JOURNAL OF LAW AND TECHNOLOGY AT TEXAS

Volume 4 • Part 1

CONSTRAINING THE CYBERMOB: USING A DOXING NOTICE AND TAKEDOWN REGIME TO OPTIMIZE THE SOCIAL UTILITY OF ONLINE SHAMING

And

THE POTENTIAL OF HEALTH DATA: EXPLORING CONSUMER GENERATED DATA AND THE BIG DATA ECOSYSTSEM

Journal of Law and Technology at Texas

Volume 4 • Part 2

Table of Contents

Constraining the Cybermob: Using a Doxing Notice and Takedown Regime to Optimize the Social Utility of Online Shaming

Erik Money*

Social media platforms have transformed an age-old institution, public shaming, into a new phenomenon known as "cybermobbing." Cybermobs cause outsized economic, reputational, and dignitary harm to their victims, resulting in a net negative social impact. Despite the severity of cybermobbing, no catch-all legal remedy is available to its victims. Even if a victim could overcome the practical barriers of getting individual mob members into the courtroom, current legal remedies are inadequate. Furthermore, § 230 of the Communications Decency Act immunizes Interactive Computer Service Providers ("ICSPs") against any potential liability. Cybermobbing victims are bereft of remedies.

After introducing the concept of cybermobbing, this Note examines case studies of cybermobbing, explains why victims cannot recover against cybermobs, considers the social utility provided by online shaming, and proposes statutory reform to optimize its social utility. This Note proposes sample legislation which uses the Digital Millennium Copyright Act as a template to create a notice and take-down regime for posts that expose personal information of private individuals (i.e., to "dox"). Under this Note's proposed sample legislation , entitled the Doxing Notice and Takedown Act ("DNTA"), ICSPs would be required to remove posts that dox private individuals upon notification. At that point, the poster could provide

---

* Juris Doctor candidate, University of St. Thomas School of Law, class of 2020. I would like to thank Professor Thomas Berg, Arlene Schuweiler, Alex Landreville, and Ryan Paukert for their valuable insights and assistance. The views expressed in this Note belong to the author alone.

counter-notification showing that the individual is a public figure or that the messages do not dox the individual. Because the exposure of personal information is what allows cybermobs to cause real-world harm, the DNTA would be an affirmative first step to optimize the social utility of online shaming.

Table of Contents

I. Introduction

Public shaming is nothing new. In the 1500s, transgressive individuals were met with scold's bridles, pillories, stockades, cucking stools, and other forms of corporal punishment.[1] A sign would often accompany the punishment, announcing the particular sin of the shamed community member.[2] Fortunately, physical public shaming fell out of favor in the 1600s, a development accredited to urbanization, industrialization, and the rise of the prison system.[3] With the advent of social media, however, public shaming has reared its ugly head with renewed vigor.[4] This digital shaming is a different beast from its predecessor.

The cybermob can attack anyone, anywhere, and for any reason.[5] The practice is known as "cybermobbing," a phenomenon where a group of people utilize an online platform to insult, dox,[6] threaten, and/or

---

[1] Matthew Green, *A Grim and Gruesome History of Public Shaming in London: Part 1*, LONDONIST (Jan. 19, 2017), https://londonist.com/2015/12/publicshaming1.

[2] *See* Kristine L. Gallardo, *Taming the Internet Pitchfork Mob: Online Public Shaming, The Viral Media Age, and the Communications Decency Act*, 19 VAND. J. ENT. & TECH. L. 721, 725 (2017).

[3] *Id.*

[4] *Id.*

[5] *See* Kate Klonick, *Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age*, 75 MD. L. REV. 1029, 1031 (2016). Klonick lucidly notes that "low cost, anonymous, instant, and easy access to the Internet has eviscerated whatever 'natural' limits there were to public shaming and has served to amplify its effects. Now, any perceived violation of a social norm—a racist Tweet, a sexist joke, taking up too much room on public transportation—can result in immediate, prolific condemnation from millions of people all over the world. Today, it is easier than ever to use shaming to enforce so-called social norms, and it is easier than ever for shaming to spin out of control." *Id.* (internal citations omitted).

[6] "[T]o publicly identify or publish private information about (someone) especially as a form of punishment or revenge." *Dox*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/dox (last visited Apr. 19, 2020).

humiliate another individual.[7] A cybermobbing normally begins when an individual is shown in a controversial light, having said or done something inappropriate.[8] The controversy does not need to be recent; victims can be, and often are, mobbed for something they said or did years ago.[9] Typically, targets provoke a mob by saying something controversial online.[10] Nevertheless, targets may also be mobbed for expressing moderate but unpopular opinions,[11] making silly jokes in real life,[12] or for simply being in the wrong place at the wrong time.[13] The victim is then publicly excoriated on social media, insulted, doxed, threatened, and potentially fired by an employer caving to public pressure.[14] The impact is devastating, normally far outsizing whatever misdeed—if any—provoked the mob. Some have been fired from their jobs,[15] others have had their career prospects ruined entirely,[16] and still others have killed themselves.[17] Despite the life-altering impact of cybermobbing, victims have little recourse.

---

[7] While the phenomenon has not yet been reduced to a formal definition, one writer has described "Cyber-mobbing" as "Cyber-cruelty that involves a group sharing the same malicious mindset or intent." Sue Scheff, *When Cyberbullying Turns Into Cybermobbing: Death by Suicide,* HUFFINGTON POST (Sept. 24, 2013), https://www.huffpost.com/entry/when-cyberbullying-turns-into-cyber-mobbing_b_3957416.

[8] *See infra* Section II.a.

[9] *Id.*

[10] *Id.*

[11] *See* Daniella Greenbaum, *The Social Media Mob is a Danger to Society*, WASH. POST (July 12, 2018, 5:46 PM), https://www.washingtonpost.com/opinions/the-social-media-mob-is-a-danger-to-society/2018/07/12/eef13834-860b-11e8-9e80-403a221946a7_story.html (opinion columnist for Business Insider pressured into resigning for saying a female actress should be able to portray a transgender man); Michael Friscolanti, *Why Andrew Potter Lost his "Dream Job" at McGill*, MACLEAN'S (Mar. 23, 2017), https://www.macleans.ca/news/canada/why-andrew-potter-lost-his-dream-job-at-mcgill (professor forced to resign from "dream job" over article opining that "Quebec is an almost pathologically alienated and low trust society, deficient in many of the most basic forms of social capital that other Canadians take for granted.").

[12] *See* Klonick, *supra* note 5, at 1030–32 (discussing incident where a man was fired for making "dongles" joke at tech conference after a woman posted his picture online and that woman was subjected to threats of physical harm in a retaliatory mobbing).

[13] *See infra* Section II.a (discussing Cantrell and Tripathi case studies).

[14] *See generally infra* Section II.a discussion about cybermobbing case studies.

[15] *See infra* Section II.a regarding Justine Sacco.

[16] DANIELLE KEATS CITRON, HATE CRIMES IN CYBER SPACE 8 (Harv. Univ. Press, 2014) (noting that most employers, roughly 90 percent, rely on online reputation as an employment screen for prospective hires).

[17] *See infra* Section II.a regarding Cantrell. Even if the victim does not commit suicide, the individual is still at much higher risk for developing a mental illness, such as

Pursuing individual mob members is impractical because of internet anonymity, jurisdictional issues, the number of defendants, the possibility of judgment-proof defendants, and the likelihood that, individually, each defendant's actions are not actionable. Attempts to hold Interactive Computer Service Providers ("ICSP") liable will be frustrated by § 230 of the Communications Decency Act ("CDA").[18] This Note proposes that Congress amend the CDA and pass legislation akin to this Note's proposed Doxing Notice and Takedown Act to curb cybermobbing.[19]

Section II of this Note describes case studies of cybermobbing and examines its social utility. In Section III, this Note explains why holding individual members of the mob is impracticable under current law. Section IV proposes that Congress amend the CDA and pass the Doxing Notice and Takedown Act.

II. The Phenomenon of Cybermobbing

Online shaming is essential for normative role enforcement.[20] But oftentimes, such shaming devolves into cybermobbing, a practice which inflicts irreparable harm unrelated to a violated norm. This section discusses case studies of cybermobbing and evaluates its social utility. On balance, it concludes that cybermobbing has a net negative effect on society and requires a statutory solution.

A. Cybermobbing Case Studies

On December 20, 2013, Justine Sacco made an unforgettable Tweet before boarding a plane from London to Cape Town:

- "*Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!*"[21]

---

depression, anxiety, panic attacks, post-traumatic stress disorder, or anorexia nervosa. *See* CITRON, *supra* note 16, at 10–11.

[18] Communications Decency Act, 47 U.S.C. § 230 (2018). The term "interactive computer service provider" refers to online platforms like Twitter, Facebook, and YouTube.

[19] *Id.*

[20] *See generally* Klonick, *supra* note 5.

[21] Ed Pilkington, *Justine Sacco, PR Executive Fired Over Racist Tweet, "Ashamed"*, GUARDIAN (Dec. 22, 2013, 6:26 PM), https://www.theguardian.com/world/2013/dec/22/pr-exec-fired-racist-tweet-aids-africa-apology.

Not only was this Tweet in poor taste, it was also a horrible career move, as Sacco was a corporate communications director at the time.[22] The post remained up while Sacco was in the air, and her account remained unresponsive during the Twitter uproar, which lasted roughly eleven hours.[23] The hashtag "#HasJustineLandedYet" began trending.[24] Days later, Sacco's employer fired her, commenting that it hoped that "time and action, and the forgiving human spirit, will not result in the wholesale condemnation of an individual who we have otherwise known to be a decent person at core."[25]

James Gunn, the director for "Guardians of the Galaxy," was similarly fired after an organized political backlash resurfaced his year-old Tweets, which included pedophilic jokes.[26] After Gunn became a vocal critic of President Trump, Mike Cernovich, an conservative political pundit, dug up Gunn's Tweets and broadcast them on Twitter and on his personal website.[27] He concluded by stating "James Gunn works for Disney," provided Disney's e-mail address, and prompted users to email Disney to ask "why they trust James Gunn around children." Gunn was fired shortly thereafter.[28]

Sarah Jeong faced similar backlash for her Tweets. Jeong, a Harvard Law School graduate, is a writer specializing in the intersection of law and technology.[29] The New York Times's decision to appoint her as a lead technology writer for its editorial board was met with immediate backlash from certain news sites, which reposted her Tweets from years earlier, including:[30]

---

[22] *Id.*
[23] *Id*.
[24] *Id.*
[25] *Id.*
[26] Brooks Barnes, *Disney Fires 'Guardians of the Galaxy' Director Over Offensive Tweets*, N.Y. TIMES (July 20, 2018), https://www.nytimes.com/2018/07/20/business/media/james-gunn-fired-offensive-Tweets.html.
[27] Mike Cernovich, *James Gunn Endorses Pedophilia in 10,000 Deleted Tweets*, CERNO (last accessed Oct. 20, 2019), https://www.cernovich.com/james-gunn-endorses-pedophilia-in-10000-deleted-Tweets/.
[28] Disney later rehired Gunn, but the backlash against Gunn is still referenced in political discussions. *Id.*
[29] *See Author Profile: Sarah Jeong*, FORBES, https://www.forbes.com/profile/sarah-jeong/#432ebf6436f6 (last visited June 1, 2020).
[30] *See, e.g.*, Jack Crowe, *Newest Member of NYT Editorial Board Has History of Racist Tweets*, NAT'L REV. (Aug. 2, 2018, 11:24 AM), https://www.nationalreview.com/news/sarah-jeong-new-york-times-hires-writer-racist-past/.

