from gaining compensation.

C. The Communications Decency Act

The Communications Decency Act (CDA) has created another hurdle for victims of VR identity misappropriation. When plaintiffs cannot seek redress from the perpetrator themselves (whether for lack of personal jurisdiction or failing to identify an anonymous defendant), the last-ditch effort for the plaintiff is to try to sue the VR service provider. VR providers are akin to ISPs due to the expansive definition of ISPs provided by Section 230 of the CDA.[216]

---

[212] Doe v. Cahill, 884 A.2d 451, 457 (Del. 2005).

[213] Burrell, *supra* note 209 at 732; *see* Zeran v. Am. Online, Inc., 129 F.3d 327, 334 (4th Cir. 1997).

[214] Burrell, *supra* note 209, at 730. Courts consider anonymity most critical in circumstances such as "'governmental whistle blowing; labor organizing; dissident movements in repressive countries; gay and lesbian issues; and resources dealing with addiction, alcoholism, diseases and spousal abuse,' as well as where the speech at issue contributes to important public debate." *Id*. (quoting Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 329 (2008)).

[215] FED. R. CIV. P. 4(m).

[216] *Infra* note 230; *see also* Burrell, *supra* note 209, at 719. The CDA defines an interactive computer service as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C.

Unfortunately for victims, the CDA and subsequent case law interpreting the statute have rendered ISPs virtually immune to all transgressions, and thus misappropriations, that occur on their computer programs. Not only does this prevent the plaintiff from suing them directly, but it also creates a disincentive for ISPs from policing their own networks.

The CDA was passed in 1996 with the purpose of regulating obscene content on the Internet.[217] Congress also sought to promote the free exchange of information over the Internet and to encourage self-regulation of Internet content by ISPs.[218] In doing so, Congress had to balance two conflicting interests: (1) protecting users from inappropriate and offensive material and (2) maintaining the Internet as a forum for the free exchange of information and ideas.[219]

Congress took two different approaches to policing online content. First, it created a set of government-enforced criminal regulations on online activity, which the Supreme Court struck down in *Reno v. ACLU* on the basis that such regulation would hinder free speech and violate the First Amendment.[220] The second approach was a hands-off, self-regulation approach which survives today in Section 230 of the Act.[221]

Section 230 was passed to protect "'Good Samaritan[] ISPs … who take steps to screen indecency and offensive material for their customers'; and … to establish a policy against online content regulation by the federal government".[222] Section 230 was passed as "a direct response to the ruling in *Stratton-Oakmont, Inc. v. Prodigy Services, Co.*, where an ISP was held liable as a publisher because it had been vetting obscene materials."[223] "Prior to *Stratton*, [ISPs] were treated as distributors (not publishers) of third-party content posted to the Internet."[224] The distributor's liability standard finds ISPs

§ 230(b) (2012).

[217] Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 249 (2007).

[218] 47 U.S.C. § 230(b) (2012).

[219] *Id.*; S. REP. No. 104-23, at 59 (1995) (noting that Congress "has been troubled by an increasing number of published reports of inappropriate uses of telecommunications technologies to transmit pornography, engage children in inappropriate adult contact, terrorize computer network users through 'electronic stalking' and seize personal information").

[220] Reno v. ACLU, 521 U.S. 844, 859–60, 885 (1997).

[221] *See* Medenica & Wahab, *supra* note 217, at 251.

[222] Burrell, *supra* note 209, at 719 (alteration in original) (quoting 141 CONG. REC. 22,045 (1995) (statement of Sen. Cox)).

[223] *Id.*; 1995 WL 323710 at *1, *2, *5 (N.Y. Sup. Ct. May 24, 1995).