- *"White men are bullsh*t."*
- *"#cancelwhitepeople"*
- *"Dumb*ss f***ing white people marking up the internet with their opinions like dogs pissing on fire hydrants."*
- *"Are white people genetically disposed to burn faster in the sun, thus logically being only fit to live underground like groveling goblins."*
- *"Oh man it's kind of sick how much joy I get out of being cruel to old white men."*[31]

The cybermob quickly called for her firing.[32] Unlike other cybermobbing victims, though, Jeong's employer decided not to take action based on the social media reactions.[33]

While these thoughtless Tweets speak volumes about their authors, the statement by Sacco's employer rings true. Otherwise decent people say thoughtless things. In the past, such statements might have made for upset water-cooler conversation.[34] The offender might have been fired and could have sought work elsewhere. At worst, the offender could have moved to a different city, where he or she could have started anew. Cybermobs, however, have ensured that these people's names are forever associated with what might have been a temporary lapse in judgment.

Even worse than the cases described above are those in which the alleged inciting incident did not occur at all. A recent example is the Covington Catholic High School debacle. This cybermobbing episode was sparked by a video depicting what seemed to be a disturbing scene: a

---

[31] Andrew Sullivan, *When Racism is Fit to Print*, N.Y. MAG. (Aug. 3, 2018), http://nymag.com/intelligencer/2018/08/sarah-jeong-new-york-times-anti-white-racism.html (collecting and compiling the controversial Tweets) (altered to obscure profanity).

[32] *Id.*

[33] Jaclyn Peiser, *Times Stands by Editorial Board Member after Outcry Over Old Tweets*, N.Y. TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/business/media/sarah-jeong-new-york-times.html. In August 2019, Jeong resigned her position on the editorial board, after serving less than a year. Brian Stelter, *Reliable Sources: Sarah Jeong Departs NYT Editorial Board*, CNN BUS. (Sept. 27, 2019), https://mailchi.mp/cnn/rs-sept-27-2019?e=e237f491cb.

[34] *See* Megan Mcardle, *The Power of Social Media Mobs and the Permanence of the Wreckage They Leave Behind*, GOV'T. TECH. (Aug. 23, 2017), https://www.govtech.com/social/The-Power-of-Social-Media-Mobs-and-the-Permanence-of-the-Wreckage-They-Leave-Behind.html.

crowd of MAGA-hatted[35] teenagers harassing a Native American veteran, Nathan Phillips, and engaging with a group of Black Israelites, at the Lincoln Memorial.[36] Nicholas Sandmann, a 15-year old student, was prominent in this video and appeared to be smirking while obstructing Phillips's path.[37] The video quickly spread through social media and polarized the American public.[38] The news coverage and the accompanying cybermobbing, seemingly jumped to conclusions, based on a combination of the short video and interviews with Phillips who claimed the teenagers had surrounded and harassed him.[39]

The backlash on Twitter was immediate and brutal. High-profile celebrities condemned Sandmann and the other students with incendiary language:

- *"Baby snakes"*[40]
- *"Mocking, condescending, disrespecting, ***HOLE"*[41]
- *"Horrible smug ***wipe"*[42]

At least one celebrity called for the doxing of the children present in the video:

- *"Ps. The reply from the school was pathetic and impotent. Name these kids. I want NAMES. Shame them. If*

---

[35] "MAGA" stands for "Make America Great Again" and was the campaign slogan of President Donald J. Trump. Karen Tumulty, *How Donald Trump Came Up with "Make America Great Again"*, WASH. POST (Jan. 18, 2017), https://www.washingtonpost.com/politics/how-donald-trump-came-up-with-make-america-great-again/2017/01/17/fb6acf5e-dbf7-11e6-ad42-f3375f271c9c_story.html.

[36] Wootson Jr et al., *"It was Getting Ugly": Native American Drummer Speaks on his Encounter with MAGA-hat-wearing Teens*, WASH. POST (Jan. 22, 2019, 3:47 PM), https://www.washingtonpost.com/nation/2019/01/20/it-was-getting-ugly-native-american-drummer-speaks-maga-hat-wearing-teens-who-surrounded-him/.

[37] *Id.*

[38] *Id*.

[39] *See id.*

[40] Jim Carrey (@JimCarrey), TWITTER (Jan. 22, 2019, 2:04 PM), https://twitter.com/JimCarrey/status/1087788108488167424.

[41] Debra Messing (@DebraMessing), TWITTER (Jan. 21, 2019, 12:57 PM), https://twitter.com/DebraMessing/status/1087454142187081729 (altered to obscure profanity).

[42] Rosie O'Donnell (@Rosie), TWITTER (Jan. 19, 2019, 1:52 PM), https://twitter.com/Rosie/status/1086743221802336258 (comparing a picture of Sandmann to a picture of white segregationists assaulting a group of black men) (altered to obscure profanity).

> *you think these ****ers wouldn't dox you in a heartbeat, think again."*[43]

However, further videos did not corroborate Phillips's claims and the cybermob's narrative.[44] First, the teenagers apparently were not harassing Phillips and instead were using school cheers to drown out hateful slurs thrown at them by other protestors.[45] Second, although Phillips had an alternate path to the Lincoln Memorial, Phillips approached Sandmann and the other students with the intention to confront the group.[46]

By the time the full story was uncovered, the damage had been done. Sandmann had been doxed and received numerous death threats and media scorn.[47] His school, Covington Catholic High School, was closed for several days due to bomb threats.[48] Sandmann has since sued numerous news outlets that repeated Phillips' misleading statements.[49] A charitable observer might note that some of the criticisms of Sandmann were based in reality, given that he wore a politically divisive hat in public and arguably thrust himself into the spotlight. But the same cannot be said of the next two cases involving mistaken identity.

---

[43] Kathy Griffin (@Kathygriffin), TWITTER (Jan. 20, 2019, 5:05 AM), https://twitter.com/kathygriffin/status/1086927762634399744?lang=en (altered to obscure profanity).

[44] *See, e.g.*, Michael E. Miller, *Viral Standoff Between a Tribal Elder and a High Schooler is More Complicated Than it First Seemed*, WASH. POST (Jan. 22, 2019, 3:56 PM), https://www.washingtonpost.com/local/social-issues/picture-of-the-conflict-on-the-mall-comes-into-clearer-focus/2019/01/20/c078f092-1ceb-11e9-9145-3f74070bbdb9_story.html.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Dan Griffin, *No Danger Found at Diocese of Covington; FBI Investigates Packages*, WLWT5 ABC NEWS (Jan. 23, 2019, 11:34 PM), https://www.wlwt.com/article/authorities-respond-to-reports-of-suspicious-package-at-diocese-of-covington/26015081; John London, *Prosecutor: Hundreds of Threats Made Against Covington Catholic After DC March Firestorm*, WLWT5 ABC NEWS (Jan. 23, 2019, 5:31 PM), https://www.wlwt.com/article/prosecutor-hundreds-of-threats-made-against-covington-catholic-after-dc-march-firestorm/26014571#.

[49] Cameron Knight, *Sandmann Files 5 More Defamation Lawsuits Against Media Outlets*, CINCINNATI ENQUIRER (Mar. 3, 2020, 11:51 AM), https://www.cincinnati.com/story/news/2020/03/03/sandmann-files-5-more-defamation-lawsuits-against-media-outlets/4938142002/. *See*, *e.g.*, Sandmann v. WP Co. LLC., 401 F. Supp. 3d 781 (E.D. Ky. 2019).

After the Boston marathon was bombed on April 15, 2013, a group of individuals gathered on Reddit to find the perpetrator.[50] The group created a subreddit[51] titled "/r/findbostonbombers" and began speculating about the bomber's identity using information found online and in the news.[52] They identified a college student named Sunil Tripathi. Tripathi had been missing since March 16, 2013[53] and resembled "Suspect #2." The F.B.I. had been working with his family to find him.[54] After the group spread its conclusion on Reddit, Tripathi's sister received 58 phone calls on April 19 from reporters looking for a scoop, and from others with less kind words.[55] The Facebook page "Help Us Find Sunil Tripathi," which had previously been set up by Sunil's family when he went missing in mid-March, had to be taken down after users posted a high volume of threatening messages.[56] However, it turned out that Tripathi was missing not because he was hiding, but because he had died before the bombings even took place.[57]

In another case of mistaken identity, Robert Cantrell was wrongfully accused of murdering a seven-year-old black girl named Jazmine Barnes. Barnes had been murdered in a drive-by shooting on the same day that Cantrell had arrested for a separate robbery.[58] Cantrell, who was in custody for the robbery-evasion, resembled the initial composite

---

[50] Alexander Abad-Santos, *Reddit's "Find Boston Bombers" Founder Says "It Was a Disaster" but "Incredible"*, ATLANTIC (Apr. 22, 2013), https://www.theatlantic.com/national/archive/2013/04/reddit-find-boston-bombers-founder-interview/315987.

[51] "Subreddits are subsidiary threads or categories within the Reddit website. They allow users to focus on a specific interest or topic in posting content that gets voted up or down by relevance and user preference." *Subreddit*, TECHOPEDIA, https://www.techopedia.com/definition/31607/subreddit (last visited Aug. 2, 2019).

[52] Abad-Santos, *supra* note 50.

[53] Jay C. Kang, *Should Reddit Be Blamed for the Spreading of a Smear?*, N.Y. TIMES MAG. (July 25, 2013), https://www.nytimes.com/2013/07/28/magazine/should-reddit-be-blamed-for-the-spreading-of-a-smear.html.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] Jess Bidgood, *Body of Missing Student at Brown is Discovered*, N.Y. TIMES (Apr. 25, 2013), https://www.nytimes.com/2013/04/26/us/sunil-tripathi-student-at-brown-is-found-dead.html.