[224] Rachel Purcell, *Is that Really Me?: Social Networking and the Right of Publicity*, 12 VAND. J. ENT. & TECH. L. 611, 616 (2010).

liable in suits arising from third party created material "only if the ISP 'knew or had reason to know' that the questionable content was posted."[225] On the other hand, the publisher's liability standard treats ISPs as if they created the content themselves with a strict liability standard.[226] The court applied the publisher liability standard to Prodigy Services because the company attempted to regulate or vet the content on its service.[227] Consequently, the *Stratton* ruling "discouraged [ISPs] from voluntarily monitoring material posted to the Internet, since abstaining from monitoring was the only way [ISPs] could limit their exposure to liability for third-party generated content."[228] Thus, Section 230 was passed to prevent ISPs from being held to publisher liability standards and to encourage ISPs to actively pursue content regulation programs and invest into methods and technologies for protecting users from obscene content.[229]

In relevant part, Section 230 states "[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."[230] Since its enactment, however, Section 230 has become a shield from liability even when ISPs attempt no regulation whatsoever, running counter to the purpose of Section 230.[231] The protected intermediaries include not only regular ISPs, but also a range of "interactive computer service providers" consisting of nearly any online service that publishes third-party content.[232] VR content companies fit the description of interactive computer service providers because it will display the content of its users.

A year after Congress passed the CDA, the *Zeran v. American Online, Inc.* case was decided by the Fourth Circuit.[233] The case was about content posted on an AOL message board that advertised merchandise in support of the Oklahoma

---

225 *Id*. (quoting Cubby, Inc. v. Compuserve Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991)).

226 *Id*.

227 *Stratton Oakmont, Inc.*, 1995 WL 323710 at *5.

228 Purcell, *supra* note 224.

229 H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.).

230 47 U.S.C. § 230(c)(1) (2012). Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id*. § 230(f)(2). The term "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." *Id.* § 230(f)(3).

231 Burrell, *supra* note 209, at 710–11.

232 *See id* at 721.

233 129 F.3d 327, 327 (4th Cir. 1997).

City Bomber.[234] The plaintiff was fraudulently connected to the sales of the shirts and was soon bombarded with angry phone calls, including death threats.[235] The plaintiff contacted AOL and requested that AOL take down the posts, "but despite AOL's efforts, the posts remained online."[236] The plaintiff then sued AOL for an "unreasonable delay" in taking down the posts.[237] He argued that AOL was subject to distributor liability because AOL had "reason to know" of the defamatory content because he gave the company notice of the defamatory post.[238] However, the court denied this argument and found that there is no legally enforceable distinction between distributor's liability and publisher's liability with regard to Section 230.[239] The court considered distributor's liability to be a subset of publisher's liability and ISPs are immune to both forms of liability.[240] The court reasoned that if ISPs were subject to distributor's liability, or liability upon notice, "they would face potential liability each time they received notice of a potentially defamatory statement—from any party, concerning any message."[241] The court was concerned that this liability would be crushing considering that the number of postings and the fact that ISPs, which at the time were in their infancy, would not be able to survive.[242]

Zeran, while not explicitly describing it as such, implemented a three-part test for establishing ISP immunity that has since been the majority interpretation of Section 230.[243] The defendant service provider must demonstrate: (1) that it was acting as a user or provider of an "interactive computer service"; (2) that holding it liable in the matter plaintiff seeks would treat the defendant "as the publisher or speaker" of the information furnished "by another information content provider," and (3) that the defendant itself was not the "information content provider" of the content at issue.[244]

After *Zeran*, courts further expanded the scope of Section 230 immunity. In *Batzel v. Smith*, the Ninth Circuit further expanded the scope of immunity by broadening the definition of what qualified as an ISP.[245] The defendant was an

---

234 *Id*. at 329.

235 *Id*.

236 *Id*; Burrell, *supra* note 209, at 720.

237 *Zeran*, 129 F.3d at 328.

238 *Id.* at 331.

239 *Id*. at 332.

240 *Id*.

241 *Id*. at 333.

242 *Id*.

243 Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 586 (2008).

244 *Zeran*, 129 F.3d at 330.