[58] *Inmate Once Wrongfully Accused of Killing 7-Year Old Jazmine Barnes Killed Himself Behind Bars*, ABC 13 NEWS (July 20, 2019), https://abc13.com/man-wrongfully-accused-of-killing-jazmine-barnes-kills-himself/5428054/.

sketch of Barnes's murderer, an unknown white man with blue eyes.[59] Cantrell was then accused online of the Barnes murder and the incident was labeled a hate crime, drawing the attention of millions of Facebook and Twitter users.[60] Online activist, Shaun King tweeted Cantrell's mug shot to his one million Twitter followers, stating several sources claimed Cantrell was a "racist violent (expletive)."[61] Cantrell's family received death threats.[62] One user threatened Cantrell's niece, stating that "[s]omeone is going to rape, torture and murder the women and children in your family."[63] Investigators cleared Cantrell of any involvement,[64] and two other men were arrested and charged with Barnes's murder. However, the cybermob continued harassing Cantrell and his family.[65] Seven months later, Cantrell killed himself in jail, where he was still imprisoned on the robbery-evasion charge.[66]

B. Defining Cybermobbing and Evaluating its Social Utility

These case studies underscore an important question: Is cybermobbing, on balance, a socially-desirable phenomenon? To answer this question, cybermobbing must first be defined. From the examples above, it is obvious that cybermobbing is similar to cyber harassment and cyberstalking.[67] But while cyber harassment and cyberstalking are often effectuated by a single perpetrator, cybermobbing is a "team sport, with posters trying to outdo each other. Posters compete to be the most offensive, the most abusive."[68] In the case studies above, the victims likely

---

[59] Jessica Willey, *Family of Man Wrongfully Accused by Activist Shaun King in Jazmin Barnes' Shooting Speaks Out*, ABC 13 NEWS (Jan. 8, 2019), https://abc7chicago.com/family-of-wrongfully-accused-man-receiving-violent-threats/5034081/.
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Inmate Once Wrongfully Accused of Killing 7-Year Old Jazmine Barnes Killed Himself Behind Bars*, ABC 13 NEWS, *supra* note 58.
[67] CITRON, *supra* note 16, at 3. Citron defines cyber harassment as "the intentional infliction of substantial emotional distress accomplished by online speech that is persistent enough to amount to a 'course of conduct' rather than an isolated incident" and cyberstalking as "an online 'course of conduct' that either causes a person to fear for his or her safety or would cause a reasonable person to fear for his or her safety." *Id.* By contrast, she describes a cybermob as an online group that turns "[o]nline harassment [into] a team sport." *Id.* at 5.
[68] *Id.*

would have suffered more limited real-world harm had the mob been limited to one or two individuals.

Cybermobbing is distinct from bullying, although the separation is thin.[69] Bullying is traditionally defined as: (1) verbal or physical aggression; (2) repeated over time; (3) which involves a power differential.[70] Cybermobbing seems to easily meet the first criterion, verbal aggression. Further, while the members of the cybermob might be, individually, weaker than the victim, the sheer size of the cybermob may implicate a power differential. So, the third criterion seems satisfied, as well. However, the second, repetition over time, is not. Many cybermobbings are single flare-ups, beginning and ending within a week.[71]

Cybermobbing is distinctive due to its relatively recent origins from social media. No formal definition seems to yet exist, but some have defined it as: (1) a group of persons acting in cyberspace, (2) joining together to hold accountable, (3) a victim or victims, (4) for a real or imagined misdeed or faux pas.[72] However, this definition leaves something to be desired.

Cybermobbing does not require "harassment" of the victim directly. That is, the victim need not receive harassing messages personally from the cybermob. And further, "harass" doesn't fully encompass the real-world harm effectuated by cybermobbing. Many victims have their careers ruined for something entirely unrelated to those careers. Therefore, this Note proposes the following definition as more appropriate: (1) a group of persons acting in cyberspace joining together to; (2) dox, threaten, humiliate, or call for physical or pecuniary harm against; (3) victim or victims; (4) for a real or imagined misdeed or faux pas. Given

---

[69] *See* Klonick, s*upra* note 5, at 1034 (discussing the "cyber" distinction, and its impact on exacerbating bullying, shaming, and harassing behaviors).

[70] *Id* (citing EMILY BAZELON, STICKS AND STONES: DEFEATING THE CULTURE OF BULLYING AND REDISCOVERING THE POWER OF CHARACTER AND EMPATHY 28 (2013) (citing DAN OLWEUS, BULLYING AT SCHOOL: WHAT WE KNOW AND WHAT WE CAN DO 142–52 (1993))).

[71] *See id.* at 1046–50 (examples of online shaming and cyber harassment). However, note that Klonick points out that the permanent nature of the internet allows for the mob's posts to be associated with the victim in internet searches for long periods of time. She distinguishes bullying from social shaming in that the latter seeks to enforce a violation of a social norm. *Id.* at 1034.

[72] Winhkong Hua, *Cybermobs, Civil Conspiracy, and Tort Liability*, 44 FORDHAM URB. L. J. 1217, 1246 (2017) (citing to UrbanDictionary.com *Cybermob*, URB. DICTIONARY (Feb. 24, 2008), https://www.urbandictionary.com/define.php?term=cybermob).

this definition, it is hard to imagine cybermobbing having any utility. However, the real answer is more complicated.

Public shaming and its internet cousin, online shaming via cybermobbing, play a role in social norm enforcement.[73] Online norm enforcement, in turn, is important because it is the "primary social control mechanism of the internet."[74] Online shaming, in this sense, can serve as a replacement for governmental regulation of the internet given the lack of a current online regulatory scheme. Thus, criticizing people for their own words, as happened with Sacco, Jeong, and Gunn, may be socially desirable. Even when such shaming creates real-world harm, such as loss of employment, the social utility of normative role enforcement may outweigh the potentially outsized harm in some instances.

Notwithstanding the possible social utility of online shaming, incidents where cybermobbing involves the doxing of a private individual are always socially undesirable. Cybermobs are able to inflict real-world harm by exposing the victim's private information through doxing. This is problematic for two reasons. First, the dox-inciting incident is often imagined, not real. In instances where there is no misdeed or faux pas, there is no social benefit other than the affirmation that the faux paus *would* have been socially unacceptable—a marginal benefit at best. This is true with the above examples involving Sandmann, Cantrell, and Tripathi. Second, even if the inciting incident actually occurred, the lasting reputational, economic, and dignitary harm suffered by doxing victims normally far outsizes the inciting incident. The damage is permanent.[75] Search engines turn up harmful posts years after the fact,[76] and social media platforms give the cybermob a mechanism to easily reach millions of users.[77] Therefore, cybermobbing via doxing has a net-negative impact on society due to its tendency to inflict irreparable harm unrelated to purportedly-violated social online norms. As explained in Section IV, however, the proposed Doxing Notice and Takedown Act preserves many of the positive aspects of online shaming, while deterring the drawbacks of doxing.

---

[73] *See* Klonick, s*upra* note 5, at 1044.
[74] *Id.*
[75] CITRON, *supra* note 16, at 4 (noting that using the internet to harass or stalk extends the life of such behavior).
[76] *Id.*
[77] *Id.* at 5.

III. Victims Cannot Recover Against Cybermobs

Under current law, cybermobbing victims are generally unable to seek adequate relief. Even in the rare event that one is able to make the case for recovery, obtaining it from the mob is impractical and, as explained in Section IV, the CDA limits victims' recourse from ICSPs.[78]

As explained below, under existing law, cybermob victims are blocked from obtaining adequate relief for two reasons. First, an individual mob members' actions generally are not actionable. Second, even if these actions were actionable , or if the victim could otherwise impose some sort of civil conspiracy cause of action,[79] practical difficulties involving internet defendants inhibit recovery.

A. An Individual Member's Cybermob Participation is Likely Not Actionable

Common law torts and applicable statutes are inadequate remedies as private causes of action against individuals in the cybermob. This section analyzes why both common law torts (tortious interference, privacy, defamation, and intentional infliction of emotional distress) and statutory regimes (cyberbullying) fail as satisfactory remedies for cybermobbing via doxing.

i. Tortious Interference is an Insufficient Remedy

Tortious interference with a contract seems, at first, like the best bet for recovery for a recently fired cybermobbing victim. The tort occurs when a person, without privilege, induces or causes a third person not to enter or continue a business relation with another.[80] It requires: (1) the existence of a valid contractual relationship; (2) the defendant's knowledge of the existence of the relationship; (3) the defendant's intentional interference with that relationship; (4) absence of justification; and (5)

---

[78] *See infra* Section IV.

[79] *See* Hua, *supra* note 72, at 1263–64. Hua argues that a civil conspiracy cause of action solves some problems inherent in cybermobbing; namely, the problems of individual non-actionability and personal jurisdiction. *Id.* However, this still leaves the problems of internet anonymity, judgement-proof defendants, and, as Hua points out, the possibility that no true "meeting of the minds" took place. *Id.* at 1263.

[80] 44B AM. JUR. 2D INTERFERENCE § 47 (2019).

damages resulting from the defendant's wrongful interference with the relationship.[81]

At first, the tort seemingly provides a remedy for Gunn and Sacco, who were fired after public pressure was put on their employers.[82] However, it is unclear whether any one mob member's actions would rise to the level of tortious interference in these cases.[83] Collectively, the statements by the mob had the effect of interfering with the contracts in question. However, the victim could likely not point to any one member of the mob, even the loudest member, to prove there would not have been a breach but for his or her activities, which is what is required under the tort.[84] Further, the employer could point to the inciting incident itself as the reason for firing, rather than the public backlash. And lastly, the reputational harm resulting from a cybermobbing might not instantiate itself in the form of a breached contract. So, tortious interference misses the mark.

ii. Remedies for Privacy Torts are also Insufficient

The four privacy torts are also near misses: (1) unreasonable intrusion upon the seclusion of another; (2) publicity that places another in a false light before the public; (3) Public disclosure of embarrassing private facts about another; and (4) appropriation of another's name, image or likeness.[85] Intrusion upon seclusion and public disclosure of embarrassing facts both fail as remedies because the nature of cybermobbing is to generally excoriate the victim for a perceived public faux pas. To establish liability, the plaintiff must demonstrate there was an intrusion upon the plaintiff's physical solitude or seclusion, as by invading his or her home or conducting an illegal search.[86] The intrusion must be offen-

---

[81] These claim elements may vary by jurisdiction. *Id.*(citing e.g., Effs v. Sony Pictures Home Entm't, Inc., 197 So.3d 1243, 1244 n.2 (Fla. 3d DCA 2016)).
[82] *See supra* Section II.
[83] To establish tortious interference with a contract, the plaintiff must show that the defendant actually induced the other party of the contract into breaching it. *See, e.g.,* Maricultura Del Norte, S. de R.L. de C.V. v. Umami Sustainable Seafood, Inc., 769 Fed.Appx. 44, 55 (2d Cir. 2019) (affirming dismissal of tortious interference because plaintiff did not prove "that there would not have been a breach but for the activities of defendants.").
[84] *Id.*
[85] *See generally* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). The last type, appropriation, is obviously not an appropriate remedy and is not discussed further.
[86] 77 C.J.S. *Rights of Privacy and Publicity* § 24 (2020).

sive to a reasonable person.[87] Sandmann was videotaped in a public place, the Lincoln Memorial, so he had no expectation of privacy.[88] Sacco, Jeong, and Dunn were criticized for publicly-posted Tweets, so there is again no argument for unreasonable intrusion. Lastly, Cantrell's arrest information and mugshot were materials of public record.[89] The only case that is even close is Sunil Tripathi's, whose family maintained a Facebook page dedicated to finding him.[90]

iii. False Light Publicity and Defamation Torts are Impracticable Solutions

False light publicity also likely fails as a realistic remedy.[91] Many victims—like Sacco, Jeong, and Dunn—were not put in a false light; they were criticized for their own words. And victims who *were* put in a false light, like Sandmann, Tripathi, and Cantrell, must still establish that the defendants "had knowledge or acted in reckless disregard as to the falsity of the publicized matter and false light in which the [victim] would be placed."[92]

Defamation is similar to false light publicity in that it also falls short as a catch-all solution to cybermobbing. The reach of defamation is quite limited because of First Amendment concerns.[93] The tort generally requires: (1) a false and defamatory statement concerning another; (2) an unprivileged publication to a third party; (3) fault amounting to at least

---

[87] *Id.*

[88] *See supra* Section II. Although Sandmann could argue that the disclosure of his name by being doxed was a breach of privacy, he would be unable to pursue the cybermob for the reasons stated *infra* Section III(B).