245 333 F.3d 1018, 1030 (9th Cir. 2003).

administrator of an email listserv[246] who had forwarded allegedly defamatory content to the listserv.[247] The court defined an interactive computer service as "any information services or other systems, as long as the service or system allows 'multiple users' to access a 'computer server.'"[248] The court held that the administrator was immune as an ISP under Section 230.[249] Additionally, in *Barrett v. Rosenthal*, the Supreme Court of California held that republishing information did not make one an information content provider.[250]

The legislative history does not indicate whether Congress intended the immunity granted to service providers to also apply to Internet users and general posters of content in the sense applied in *Barrett*.[251] In fact, the *Barrett* court itself recognized that users are in a different position than providers.[252] Most significantly, individual users "do not face the massive volume of third-party posting that providers encounter" and thus, "self-regulation is a far less challenging enterprise for them."[253] And "[u]sers are more likely than service providers to actively engage in malicious propagation of defamatory or other offensive materials."[254]

These cases illustrate the general trend of courts interpreting Congress's intent solely to favor freedom of speech and deregulation in online policy, and courts have done so at the expense of Congress's equally important aim to fight online obscenity through "vigorous enforcement" of federal online regulation.[255] Even worse is the continual justification of this treatment on the basis of protecting an infant Internet industry, as ISP companies are now mature and are major forces in our economy today.[256] Effectively, these decisions, coupled with

---

246 A listserv is an application that distributes messages to subscribers on an electronic mailing list. *Id.* at 1021, n.2.

247 *Id*. at 1021–22.

248 *Id*. at 1030.

249 *Id.* at 1031.

250 146 P.3d 510, 519 (Cal. 2006). The court did express slight reservations but deferred to the language of the CDA stating, "the prospect of blanket immunity for those who intentionally redistribute defamatory statements on the Internet has disturbing implications. Nevertheless, by its terms Section 230 exempts Internet intermediaries from defamation liability for republication … to protect online freedom of expression and to encourage self-regulation, as Congress intended." *Id*. at 529.

251 Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 152 (2008).

252 *Barrett*, 146 P.3d at 526.

253 *Id*.

254 *Id*.

255 Burrell, *supra* note 209, at 722.

256 Akin Oyedele, *FORGET FANG*: *Goldman Adopts a New Acronym for the Most Powerful Tech Stocks Driving the Market*, BUSINESS INSIDER (June 9, 2017), https://www.businessinsider.com/faamg-tech-stocks-market-goldman-2017-6 (noting that Facebook, Amazon, Apple, Microsoft, Netflix, and Google are the most

user anonymity laws (discussed in Section B) have eviscerated protections against online misconduct.[257] As Burrell writes, "this one-sided policy creates a 'user-beware' Internet."[258] This type of environment only reinforces the position that VR users will be immersed into a world where they cannot seek redress for their misappropriated identity.

Importantly, some courts have held that the right of publicity is an exception to the broad immunity granted by Section 230.[259] This means that, in certain circuits, some victims of identity misappropriation that assert a right of publicity claim can sue the VR provider (or ISP) directly, without fearing immunity. While this is not the nationwide standard, it does display a willingness to give victims of identity misappropriation a chance to sue the ISP directly.

In *Doe v. Friendfinder Network*, a woman discovered a profile on an adult website using her name and other biographical information.[260] On the profile was a nude photo of a woman with enough resemblance that a reasonable person could identify the plaintiff.[261] After suing the ISPs on multiple tort claims, the district judge dismissed all but the right of publicity claim.[262] The court ruled that "while Section 230(e)(2) exempts her right of publicity claim from the immunity provision of the CDA, that provision applies with full force to the other invasion of privacy claims asserted in her complaint."[263] The *Friendfinder* court also argued that the plain language of Section 230(e)(2) exempted right of publicity claims.[264] The court also recognized that allowing state law intellectual property claims would not have a "devastating" impact on the Internet.[265] Responding to the crushing liability rationale Congress enlisted when drafting Section 230 immunity, the court pointed out that "both the Internet and so-called 'e-commerce' remain alive and well, and show no signs of imminent collapse."[266]

---

powerful drivers of the S&P 500 and NASDAQ).

257 *See* Burrell, *supra* note 209, at 723.

258 *Id*.

259 Doe v. Friendfinder, 540 F. Supp. 2d 288, 301 (D.N.H. 2008). However, not all courts recognize this exception. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) (holding that ISPs are immune from right of publicity claims).

260 *Friendfinder*, 540 F. Supp. 2d at 292.

261 *Id*.

262 *Id*. at 291.

263 *Id*. at 303 (citing MCCARTHY, *supra* note 91, §3:42).

264 *Id.* at 301. § 230(e)(2) states that "nothing in this section shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2) (2012).

265 *Friendfinder*, 540 F. Supp. 2d. at 301.

266 *Id*. at 301–02.

However, not all jurisdictions regard the right of publicity as an exemption to Section 230 immunity. In *Perfect 10, Inc. v. CCBill LLC*, the Ninth Circuit held that inclusion of intellectual property rights would both "be contrary to Congress's expressed goal of insulating the development of the Internet from the various state-law regimes"[267] by "fatally undermin[ing] the broad grant of immunity provided by the CDA."[268] Hence, the court ruled that the right of publicity, trade defamation, unfair competition, and dilution, among others, were not exempted by Section 230(e)(2).[269] The court also found that the CDA only abrogates ISPs immunity for federal intellectual property claims.[270] But, as discussed earlier, there is no federal intellectual property claim for the right of publicity.[271]

Some academics have argued that the *Friendfinder* court's reasoning that ISPs should not be immune from any intellectual property claims is most persuasive based on the text of the CDA.[272] Section 230(e)(2) reads "[n]othing in this section shall be construed to limit or expand *any* law pertaining to intellectual property."[273] As Purcell explains, "[t]he Supreme Court has noted in other contexts that the term 'any' is 'expansive language [that] offers no indication … that Congress intended [a] limiting construction.'"[274] Thus, as the *Friendfinder* court argues, "any law pertaining to intellectual property should include both state and federal law."[275]

Nevertheless, this evolving circuit split concerning ISP immunity for the right of publicity reveals yet another massive hurdle that VR victims face when seeking identity protection and redressability. Until this split is resolved, victims in jurisdictions that currently extend sweeping immunity will remain dependent on finding redressability through claims against the individual user, which, as we have seen, presents many seemingly insufferable challenges to victims of identity misappropriation.

---

267 488 F.3d 1102, 1118 (9th Cir. 2007).
268 *Id.* at 1119, n.5.
269 *Id*. at 1119.
270 *Id*.
271 *See supra* note 137 and accompanying text.
272 Purcell, *supra* note 224, at 623.
273 47 U.S.C. § 230(e)(2) (2012) (emphasis added).
274 Purcell, *supra* note 224, 623–24 (citing *Friendfinder*, 488 F.3d at 299).
275 *Id*.

IV. PROPOSED SOLUTIONS TO LIFT THE PROCEDURAL HURDLES THAT PROTECT VR IDENTITY THIEVES

VR will increase the ease with which ordinary people could lose their VR identities which will threaten the social framework of VR society and its millions of eventual users.[276] Unfortunately for these victims, identity protection law is currently comprised of an inconsistent web of legal protection caused by various procedural hurdles.[277]

So, what can be done to lift these hurdles to create a VR society where users feel safe to use their actual likeness when interacting with others? First, courts need to revamp what amounts to minimum contacts for cyber interactions. Second, the legal system needs to reform its preference towards online anonymity when a certain IP address is connected to identity misappropriation or other cyber-crimes. Third, Congress should redraft the Communications Decency Act to place liability on the ISPs to incentivize these now established companies to police their own networks. By implementing these changes, the substantive law should evolve to a point where users will be adequately protected to use their real likeness on VR platforms.

A. Fitting the International Shoe onto VR

The legal system needs to seriously revamp what amounts to minimum contacts for cyber interactions or apply the Active Website standard to VR applications so that plaintiffs could compel VR identity thieves into their forum court.