[89] *For Immediate Release*, MONTGOMERY CTY. (Dec. 31, 2018), http://www.mctxsheriff.org/news_detail_T6_R407.php (last visited Apr. 24, 2020).

[90] *See* Kang, *supra* note 53 (discussing threatening messages posted to the family's Facebook page).

[91] *See generally* 6 AM. JUR. PROOF OF FACTS 3D 585 (originally published in 1989).

[92] RESTATEMENT (SECOND) OF TORTS § 652E(b) (AM. LAW. INST. 1965).

[93] New York Times v. Sullivan, 376 U.S. 254, 279-80 (1964) (holding the First Amendment bars public officials from recovering for defamatory remarks relating to their "official conduct" unless they can prove the statements were made with "actual malice"); Curtis Pub. Co. v. Butts, 388 U.S. 130 (1967) (extending "actual malice" requirement to public "figures," not just public "officials."); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (holding private figures must also establish "actual malice" when seeking "presumed" or "punitive" damages); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985) (narrowing Gertz v. Robert Welch, Inc. by only requiring private figures to prove actual malice to establish presumed damages when defamatory remarks relate to matters of public interest).

negligence on the part of the publisher; and (4) either actionability of the statement irrespective of special harm or the existence of special harm cause by the publication.[94]

Some authors suggest defamation as a measure against cybermobbing,[95] but this stance overstates the reach of defamation liability. The first element presents an insurmountable sticking point for most victims of cybermobbing because statements made by the cybermob are often true.[96] Even when such statements cast the victim in a false light, they generally constitute assertions of opinion, which, by definition, cannot be false. As illustrated by the dismissal of Sandmann's defamation suit, courts generally agree that such attacks on victims are "nonactionable opinion."[97] Recovery is further complicated when the plaintiff is a public figure.[98] These impediments make defamation an unsatisfying option for cybermobbing victims.

---

[94] These elements are based on Kentucky law. *See* Sandmann v. WP Co. LLC., 401 F. Supp. 3d 781, 787 (E.D. Ky. July 26, 2019) (applying Kentucky law). While the exact elements differ state to state, each state has some requirement that the statement be false and defamatory. *See, e.g.*, 128 AM. JUR. TRIALS 1, ch.II.A §§ 3–8 (originally published in 2013).

[95] *See* Klonick, *supra* note 5, at 1059–60 (pointing to defamation law as "a relatively effective protection against unhinged shaming," but also noting problems with litigation expenses, judgment-proof defendants, and anonymous defendants). *See also*, Cory Batza, *Trending Now: The Role of Defamation Law in Remedying Harm from Social Media Backlash*, 44 PEPP. L. REV.429, 452–74 (2017). Batza points out many of the difficulties cybermobbing victims face in recovering for defamation; such as the CDA immunity for ISPs, anonymous defendants, and nonactionable opinions. *Id.* at 452–54. Instead of advocating for alternative causes of action for cybermobbing victims, though, Batza argues that courts should reach certain findings in their defamation analyses. *Id.* at 459–74. Namely, Batza argues that the average social media user shouldn't be considered a public figure because of his or her use of the Internet, even for a limited purpose, and that mob shaming should not be considered a matter of public concern. *Id.*

[96] *See, e.g.*, *infra* Section II.a.

[97] *See Sandmann*, 401 F. Supp. 3d at 791–94 (dismissing defamation claims as not actionable because the statements did not specifically reference Sandmann and/or did not state or imply "actual, objectively verifiable facts", and because the social media scorn was beyond the four corners of the written communication at issue). Sandmann presumably did not sue individual Twitter users because the Tweets directed at him would similarly be considered nonactionable.

[98] *See, e.g.*, 6 AM. JUR. PROOF OF FACTS 3D 585, *supra* note 91, at § 11 (in jurisdictions that make the private/public distinction, a plaintiff who is a public figure must make a showing of "actual malice" by the defendant).

iv. Recovery Under Intentional Infliction of Emotional Distress is also Difficult

As an alternative to defamation, some authors point to intentional infliction of emotional distress (IIED).[99] However, recovering under IIED can be incredibly difficult.[100] Plaintiffs must prove: (1) extreme and outrageous conduct with either the intention of, or reckless disregard for, causing emotional distress; (2) the suffering of severe or extreme emotional distress; and (3) actual or proximate causation.[101] IIED is not a workable solution because it is strongly disfavored in the law.[102] Only the most egregious conduct is sufficient to satisfy the first element.[103] Posting mean things on the internet likely does not qualify. So, IIED, like other common law torts, is an inadequate remedy for cybermobbing.

v. Current Statutory Regimes Provide Insufficient Remedies

Current statutory protections, such as cyberbullying statutes, are also insufficient. While some of the conduct described above certainly fits with a conventional understanding of the term "bullying," such statutes do not protect cybermobbing victims. While states have methods of prohibiting bullying and cyberbullying, they only protect students and children, not adults.[104] Additionally, many of these statutes are only "model acts," which do not necessarily carry the full force of law.[105] Further complicating things is the fact that Congress has not acted directly on cyberbullying and the laws that do exist do not create private rights of action. Cyberbullying statutes do not fully address the problem of cybermobbing.

---

[99] *See* Klonick, *supra* note 5, at 1059–60; Gallardo, *supra* note 2, at 731.
[100] 136 AM. JUR. 3D *Recognition of IIED* § 2 (2013) (describing conduct warranting liability under this tort as "a very small slice of human behavior").
[101] *Id.* at § 4.
[102] Andrews v. Staples the Office Superstore East, Inc., 2013 WL 3324227, at *15 (W.D. Va. July 1, 2013).
[103] *See, e.g.*, Medcalf v. Walsh, 938 F. Supp. 2d 478, 488 (S.D. N.Y. Apr. 9, 2013) ("Only the most egregious conduct has been found sufficiently extreme and outrageous to establish this tort").
[104] *See, e.g.*, Minn. Stat. § 121A.031 (defining bullying as harmful conduct that involves "an actual or perceived imbalance of power between the *student* engaging in prohibited conduct . . . .") (emphasis added); Cal. Ed. Code § 48900 (similarly using the language "pupil" to define bullying).
[105] *Laws, Policies, & Regulations*, STOP BULLYING.GOV, https://www.stopbullying.gov/laws/index.html (last reviewed Jan. 7, 2018).

B. Even if a Cause of Action Fits, Practical Difficulties Bar Recovery

Assuming the victim had a meritorious claim, additional practical issues would bar recovery. Oftentimes, the mob is composed of anonymous or pseudonymous members, so the victim does not know who to sue. But even if the victim can correctly identify defendants, two more issues appear. First, members of the mob may be judgment-proof. Second, the sheer number of people involved in most cybermobs makes it impracticable to identify, serve, and enforce a judgment on all or any of them. The amount of resources required to do so would be prohibitive. Therefore, the victim is all but barred from suing individual mob members. As explained below, the victim cannot simply turn to the online platform, the "ICSP," for relief, either.

IV. The Communications Decency Act Does Not Deter Cybermobbing and Should Be Supplemented By the Doxing Notice and Takedown Act

ICSPs are immune from liability for cybermobbings under the CDA.[106] Section 230 of the CDA clarifies that ICSPs do not become "publishers" of material when they exercise "Good Samaritan" blocking and screening of offensive material.[107] Section 230 has been interpreted broadly, preventing ICSP liability for essentially all user postings except for child pornography, intellectual property violations, and other select types of content.[108] After summarizing the history of the CDA in subsection A of Section IV, subsection B argues that Congress should amend the CDA and pass the Doxing Notice and Takedown Act ("DNTA"), the sample legislation proposed by this Note and included in Appendix A. Subsection C walks through the sample legislation and explains why it is consistent with the First Amendment.

---

[106] 47 U.S.C. § 230 (2018).
[107] *Id.*§ 230(c).
[108] Hassell v. Bird, 420 P.3d 776, 793 (Cal. 2018); KATHLEEN ANN RUANE, CONG. RESEARCH SERV., LSB10082, HOW BROAD A SHIELD? A BRIEF OVERVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT 2 (2018), https://fas.org/sgp/crs/misc/LSB10082.pdf; Matt Laslo, *The Fight Over Section 230—and the Internet as We Know It,* Wired (Aug. 13, 2019, 3:18 PM), *https:*//www.wired.com/story/fight-over-section-230-internet-as-we-know-it/.

A. History of the Communications Decency Act

The CDA was passed as an amendment to the Telecommunications Act of 1996.[109] Specifically, the "Good Samaritan" provision of the CDA was a reaction to *Stratton Oakmont, Inc. v. Prodigy Services Co*,[110] where the defendant, Prodigy, was penalized for screening materials posted to its site to make it more family-friendly.[111] The court held that, by screening the posts, Prodigy had made itself a "publisher" of the posts and thus, was liable for any defamatory remarks it failed to exclude.[112] Under this reasoning, Prodigy could have only avoided publisher liability if it allowed users to post freely without screening. Fearing the twisted incentive created by the *Stratton Oakmont* court, Congress passed the "Good Samaritan" provision of the CDA.[113] The section reads:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> No 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.
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable,

---

[109] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 47 U.S.C.).

[110] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995); H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) (stating one of the purposes of § 230 was to "overrule Stratton Oakmont v. Prodigy"). *See also* Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility? Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 247 (2007); Gallardo, *supra* note 2, at 733–35.

[111] *Stratton Oakmont*, 1995 WL 323710 at *2.