As it stands, VR users likely fall within the third category of minimum contacts, the Interactive Website.[278] Therefore, a defendant must make additional non-Internet contacts (travel, mail contacts, etc.) to the plaintiff's forum in order to purposefully avail himself to that forum.[279] The problem with that is that it is unlikely that a VR identity thief will ever make a non-Internet contact with the plaintiff's specific forum, especially in the case of an international VR thief. This effectively creates a de facto barrier to the plaintiff's most convenient forum, stifling enforcement as plaintiffs (especially those with little value in their identity) are unlikely to pursue legal action across the country.

---

276 *Supra* Part II.

277 *See supra* Part II.

278 *See supra* note 165 and accompanying text.

279 Barrett v. Catacombs Press, 44 F. Supp. 2d 717, 726 (E.D. Pa. 1999).

Taking into consideration the realities of the Internet age, courts should reclassify what types of digital contacts would satisfy minimum contacts and remove, or significantly lessen the importance of, non-Internet contacts. However, because the Internet is an infinitely connected network that reaches every state, without some limitation on personal jurisdiction, defendants could be summoned into any forum raising *Burger King* fairness concerns.[280]

Thus, courts need to implement a balancing test that weighs the desirability of convenience for the plaintiff with fairness to the defendant. For VR identity misappropriation cases, the court should balance: (1) the severity of the misappropriation; (2) any evidence that demonstrates the defendant targeted the plaintiff particularly; and (3) a showing that the defendant used the plaintiff's identity to defraud citizens of the plaintiff's forum state. Additionally, courts can look to other factors that persuade a court that it would be constitutional to hail the defendant to the forum. For instance, courts can review the defendant's history of misappropriation and other cybercrimes, and other cybercrimes committed during the act of misappropriation (such as hacking).

Alternatively, courts can apply the "active website"[281] status to VR applications and its users. An active website is one where the parties interact back and forth, make purchases, enter into contracts, and conduct activities that involve the participation of both parties.[282] While most user-driven applications have been treated as interactive websites, the intimate and realistic interactions among VR users should compel users to a higher level of jurisdiction. VR users' continuous and systematic interactions will be very similar to real-life interaction, particularly in comparison to current social media websites. These incredibly realistic interactions should cause users to reasonably anticipate possible litigation, and thus, compel courts to find that there is personal jurisdiction over these users. The argument becomes even stronger if VR applications indicate what state each user comes from so that each user knows exactly where they could be summoned to. Thus, if VR applications are classified as active websites, then VR identity thieves would be subject to personal jurisdiction in every one of their victims' forums.

By revamping the contacts needed to survive personal jurisdiction for interactive websites or by classifying VR applications as active websites, victims

---

[280] *See* Burger King v. Rudzewicz, 471 U.S. 462, 476–78 (1985); *see also*, Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945).

[281] *See supra* notes 155–59 and accompanying text.

[282] *See supra* notes 155–58 and accompanying text.

of identity theft will be given the tools to sue the person that stole their VR identity.

B. Removing the Shield of Anonymity for VR Identity Thieves

In addition, courts, particularly those with strict John Doe subpoena standards, must lower their deference towards online anonymity when a certain IP address is linked to cybercrime. As a practical matter, plaintiff-friendly standards need to be implemented so that plaintiffs can assert their legal rights in court and at least be heard by the justice system. From a constitutional standpoint, once a user commits a cybercrime or infringes on another's property right, they would then sacrifice their First Amendment right to remain anonymous. The Supreme Court has limited the First Amendment in the past when the speaker was promulgating false statements of facts.[283] More importantly, courts have tempered with a defendant's First Amendment right to free speech in favor of intellectual property rights.[284]

Here, anonymous VR identity thieves infringe on a user's intellectual property right of publicity by stealing their likeness and defrauding others by using a stolen identity. In effect, these thieves both promulgate false statements of facts and infringe on the user's intellectual property rights. Thus, an ISP should be compelled to disclose the identity of such an IP address so that the plaintiff can identify who the infringer is so that they can either file a claim at the defendant's domicile or reach out to the defendant and seek redress out of court.

To remove the undeserved shield of anonymity, courts need to adopt John Doe subpoena standards similar to the standards adopted in *Seescandy*[285] or *America Online* (the "good faith" standard).[286] In *Seescandy*, the court required that the plaintiff demonstrate that: (1) his claim was strong enough to survive a motion to dismiss; (2) that the information sought would likely lead to identifying the defendant; and (3) he took sufficient steps to locate the defendant.[287] In *American Online*, the court adopted the "good faith" standard which balanced the defendant's right to communicate anonymously with the

---

[283] Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974) ("[T]here is no constitutional value in false statements of fact.").

[284] *See* Hart v. Electronic Arts, Inc., 717 F.3d 141, 170 (2013). The court used the transformative use rest to determine if a video game developer's use of a college football player's likeness amounted to a violation of the right of publicity. *Id*. at 165–70. *See also* Facenda v. N.F.L. Films, Inc., 542 F.3d 1007, 1018 (3rd Cir. 2008).

[285] Columbia Ins. Co. v. Seescandy, 185 F.R.D. 573 (N.D. Cal. 1999).

[286] Zeran v. America Online, 2000 WL 1210372 *6 (Va. Cir. Ct. Jan. 31, 2000).

[287] *Seescandy*, 185 F.R.D. at 578–79.

need to assure that those persons who abuse the opportunities presented by this medium will be served justice.[288]

While some critics have argued that these standards are too deferential to plaintiffs,[289] they at least give plaintiffs the ability to identify the person who stole their identity so that they could initiate a suit and have their case heard by their peers. The alternative, more defendant-protective standards, such as those articulated in *Dendrite*[290] or *Cahill*,[291] amount to a serious failure of the justice system in the context of an alleged cyber-criminal defendant. These courts gave substantial weight to the defendant's First Amendment right of free speech and did not take into consideration the alleged actions of the defendant when constructing their respective balancing tests.[292] Further, these standards, especially the *Cahill* standard, would not be workable for VR identity misappropriation cases because the standards require the plaintiff survive summary judgment, without even knowing the identity of the defendant.

Instead, a better legal system would base its John Doe subpoena standard off the alleged actions of the defendant—the more serious the action, the less deferential to the defendant. Under the most plaintiff-friendly *Seescandy* standard, the plaintiff would still have to satisfy a motion to dismiss,[293] so the plaintiff could not resort to alleging baseless crimes in hopes of winning a favorable standard. This solution does not solve the entire problem, as victims of minor thefts sitting in defendant-favorable jurisdictions would likely still not be able to compel the disclosure of their perpetrator. Nonetheless, this solution would be a great start by giving more victims in defendant-favorable jurisdictions a chance for their cases to be heard.

Under this proposal, the First Amendment right of anonymous free speech gives way in order to protect user's VR identity and prevents VR identity thieves from hiding under an undeserved blanket of constitutional protection. However, the plaintiff would likely be required to file a claim only at the defendant's place of residence because of Internet personal jurisdiction law (discussed in Section A). While suing in the defendant's place of residence is more desirable than

---

288 *America Online*, 2000 WL 1210372, at *6.

289 *See* Sophia Qasir, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, 81 FORDHAM L. REV. 3651, 3686 (2013).

290 Dendrite Inc. v. John Doe, 775 A.2d 756 (N.J. 2001).

291 John Doe v. Cahill, 884 A.2d 451 (Del. 2005).

292 *See supra* notes 195–200, 204–208 and accompanying text. In *Cahill*, the defendant was accused of posting a defamatory statement made on the Internet. 884 A.2d at 454. In *Dendrite*, the defendant was also accused of posting a single defamatory statement about a corporation. 775 A.2d at 760.