[112] *Id.* at *4.

[113] H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) (stating one of the purposes of 230 was to "overrule Stratton Oakmont v. Prodigy."). *See* also Medenica & Wahab, *supra* note 110, at 249–50; Gallardo, *supra* note 2, at 734–35.

whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[114]

In addition to overruling *Stratton Oakmont*, the CDA's § 230 was intended to generally protect the growth and expansion of the internet, preserve a vibrant free market unfettered by regulation, encourage technological development, and "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[115]

The Fourth Circuit, in *Zeran v. Am. Online*, was the first appellate court to apply § 230.[116] Beyond laying out the elements an ICSP must prove to avoid liability using the § 230 carveout,[117] the *Zeran* court controversially went one step further. The *Zeran* court held that § 230 immunity applied to all claims not explicitly excluded in the CDA statute.[118] Since then, courts have used the CDA to bar ICSP liability for defamation, employment torts, negligent misrepresentation, cyberstalking, and breach of contract.[119] Thus, despite the legislative purpose provision in § 230(b) seemingly endorsing the punishment of online harassment, courts have broadly interpreted the Good Samaritan immunity provision to prevent ICSP liability for such harassment.[120]

B. Congress Should Augment the Communications Decency Act by Passing the Doxing Notice and Takedown Act

Section 230 of the CDA is far from universally loved. Many argue that it creates similar incentives to the *Stratton Oakmont* court's holding, such that ICSPs are encouraged to leave content unfiltered in

---

[114] 47 U.S.C. § 230(c) (2018).
[115] *Id.* § 230(b).
[116] Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).
[117] *Id.* at 328–35.
[118] *Id.* at 330–34; *see also* Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How Zeran v. America Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L. J. 583, 585 n.14 (2008) (collecting cases) .
[119] Ziniti, *supra* note 118, at 585. *But see* Doe v. Internet Brands, Inc., 824 F.3d 846, 854 (9th Cir. 2016) (holding that § 230 does not protect an ISP against a failure-to-warn claim).
[120] *See* Ziniti, *supra* note 118, at 585.

order to avoid publisher-liability and unnecessary cost.[121] Some legal commentators assert that the CDA section should nonetheless be left untouched.[122]

Other spectators disagree.[123] Proposed solutions include: a flat-out repeal of the CDA, [124] amending the CDA and imposing notice and take-down regime for defamatory statements,[125] and free-market solutions.[126] While many of these proposals have merit, this Note proposes that the best solution would be legislation that imposes a notice and takedown regime for posts that dox private individuals. This proposed statute would be consistent with the original Congressional intent behind the CDA and would preserve many of the benefits of online shaming, while resulting in the optimal amount of information being disseminated online.

i. The DNTA is Consistent With the Legislative Intent Behind the CDA

Courts have interpreted the CDA to generally immunize ICSPs from liability for any harm caused on their platforms. [127] This statutory interpretation departs from the original legislative intent behind the CDA, which specifically addressed ICSP-publisher liability for attempts to block violent or obscene sexual material.[128] Congress should amend the CDA and pass the DNTA to return to the original legislative intent behind the CDA.

Currently, the CDA is inadequate to combat cybermobbing. Further, addressing cybermobbing is likely beyond the scope of the CDA, as the CDA was passed to combat defamation. Defamation is distinct from cybermobbing for several reasons. First, publisher liability for defama-

---

[121] Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003).
[122] *See generally* Ziniti, *supra* note 118.
[123] *Id.*
[124] *See* Matthew G. Jeweler, *The Communications Decency Act of 1996: Why § 230 Is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers,* 8 U. PITT. J. TECH. L. & POL'Y 1, 1 (2007).
[125] *See* Medenica & Wahab, *supra* note 110, at 239.
[126] Gallardo, *supra* note 2, at 741–43.
[127] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).
[128] Communications Decency Act of 1996, Pub. L. No. 104–104, 110 Stat. 138 (1996) (codified as amended in scattered sections of 47 U.S.C.); *Stratton Oakmont*, 1995 WL 323710, at *1 (superseded by statute, Communications Decency Act, 47 U.S.C. § 230, as recognized in Shiamili v. Real Est. Grp. of N.Y., Inc., 952 N.E.2d 1011 (N.Y. 2011)).

tion far predates the advent of the internet.[129] Second, defamation relates to a unique sort of harm, whereas cybermobbing is linked to a more general, extensive harm. Finally, a defamer is not reliant on an online publisher or platform to defame a plaintiff. In contrast, a cybermobbing incident cannot occur without a social media platform. Further, cybermobs are uniquely enabled by the "low-cost, anonymous, instant, and easy access to the internet" made possible by social media sites.[130] In this sense, cybermobbings could be analogized to other torts; the ease of cybermobbing could reflect a "defect" by the ICSP under product liability[131] or negligent entrustment of a chattel if property is misappropriated while using the platform.[132] Because of these differences from defamation, the CDA is not adequate to frustrate cybermobbing.

The CDA is one of the most consequential laws governing the internet, but most of the modern internet and its modern problems—including cybermobbing— did not exist when the CDA was passed in 1996.[133] Thus, Congress could not have anticipated provider immunity for cybermobbing within the CDA, because the phenomenon had not yet occurred. Although proponents of the CDA could argue that § 230(b) was intended to establish immunity against unforeseen types of harm in order to foster the growth of the internet,[134] they would need to ignore, or at least deemphasize, other language in § 230, which notes the policy goals

---

[129] *See* 6 AM. JUR. PROOF OF FACTS 3D 585, *supra* note 91 (discussing defamation cases predating the internet).

[130] Klonick, *supra* note 5, at 1031 (noting that this easy access "has eviscerated whatever 'natural' limits there were to public shaming and has served to amplify its effects.").

[131] Users are far more likely to send hateful and incendiary messages when using an online platform. *See* CITRON, *supra* note 16. One could argue that the failure of an ICSP to take this into account when constructing and maintaining its platform could be considered a "defect."

[132] RESTATEMENT (SECOND) OF TORTS § 308 (1965) (defining the tort of negligent entrustment). *But cf. Doe*, 347 F.3d at 661 (rejecting this theory when ISP hosted website which sold videos of underage male athletes).

[133] "When the most consequential law governing speech on the internet was created in 1996, Google.com didn't exist and Mark Zuckerberg was 11 years old." Daisuke Wakabayashi, *Legal Shield for Websites Rattles Under Onslaught of Hate Speech*, N.Y. TIMES (Aug. 6, 2019), https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html.

[134] The policy section found in 47 U.S.C. § 230(b) (2018) provides that:

> It is the policy of the United States—
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

of deterring of "harassment by means of computer."[135] In short, the DNTA is not a radical proposition; it is consistent with what the legislature originally intended and would bring the CDA more squarely into the 21st century.

ii. Public Policy Supports a Change From Total Immunity

There are significant public policy arguments that support a change to the current CDA regime. The CDA allows cybermobs to use social media platforms to cause damage that would otherwise be considered tortious if done through a different medium or if effectuated by one individual acting alone.[136] Even worse, it leaves ICSPs with no incentive to prevent cybermobbings. As explained by then-Circuit Judge Frank Easterbrook, if § 230(c)(1) "blocks civil liability when web hosts and other Internet service providers (ISPs) refrain from filtering or censoring the information on their sites,"[137] then:

> § 230(c) as a whole makes ISPs indifferent to the content of information they host or transmit . . . . As precautions are costly, not only in direct outlay but also in lost revenue from the filtered customers, ISPs may be expected to take the do-nothing option and enjoy immunity under

---

> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
>
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
>
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
>
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

[135] *See id.* § 230(b)(5).

[136] *See supra* Section III (discussing the general lack of relief available to cybermobbing victims). For instance, if one individual achieved the result of getting a victim fired, they may be liable for tortious interference with a contract. Change the medium, the number of perpetrators, and the public nature of the wrong, and suddenly relief for the victim disappears.

[137] Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003).

> § 230(c)(1). . . . Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?[138]

Judge Easterbrook resolved the tension between the statute's title ("Protection for 'Good Samaritan' Blocking and Screening of Offensive Material") and its text (which protects ICSPs when they fail to block offensive material) by yielding to its text.[139] But, as explained above, the legislative intent behind § 230 supports a finding that CDA immunity should not be all-encompassing.

Concerns with amending the CDA relate to the suppression of online speech. These concerns are held by some of the biggest players in the tech industry, many of whom provided written testimony at a late 2019 House Commerce Committee meeting on § 230 of the CDA.[140] Steve Huffman, the CEO of Reddit, testified that "even small changes to [the CDA] will have outsized consequences for our business, our communities, and what little competition remains in our industry."[141] Huffman maintained that Reddit's self-moderation policy is an adequate measure for content control. Eliminating § 230, he explained, would destroy Reddit's ability to make good-faith content moderation, and even a slight narrowing of § 230 would create an unworkable regulatory burden on small social media sites and would "chill discussion and hurt the vulnerable."[142]

---

[138] *Id.* at 659–60.
[139] *Id* (citing Brotherhood of R.R. Trainmen v. Baltimore & Ohio R.R. Co., 331 U.S. 519, 528–29 (1947)).
[140] *Fostering a Healthier Internet to Protect Consumers: Hearing Before the H. Comm. on Energy and Commerce*, 116th Cong. (2019). For a summary of the hearing and some attendant commentary, *see* Eric Goldman, *Roundup of the House Commerce Committee Hearing on Section 230*, TECH. & MARKETING L. BLOG (Oct. 17, 2019), https://blog.ericgoldman.org/archives/2019/10/roundup-of-the-house-commerce-committee-hearing-on-section-230.htm.
[141] Steve Huffman, Co-Founder and CEO of Reddit, Inc., Testimony Submitted for the Record at U.S. House of Representatives Committee on Energy and Commerce Hearing on "Fostering a Healthier Internet to Protect Consumers" 1 (Oct. 16, 2019), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Huffman_rev.pdf.
[142] *Id* at 3 (comma removed).

Katherine Oyama, a Google representative, gave a similar statement.[143] She stated that, without § 230, any sites that moderate content could be held liable for defamatory statements, which would result in companies either ceasing to filter content, leading to more harmful content, or over-filtering content, leading to suppression of political speech.[144]

Concerns about the CDA's protection of speech are not uncommon.[145] As Elliot Harmon, a director at the Electronic Frontier Foundation, stated:

> If lawmakers weakened Section 230, they wouldn't just be threatening those spaces—they would risk kicking some people completely off the internet. Without Section 230, platforms would effectively have to determine the risk of a user before that user would ever be allowed to speak.[146]

These arguments have merit—unfettered internet speech is certainly a priority. However, updating the CDA is, on balance, a better policy than leaving it as is. As a preliminary matter, these statements anticipate a complete abandonment of the CDA, a position not advocated by this Note. If the DNTA became law, the CDA would continue to protect good-faith provider screening of content, but limit total ICSP immunity.