293 *See supra* note 176 and accompanying text.

having no forum at all, it is hard to imagine a "regular joe" plaintiff with minimal value in his identity, traveling far and paying for legal expenses for what is likely a minimal judgment.

C. Redrafting the 1996 Communications Decency Act for 2019's Internet Landscape

Congress must also redraft the Communications Decency Act to hold ISPs and other interactive computer services responsible for the actions that occur on their Internet products, in this case VR programmers and software developers. The CDA was designed to shield young, exciting Internet companies from crushing liability in the early stages of the Internet.[294] However, these companies are not the same companies they were in 1996. For the most part, these companies are corporate powerhouses that encompass the idea of being "too big to fail" and whose success is a major determinate of the success of the stock market.[295] Hence, these companies can now afford *both* the potential liability and the cost of prevention.[296] If incentivized, these companies can invest in tools (like AI, machine learning) that find stolen identities and remove them from the program.

However, as it stands these conglomerates are being wrongfully shielded by Internet protectionist policies from the late 1990s. Reducing ISP immunity will help in two ways. First, it will give victims *some* means of recourse, assuming the above procedural concerns remain unaddressed and the victim can't sue the infringer (by lack of personal jurisdiction or strong anonymity deference). Second, it will incentivize ISPs to invest in detection tools to police their own network and reduce the frequency of cyber-crimes like identity misappropriation.

First, to reduce ISP immunity, courts should align with the *Friendfinder* reasoning that the CDA was intended to allow all intellectual property claims against ISPs.[297] The language of Section 230(e)(2) of the CDA clearly states that "[n]othing in this section shall be construed to limit or expand *any* law pertaining to intellectual property."[298] Hence, even though Congress intended to protect young Internet companies (an intention that does not apply to 2020 Internet

---

294 Burrell, *supra* note 209, at 719 (citing 141 CONG. REC. 22,045 (1995) (statement of Sen. Cox)).

295 Akin Oyedele, *supra* note 256.

296 These are two of the factors from Judge Learned Hand's famous B > PL formula in *United States v. Carroll Towing*, 159 F.2d 169 (2d. Cir. 1947).

297 *Jane Doe v. Friendfinder*, 540 F. Supp. 2d 288, 300–02 (D.N.H. 2008).

298 47 U.S.C. § 230(e)(2) (2012).

companies), it still recognized the danger of immunizing ISPs from intellectual property claims. Thus, courts in all jurisdictions should appreciate the clear language of Congress coupled with the now less-important Congressional intention of shielding young Internet companies.

Further, courts need to abandon the reasoning of the *Barrett* court that included all users in the interactive service provider definition of the CDA and, thus, immune from liability.[299] The court seems to ignore that users are in completely different positions than ISPs when it comes to potential liability and self-mitigation. For instance, a Facebook user can control what they post and are only responsible for their own content. Facebook itself, on the other hand, would face liability for its over two billion monthly users.[300] Thus, at the very least, courts need to treat users like what they really are, publishers of online content, and hence liable for what they create.

Lastly, Congress should incorporate into the CDA, and other relevant Internet statutes, victim compensation funds sponsored by these Internet companies for victims of cybercrimes. Statutes can condition recovery from the fund on providing the ISP sufficient notice and whether the crime could have been prevented had the ISP performed reasonable diligence in responding to the notice. Not only would this undo the reverse incentive of ISPs to address notices of crimes on their networks[301], but it would compensate the unfortunate plaintiff that had his identity stolen.

All together, these changes to the CDA and subsequent precedent would help prevent future theft and deter future identity thieves from misappropriating because they can be discovered and brought to justice.

D. Effect of Proposals on Substantive Identity Law

Incorporating these proposals would give plaintiffs the opportunity to bring identity misappropriation suits into court (whether against the particular infringer or the ISP). Once in court, the legal system and its community of scholars can comment on what substantive legal protections are the most desirable. In doing so, the legal community can resolve the various splits of authority on the sources of identity protection law discussed in this Comment.