Total ICSP immunity under the CDA is bad policy for two additional reasons. First, the above tech executives' statements only consider the suppression of speech caused by over-screening content; they do not fairly consider the speech that is discouraged by under-screening. For example, providers' failure to screen content inevitably results in harassment. Users facing such harassment may be intimidated into not participating, which reduces the quantity and quality of online speech. As Danielle Keats Citron, a professor of law at Boston University, noted in her testimony:

---

[143] *See generally* Katherine Oyama, Global Head of Intellectual Property Policy, Google, Inc., Written Testimony for U.S. House of Representatives Committee on Energy and Commerce Hearing on "Fostering a Healthier Internet to Protect Consumers" (Oct. 16, 2019), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Oyama.pdf.

[144] *Id.* at 4–5.

[145] Elliot Harmon, *Changing Section 230 Would Strengthen the Biggest Tech Companies*, N.Y. TIMES (Oct. 16, 2019), https://www.nytimes.com/2019/10/16/opinion/section-230-freedom-speech.html.

[146] *Id.*

> More often, targeted individuals are women, women of color, lesbian and trans women, and other sexual minorities. They do not feel safe on or offline. They experience anxiety and severe emotional distress. Some victims move and change their names. In the face of online assaults, victims have difficulty finding employment or keeping their jobs because the abuse appears in searches of their names. Online abuse not only makes it difficult to make a living, but it silences victims. Targeted individuals often shut down social media profiles, blogs, and accounts.[147]

Second, total provider immunity, as § 230 currently provides for, enables cybermobbings, which have a net-negative social impact when they involve doxing private individuals. Cybermobs often obfuscate the truthfulness of an individual's perceived social faux paus, which limits social utility stemming from harassment of an individual. The cybermob's pursuit of doxing based on a particular incident has significant consequences for victims, such that victims are often fired or otherwise suffer irreparable reputational, financial, or emotional harm unrelated to any social norm they violated. Amending the CDA and passing the DNTA would help address these issues.

C. What is the DNTA and How is it Consistent With the First Amendment

Congress should amend the CDA and pass the DNTA to address the numerous issues referenced in this Note.[148] The proposed legislation borrows from the notice and takedown structure of the Digital Millennium Copyright Act ("DMCA") to create a notice and takedown regime for online posts that dox private individuals.[149] The DNTA also borrows some principles from defamation law, but relies on doxing-based liability, rather than publisher liability, for defamation.

---

[147] Danielle Keats Citron, Professor of Law, Boston University School of Law, Prepared Written Testimony and Statement for the Record for U.S. House of Representatives Committee on Energy and Commerce Hearing on "Fostering a Healthier Internet to Protect Consumers" 7 (Oct. 16, 2019) (internal citations omitted), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Citron.pdf.

[148] For the DNTA to be effective, the CDA must be amended as shown in Appendix A, where the text of the DNTA is also available. *See infra* Appendix A.

[149] *See generally infra* Appendix A; 17 U.S.C. § 512 (2018) (detailing the notice-and-takedown regime under the DMCA).

If a person discovers his or her personal information online, the DNTA allows that person to contact the ICSP to request the information be taken down.[150] The ICSP must have a publicly-available channel in which to receive such requests.[151] Upon receiving a request, the ICSP must take down the offending post within twelve hours, provided that the request meets the statutory guidelines.[152] At this point, the person who posted the information may provide counter-notification alleging specific facts and circumstances showing that the victim is not a private individual, but instead is a public figure.[153] If the poster provides such a showing, the ICSP must restore the posts unless the victim files for an injunction.[154] The DNTA punishes the misrepresentation of both the nature of the posts and the status of the victim as a private or public individual.[155]

Failure to meet these guidelines results in the ICSP being liable to any doxed victim for statutory damages.[156] From there, the ICSP may seek contribution from those who actively participated in the doxing.[157] This contribution clause deters would-be cybermobbers and, by shifting the risk of judgment-proof defendants onto ICSPs, incentivizes ICSPs to prevent cybermobs from occurring.

The DNTA also borrows from defamation law, in that it is similarly focused on protecting private individuals rather than public figures.[158] This focus on protecting private individuals more easily aligns with the First Amendment,[159] and is an important first step towards addressing cybermobs via doxing. It is also important that the DNTA protects individuals, rather than legal entities such as corporations, partnerships, or limited liability companies, both because (1) legal entities would not suffer the same particular harm that private individuals experience from doxing and (2) ICSPs might become incentivized to

---

[150] *See infra* Appendix A, DNTA § (a)(1)(C).
[151] *See infra* Appendix A, DNTA § (b).
[152] *See infra* Appendix A, DNTA § (a)(2)(A).
[153] *See infra* Appendix A, DNTA § (a)(3)(A).
[154] *See infra* Appendix A, DNTA § (a)(3).
[155] *See infra* Appendix A, DNTA § (c).
[156] *See infra* Appendix A, DNTA § (f).
[157] *See infra* Appendix A, DNTA § (g).
[158] While the distinction between a private and public figure can be unclear in certain situations, courts have generally considered candidates for public office and people who have achieved pervasive fame or notoriety as "public figures." *See, e.g.*, Curtis Pub. Co. v. Butts, 388 U.S. 130, 154 (1967).
[159] *See infra* Section IV(c)(2).

preemptively remove criticism of these entities to avoid liability. Although federal law provides some protection from doxing for certain public employees and others involved in the justice system,[160] separate legislation would need to be considered to protect public figures and public employees. This additional legislation would require a closer examination of First Amendment principles, free speech norms, and underlying policy incentives. However, this analysis is beyond the scope of this Note.

The DNTA prioritizes liability for doxing, rather than defamation, harassment, threats, or other features of cybermobbing, for three reasons. First, is the practicality consideration; doxing is easy to recognize. While harassment and threats may resemble legal criticism in certain instances, doxing and exposing a private individual's personal information never resembles appropriate speech. Second, doxing presents the few First Amendment implications. While First Amendment exceptions exist for threats and harassment,[161] ICSPs may react adversely to potential liability for threatening or harassing posts and preemptively remove actually harmless posts. This chilling effect certainly would have First Amendment concerns.[162] Because posts including personal information are easily recognized, this limits the overinclusive chilling effect of taking down harmless posts. Finally, cybermobs have greater social utility when they cannot dox their victims.[163] The exposure of personal information is what allows cybermobs to inflict real world harm and thus have net-negative social utility. By eliminating doxing, the DNTA allows cybermobs to continue enforcing norms by condemning socially-undesirable behavior while, at the same time, preventing them from imposing long-term reputational, financial, and emotional harm on individuals.

Because the DNTA proposes to amend the CDA and to impose liability for certain types of speech, constitutional questions arise. To pass muster, the DNTA must overcome two hurdles. First, in order to limit ICSP immunity for doxing, the CDA cannot be a First Amendment

---

[160] *See* 18 U.S.C. § 119 (2018) (criminalizing the posting of private information regarding specific individuals performing certain defined duties with intent).
[161] *See infra* Section IV(c)(2).
[162] *See* Note, *Section 230 as First Amendment Rule*, 131 HARV. L. REV. 2027, 2032–47 (2018) (arguing that the First Amendment requires a rule similar to §230) [hereinafter Note, *Section 230 as First Amendment Rule*].
[163] *See, e.g.*, Klonick, *supra* note 5, at 1055–57 (providing example of "manspreading" as a positive use of online shaming, which occurred without a specific doxing or cyber harassment of an individual).

rule. Second, the DNTA itself must pass separate constitutional scrutiny. The DNTA survives both.

i. The CDA is Not Required by the First Amendment and Therefore the DNTA May Allow for Limited Doxing Immunity

Although many judges and academics assume that the First Amendment does not require § 230 of the CDA,[164] some scholars argue otherwise.[165] Specifically, these scholars assert that the First Amendment requires that ICSPs should be shielded from secondary liability for both speech that is protected by the First Amendment and for speech that is not constitutionally-protected, such as defamatory statements.[166] These commentators argue that "the private censorship produced by defamation liability for internet intermediaries cannot be justified by a government interest in defamation law."[167] They further argue that since courts have used the First Amendment to pare back defamation liability,[168] courts could similarly pare back secondary liability for defamation in the online context.[169] This, they argue, leads to an optimal amount of information being disseminated in society.[170] Any contrary rule has the potential for collateral censorship which cannot be justified by any valid governmental interest.[171] However, this argument that the First Amendment requires this secondary liability for ICSPs goes too far, and therefore should fail.

However vital the role of unfettered political speech is, it does not require that ICSPs have complete immunity from secondary liability as a matter of constitutional dictate. Further, this expanded immunity would not result in optimal information creation and distribution. As this Note discusses , cybermobbing has significant and harmful economic externalities. Because the criminalization of doxing private individuals would reduce these externalities, the DNTA would actually increase the social utility of public shaming.

---

[164] Note, *Section 230 as First Amendment Rule*, *supra* note 162, at 2030 (citing, for example, *Batzel v. Smith*, 333 F.3d 1018, 1020 (9th Cir. 2003)).
[165] Note, *Section 230 as First Amendment Rule*, *supra* note 162, at 2035.
[166] *Id.*
[167] *Id.* at 2028.
[168] *See id.* at 2029.
[169] *Id.* at 2046.
[170] *Id.*
[171] *Id.* at 2035–42.

Finally, § 230 protection as a First Amendment requirement faces an uphill battle. As mentioned, the majority of courts and scholars argue that the First Amendment does not require § 230.[172] Rather, § 230 simply "reflects a 'policy choice,' not a First Amendment imperative."[173] Internet speech would be preserved by a far more reasonable rule, rather than one establishing complete immunity for ICSPs. Because the First Amendment does not require § 230, and therefore would not require the complete immunity for ICSPS, the DNTA may reduce immunity for doxing content. Specifically, the DNTA would serve to protect speech while also deterring cybermobbing and ensuring victims harmed by a cybermobbing receive compensation.

ii. The DNTA Survives First Amendment Scrutiny

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech."[174] Protection of free speech is substantial, extending even to "ideas that the overwhelming majority of people might find distasteful or discomforting."[175] However, this protection is subject to numerous exceptions.[176] The DNTA's imposition of liability for statements that dox private individuals is consistent with policies underlying two of these First Amendment exceptions.