---

[299] *Barrett*, 146 P.3d at 529.

[300] Sean W., *Facebook Has 2.32 Billion Monthy Users, Even After Endless Scandals*, MEDIUM, https://medium.com/@citysmartie/why-are-billions-of-us-still-using-facebook-45da13581b8f (last visited Jan. 11, 2019).

[301] *See supra* Part III.C.

By giving victims of VR identity misappropriation a forum, the substantive law will evolve and create a set of precedents that give all VR users (regardless of jurisdiction) the same protections so that they can use their real identity when interacting with other VR users. After all, VR will not be split into jurisdictions like the U.S. justice system. In particular, hearing more cases will allow courts to weigh in on whether there should be a federal right of publicity[302] or achiever greater uniformity across state common law.

Whether federal or common law, the evolved law needs to redefine what constitutes a benefit to the infringer so that *all* benefits (commercial or not) satisfy the benefit element. Further, non-celebrities should be allowed to recover for *at least* the value of their identity, plus any emotional and punitive damages caused by the invasion of their right. For these cases, courts should also permit recovery of emotional damages even if the plaintiff did not know of the misappropriation until later, given the relative ease of an infringer going undiscovered.[303] After all, an infringer that just wants to embarrass his victim should be culpable under the evolved statute even if the victim did not know of the misappropriation until after the damage was done.

By removing the procedural barriers to allow for the resolution of these substantive inadequacies, victims of VR identity misappropriation will have an opportunity to receive redress. Thus, users' willingness to use their real identity in VR will allow VR to become the idealized augmented reality that will bring humans even closer together.

CONCLUSION

The story has been told before: Technology progresses at an exponential rate, while the slow-moving legal system fails to catch up. With VR, there is nothing different. Until we recognize just how quickly technology and society are blending together, we will always lag behind. Perhaps, because we are human, the world we inhabit will always be a lawless "Wild West" in some form or another. But, if we are to strive for a complete legal system where no wrong goes unpunished or unrecognized, we need to start thinking of answers to these questions before millions of people are violated in virtual reality.

With the oncoming problem of VR identity misappropriation, perhaps the solution lies with the proposals of this Comment. Reconsidering what amounts to minimum contacts for cyber interactions among users, reforming online

---

302 *Supra* note 137 and accompanying text.

303 *See* Slocum v. Sears Roebuck & Co., 542 So. 2d 777 (La. Ct. App. 1989).

anonymity protection for IP addresses connected to identity misappropriation or other cyber-crimes, and redrafting the Communications Decency Act to impose liability on Internet Service Providers would give plaintiffs a course of action that they do not currently have. Bringing these actions to the courthouse (or threatening to) should reduce the frequency of identity misappropriation because perpetrators would be deterred from stealing identities and ISPs would be incentivized to police their networks—a desirable result for VR society (and society at large).

One must consider whether these proposals are made under the same legal assumptions and limitations of a pre-VR society. Perhaps one day VR users will be able to walk into a virtual courthouse, file their claim on a virtual docket, and have their case heard by a virtual judge and jury, all in the comfort of their home.[304] Maybe this Comment would make substantial headway further in the future, when technology and society become more intertwined. Whatever the case, we must remain cognizant of the legal questions and dangers VR and other emerging technologies create in hopes of finding meaningful answers so that we can adequately protect the users of such technologies.

JESSE LAKE[*]

[304] One can argue that Article III contemplated such an "inferior court" established by Congress. U.S. CONST. art. III, § 1. This very forward-thinking proposal would certainly alleviate the transaction costs associated with bringing a low-yielding identity misappropriation claim into the court house, but also raises due process concerns.

[*] J.D. Candidate, Class of 2020. I am very excited about the publication of this Comment, especially considering the pervasiveness of remote working during the COVID-19 pandemic. I'd like to thank Samuel Greeley for his support in the drafting process. I'd also like to thank Eric Pettis, Cai Roman, and Rashmi Borah for their outstanding work in editing this Comment and their management of the *Journal*.