First, a close common law analogy to doxing is the tort of publication of private information.[177] Although a publisher of this information would generally be tortiously liable, the First Amendment provides limited immunity for published information that relates to threats to public safety[178] or other matters of public concern.[179] The DNTA aligns with this exception in two ways. First, the proposed DNTA only protects private individuals, not public figures or individuals who "otherwise voluntarily

---

[172] Note, *Section 230 as First Amendment Rule*, *supra* note 162, at 2030 (citing, for example, *Batzel v. Smith*, 333 F.3d 1018, 1020 (9th Cir. 2003)).
[173] Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 421 (S.D. N.Y. Mar. 14, 2001) (citing Zeran v. Am. Online, Inc. 129 F.3d 327, 330–31 (4th Cir. 1997).
[174] U.S. CONST. amend. I.
[175] Virginia v. Black, 538 U.S. 343, 358 (2003) (citing Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting)).
[176] Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("[T]he right of free speech is not absolute at all times and under all circumstances. There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem.").
[177] *See supra* Section III.
[178] Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).
[179] *See generally* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 490 (1975).

entered the public eye because of a particular matter of public concern."[180] Second, the DNTA limits actionable harm to the exposure of a private individual's home address, place of work, school, real name, or similar personal information.[181] For the majority of cases, it is unlikely that the exposure of this information would be considered a matter of public concern. In the event that this private information would be of public concern, then it is likely that no actionable harm has occurred.

The DNTA further conforms to the constitutional boundaries defined by case law implicating First Amendment rights. In *Chaplinsky v. New Hampshire*, the Supreme Court upheld a statute that prohibited using offensive, derisive, or annoying language to deride, offend, or annoy someone lawfully in a public place.[182] The defendant challenged the constitutionality of the statute under the First Amendment after he yelled at a police officer, "You are a God damned racketeer . . . a damned Fascist," in a public place.[183] In affirming the conviction, the Court pointed to an exception to the First Amendment for lewd, obscene, profane, libelous, insulting, or fighting words—"those which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[184] Because the statute was intended to prevent breaches of the peace, it posed no constitutional issue.[185]

Chaplinsky is not a relic of a more genteel past. In 1969, the Court in *Watts v. United States* explained that states may prohibit "true threats" and still be consistent with the First Amendment.[186] In *Black v. Virginia*, a 2003 case, the Supreme Court relied on *Chaplinsky* to uphold a similar statute prohibiting the burning of crosses "with the intent of intimidating any person or group of persons."[187] In short, fighting words, threats, and statements constituting a breach of the peace are not protected by the First Amendment.

While doxing itself might not constitute "fighting words," the activity is certainly used to intimidate and threaten individuals, whether explicitly or implicitly. Having your home address, place of work, school, or name published online, could very reasonably instill fear of

---

[180] *See* DNTA's proposed definition of "private individual," *infra* Appendix A, DNTA § (d)(4).
[181] *Infra* Appendix A, DNTA § (d)(1)(A).
[182] *Chaplinsky*, 315 U.S. at 569.
[183] *Id.*
[184] *Id.* at 572.
[185] *Id.*
[186] Watts v. United States, 394 U.S. 705, 708 (1969).
[187] *Black*, 538 U.S. at 347–48.

bodily harm.[188] Thus, the DNTA likely would not violate the First Amendment because of the carveout for speech which implies threat of bodily harm to individuals, and the DNTA would pass constitutional muster.

V. Conclusion

Cybermobs have a net-negative impact on society when they are able to dox their victims by exposing and publishing private personal information online. They often obfuscate the truth or falsity of underlying incidents and create wildly-outsized consequences for alleged wrongdoers. A victim of cybermobbing is practically barred from seeking justice from the mob using existing causes of action, and the CDA should not be an additional hurdle to recovery. Thus, Congress should amend the CDA and pass the DNTA to impose liability onto ICSPs for cybermobs for doxing private individuals. This would deter online malfeasance and incentivize ICSPs to foster useful and productive online spaces. While the DNTA does not address all of the problems related to online harassment and cybermobbing, its passage would be an initial step in the providing greater protection for users of the modern internet.

---

[188] *See generally* CITRON, *supra* note 16.

Appendix

Appendix A

Amendment to the Communications Decency Act:

"The following paragraph shall be added at the end of subsection (e) as subparagraph (6):

> 'Nothing in this section shall be construed to limit the application of the Doxing Notice and Takedown Act.'"

The Doxing Notice and Takedown Act:

(a) In general

(1) A service provider shall not be liable for monetary, injunctive, or other equitable relief under this Act by reason of storage, at the direction of a user, of messages or statements that reside on a system or network controlled, operated by, or for the service of the provider, if the service provider:
   (A) does not have actual knowledge that such messages or statements on the system or network cause actionable harm;
   (B) upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the messages or statements; and
   (C) upon notification, responds expeditiously to remove or disable access to the messages or statements that are claimed to cause actionable harm.

(2) A service provider shall be liable for monetary, injunctive, or other equitable relief under this Act to a private individual if:
   (A) within 12 hours after receiving notification under paragraph (c), the service provider fails to remove or disable access to messages or statements causing actionable harm in which the private individual is identified; or
   (B) the service provider fails to designate an agent under paragraph (b) and a private individual is subsequently identified by messages or statements causing actionable harm.

(3) The service provider shall not be liable for monetary relief if it restores the messages or statements allegedly causing ac-

tionable harm after a participating individual has filed a counter-notification providing an initial showing that:

(A) the person identified in messages or statements is not a private individual; or

(B) the messages or statements do not cause actionable harm, unless the person identified files for injunctive relief in a court of competent jurisdiction.

(4) If the service provider removes or disables access to messages or statements causing actionable harm in which the private individual is identified within 12 hours after receiving notification and the message or statements are not restored, the private individual may seek monetary relief from participating individuals. The court shall award monetary relief upon finding that the claimant is a private individual and that the messages or statements caused actionable harm.

(5) The service provider shall adopt, reasonably implement, and inform subscribers and users of the service provider's system or network policy that provides for the termination in appropriate circumstances of repeat participating individual subscribers and users from the service provider's system or network.

(b) Designated agent

The limitations on liability established in this section apply to a service provider only if the service provider has designated an agent to receive notifications relating to claims of actionable harm. To designate an agent pursuant to this subsection, the service provider must make the agent's certain contact information available through its service, including on its website in a location accessible to the public.

(c) Elements of notification

(1) **Notification**

To be effective under this subsection, a notification must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(A) a physical or electronic signature of the complaining party or their agent;

(B) identification of the specific messages or statements causing actionable harm or, if there exists too many messages or statements to reasonably be identified by the individual, a representative list of such messages or statements;

(C) information reasonably sufficient to permit the service provider to locate the messages or statements;
(D) information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted;
(E) a statement that the complaining party has a good faith belief that the complaining party is a private individual and that the messages or statements cause actionable harm; and
(F) a statement that the information in the notification is accurate and if applicable, that the filing agent is authorized to act on behalf of the complaining party.

(2) **Counter-notification**
To be effective under this subsection, a counter-notification must be a written communication provided to the designated agent of a service provider that includes substantially the following:
(A) a physical or electronic signature of the participating individual or their agent filing the counter-notification;
(B) identification of the specific messages or statements the participating individual is contesting;
(C) information reasonably sufficient to permit the service provider to locate the messages or statements;
(D) information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the participating individual may be contacted;
(E) a statement containing facts and circumstances which provide an initial showing that the person identified in the messages or statements made by the participating individual is not a private individual or that the messages or statements do not cause actionable harm; and
(F) A statement that the information in the notification is accurate and, if applicable, that the filing agent is authorized to act on behalf of the participating individual.

(3) **Failure to substantially comply**
(A) Subject to clause (B), a notification that fails to comply substantially with the provisions of subparagraph (1) shall not be considered under paragraph (a) in determining whether a service provider has actual knowledge of actionable harm.

(B) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (1) but substantially complies with clauses (B), (C), and (D) of subparagraph (1), clause (A) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Definitions

(1) "Actionable harm" means:
   (A) requesting or revealing, a private individual's, or a private individual's, friend's or family member's, home address, place of work, school name or address, real name, or other personal information, when such information is not a matter of public concern and was not revealed by the private individual on the service provider's system or network; and
   (B) with the intent to harass or threaten a private individual, cause a private individual physical, financial, emotional, or other harm, or place a private individual in reasonable fear of such physical, financial, emotional, or other harm.

(2) "Monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(3) "Participating individual" means an individual who causes a statement or message causing actionable harm to be placed on the service provider's system or network.

(4) "Private individual" means a person other than:
   (A) an individual who holds public office or is a candidate for public office;
   (B) a corporation, partnership, limited liability company, or other legal entity;
   (C) an individual who has achieved pervasive fame or notoriety; or
   (D) an individual who has otherwise voluntarily entered the public eye because of a particular matter of public concern.

(5) "Service provider" means an entity that offers the transmission or routing, or provides connections for digital online communications, between or among points specified by a user, of material

of the user's choosing, without modification to the content of the material as sent or received.

(e) Misrepresentations

Any person who knowingly materially misrepresents under this section:

(1) that messages or statements cause actionable harm,

(2) that messages or statements were removed by mistake or misidentification, or

(3) that a person identified in messages or statements is or is not a private individual,

shall be liable for any damages, including costs and attorneys' fees, incurred by an alleged participating individual, by an individual identified by messages or statements causing actionable harm, or by a service provider, who is injured by such misrepresentation, as a result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be harmful, or in replacing the removed material or ceasing to disable access to it.

(f) Damages

Upon finding a service provider liable under subsection (2) of paragraph (a) of this Act or a participating individual liable under subsection (4) of paragraph (a) of this Act, the court shall award the individual identified in messages or statements monetary damages adequate to compensate the individual, but in no event less than $2,000 per message or statement causing actionable harm.

(g) Right to seek contribution

A service provider found liable under subsection (2) of paragraph (a) of this Act may seek contribution for damages from participating individuals who contributed to the messages causing actionable harm for which the service provider was found liable. Participating individuals are jointly and severally liable for such contribution.

The Potential of Health Data: Exploring Consumer Generated Data and the Big Data Ecosystem

Elijah Roden*

Table of Contents

I. Introduction

In an industry study performed by Aruba Networks, 87% of healthcare companies will have integrated connected devices, typically

* J.D., 2019, The University of Texas School of Law. I would like to thank Charles Silver and Calli Schroeder for their valuable insights and suggestions.

referred to as the Internet of Things ("IoT") by the end of 2019.[1] Healthcare organizations use devices for patient monitoring, maintenance, energy meters, imaging devices, remote operation and monitoring, and location services[2] through internally embedded medical devices,[3] wearable external medical devices,[4] assisting accessories,[5] or stationary medical devices.[6] Beyond healthcare organizations, innovations are appearing in consumer wearable devices, from smart watches[7] and "lifestyle remote[s]"[8] to sleep tracking headbands[9] and stress tracking patches,[10] providing a variety of health benefits. Mobile applications (hereinafter "apps"), like those on the Apple App Store and Google Play, are spreading prolifically as individuals download them to their smartphones, tablets, and smart watches, and the data these apps share with third parties, in many cases, is remarkably similar to the Protected Health Information ("PHI") collected by healthcare organizations. Yet, the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") statutes typically applicable to the management of health information are largely inapplicable to consumer

---

[1] *87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019,* HIPAA J. (Mar. 1, 2017), https://.hipaajournal.com/87pc-healthcare-org.anizations-adopt-internet-of-things-technology-2019-8712.

[2] *Id.*

[3] JASON HEALEY ET AL., ATL. COUNCIL, THE HEALTHCARE INTERNET OF THINGS REWARDS AND RISKS 7 (2015).

[4] James P. Dieffenderfer et al., *Wearable Wireless Sensors for Chronic Respiratory Disease Monitoring,* 2015 IEEE 12TH INT'L CONFE. WEARABLE & IMPLANTABLE BODY SENSOR NETWORKS (BSN) (2015).

[5] Kyu Jin Cho & H. Harry Asada, *Wireless, Battery-less Stethoscope for Wearable Health Monitoring,* PROC. IEEE 28TH ANN. NORTHEAST BIOENGINEERING CONF. 187 (2002).

[6] HEALEY ET AL., *supra* note 3, at 7.

[7] *See* Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J. L. & TECH. 6 (2015).

[8] Rachel Metz, *The Internet of You,* MIT TECH. REV. (May 20, 2014), https:// .technologyreview.com/s/527386/the-internet-of-you.

[9] Sam Draper, *Sleep Trackers Took the Center Stage at the IFA 2018 in Berlin,* WEARABLE TECHNOLOGIES (Sept. 12, 2018), https://.wearable-technologies.com/2018/09/sleep-trackers-took-the-center-stage-at-the-ifa-2018-in-berlin.

[10] Cathy Russey, *These Smart Patches Monitor Your Stress to Help You Lead a Happier, Healthier Life,* WEARABLE TECHNOLOGIES (Nov. 30, 2018), https://.wearable-technologies.com/2018/11/these-smart-patches-monitor-your-stress-to-help-you-lead-a-happier-healthier-life.

medical devices or mobile apps.[11] Ultimately, this inapplicability results in a largely unrestricted market of data processing and data collection, and consumers face extreme difficulty in understanding who processes their data and for what purposes. This danger extends beyond the information gathered at the point of collection as data analytics companies can utilize this information to hone their analytics tools and gain actionable insights into the lives of the subjects of the data they collected. Given the lack of transparency surrounding data collection and processing, the personal information collected in addition to the insights gathered can be used to make decisions affecting consumers who are largely unaware of the decisions being made about them. While some of these decisions may violate the law, the current framework in the United States for data privacy and processing does not provide individuals with sufficient methods to detect such illegal processing, and even if it does, "[T]here are ample pretexts to mask suspect or illegal behavior."[12]

Accordingly, this paper will be divided into three main parts. First, it will explore the general legal framework that applies to information privacy in the United States, the implementation and enforcement of HIPAA and HITECH, and the role that the Federal Trade Commission ("FTC") plays in privacy enforcement. Second, it will illustrate how data sharing occurs in practice, highlighting the degree of third-party involvement, and third, discuss potential real-world consequences of unprotected data collection for users.

II. Privacy Laws and Regulations

Though there has been discussion of a trans-substantive privacy law in the United States,[13] akin to Europe's General Data Privacy Regulation, it is not clear whether or not there will be any forceful push for legislative reform in the area of privacy and cybersecurity. Absent any substantive reform, the United States operates under a sectoral

---

[11] *See* Jennifer R. Flynn, *Break the Internet, Break the Stigma: The Promise of Emerging Technology & Media in Mental Health*, 20 QUINNIPIAC HEALTH L. J. 1, 36 (2017).

[12] Frank Pasquale, *Redescribing Health Privacy: The Importance of Health Policy*, 14 HOUS. J. HEALTH L. & POLICY 95, 108 (2014) [hereinafter Pasquale, *Redescribing Health Privacy*].

[13] Press Release, U.S. Chamber of Commerce, U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Fed. Privacy Law (Feb. 13, 2019), https://.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law.

privacy regime, in which a myriad of laws and regulations apply to different industries in different ways with different protections. The enforcement obligations of these laws are shared or divided between federal agencies, state agencies, and private parties. For example, The Gramm-Leach-Bliley Act ("GLBA") requires financial institutions, or companies that offer consumer financial products and services, to explain their information-sharing provisions and safeguard such data.[14] Enforcement of the GLBA is performed by "the FTC, the federal banking agencies, other federal regulatory authorities, and state insurance authorities . . . ."[15] Similarly for private parties, the Video Privacy Protection Act ("VPPA") enables consumers to pursue a private right of action against a service provider who "knowingly discloses, to any person, personally identifiable information" concerning the consumer's rental history.[16] Although the VPPA enables private rights of action,[17] most privacy statutes rely only on government enforcement. State-specific data privacy laws, like data breach notification laws,[18] are typically ineffective, though California's Consumer Privacy Act of 2018 ("CCPA") may change that inefficacy in 2020.[19] Still, such privacy laws enable state Attorneys General to pursue companies when they breach the representations they make to consumers.[20]

While this sectoral approach enables both personal information and industry to be regulated in a more nuanced way that focuses on particular needs, it can create unnecessary complexity and uncertainty; it

---

[14] *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Feb. 17, 2020).

[15] FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT: A GUIDE FOR SMALL BUSINESS FROM THE FEDERAL TRADE COMMISSION 14 (July 2002), *available at* https://.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

[16] Video Privacy Protection Act § 2(a)(2), 18 U.S.C. § 2710 (2018).

[17] *Id.*

[18] *State Breach Notification Laws*, NAT'L. CONF. ST. LEGISLATURES (Mar. 8, 2020), http://.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[19] *See* Rachael Myrow, *California Rings in the New Year With a New Data Privacy Law*, NPR (Dec. 30, 2019, 9:00 AM), https://.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law.

[20] *See, e.g.*, *Privacy Enforcement Actions*, OFF. CAL. ATT'Y GEN., https://.ca.gov/privacy/privacy-enforcement-actions (last visited Apr. 11, 2020). However, this paper will primarily focus on the FTC as the de facto privacy regulator.

also leaves large areas of the economy unaddressed by statute.[21] There is no federal privacy statute governing data collection by Facebook, Amazon, or Google, nor is there a federal privacy statute on the use of data by merchants, such as Walmart or Target.[22] The lack of a federal statute covering a specific industry does not mean that it is entirely unregulated. Through § 5 of the Federal Trade Commission Act, the FTC enforces privacy policies and advertisements put forth by companies by asserting that violations of representations made by the companies are deceptive trade practices.[23] Mobile apps are usually not covered by a sectoral privacy statute, such as HIPAA,[24] so the regulation of that information falls primarily to the FTC's privacy policy enforcement.

A. HIPAA and HITECH Are Too Narrow in Scope

HIPAA and HITECH and their associated regulations (hereinafter, collectively "HIPAA") contain provisions that apply to the use, processing, and storage of health-related information, even though HIPAA was not initially designed to be a data privacy and security statute.[25] Given the importance of healthcare, the drafters of HIPAA sought to modernize the healthcare profession by enabling the electronic transmission of health information, and in the process of drafting the statute, realized the potential harms inherent in electronic transmissions, causing them to add in privacy and security provisions.[26]

---

[21] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://.cfr.org/report/reforming-us-approach-data-protection.

[22] Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?,* N.Y. TIMES (Nov. 2, 2019), https://.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html.

[23] *See* FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE, LAW ENFORCEMENT, AND RULEMAKING AUTHORITY § II.1 (Oct. 2019), https://.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[24] INST. OF MED. OF THE NAT'L ACADS., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 157–58 (Sharyl J. Nass et al. eds, 2009), https://.ncbi.nlm.nih.gov/books/NBK9578/pdf/Bookshelf_NBK9578.pdf.

[25] Jordan Harrod, *Health Data Privacy: Updating HIPAA to Match Today's Technology Challenges*, SCI. IN THE NEWS, HARV. UNIV. (May 15, 2019), http://.hms.harvard.edu/flash/2019/health-data-privacy.

[26] INST. OF MED. OF THE NAT'L ACADS, *supra* note 24, at 155 (explaining that "[a]lthough privacy protections were not a primary objective of the Act, Congress recognized that advances in electronic technology could erode the privacy of health information, and included the privacy provision in HIPAA").

Under HIPAA, only "individually identifiable health information" that is "(i) transmitted by electronic media, (ii) maintained in electronic media, or (iii) transmitted or maintained in any other form or medium" is PHI under the scope of the Privacy Rule.[27] Individually identifiable health information is information that relates to the condition of an individual, provision of healthcare, or payment of healthcare, which identifies or could potentially identify an individual.[28] However, the Privacy Rule only applies to "covered entities" and "business associate[s]."[29] "If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules."[30]

The Privacy Rule imposes a number of restrictions on the uses and disclosures of PHI. As a general rule, a covered entity may only use or disclose PHI to the individual for the payment or provision of services or to a business associate with appropriate safeguards and contracts.[31] Certain uses or disclosures, however, are prohibited outright, such as the use of genetic information to determine eligibility for benefits, compute a premium, exclude based on preexisting conditions, or make a plan renewal.[32] Similarly, the sale of PHI to a third party is typically prohibited, but a covered entity may do so if they obtain consent that specifically mentions the sale and payment to the covered entity.[33]

Finally, the "Privacy Rule also confers rights on individuals with respect to their PHI."[34] Individuals have a right to receive notice of privacy practices, specifically information regarding "the uses and disclo-

---

[27] 45 C.F.R. § 160.103 (2019).
[28] *Id.*
[29] *Id*. (explaining that Covered Entities are health care providers, health plans, and health care clearinghouses that electronically transmit health information in the course of their normal health care practices. Health care providers include doctors, clinics, psychologists, chiropractors, nursing homes, and pharmacies; a health plan includes health-insurance companies, HMOs, company health plans, and government programs that pay for health care, such as Medicare and Medicaid. A health care clearinghouse includes entities that process nonstandard health information they receive from another entity into a standard form. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity, through benefit management, data aggregation, or cloud hosting services).
[30] *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Apr. 16, 2015), https://.hhs.gov/hipaa/for-professionals/covered-entities/index.html.
[31] 45 C.F.R. § 164.502 (2019).
[32] *Id*.
[33] 45 C.F.R. § 164.508 (2019).
[34] INST. OF MED. OF THE NAT'L ACADS,, *supra* note 24, at 160.

sures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information."[35] Section 164.522 enables individuals to "request restriction of uses and disclosures."[36] However, the covered entity is only required to agree to the restriction if either "the disclosure is for the purpose of carrying out payment or healthcare operations and is not otherwise required by law" or the PHI "pertains solely to a health care item or service for which the individual, or person . . . on behalf of the individual, has paid the covered entity in full."[37]

Though the Privacy and Security Rule in HIPAA initially represented a genuine exercise to protect the confidentiality, availability, and integrity of patient data,[38] technological innovation has exposed the systemic issues within HIPAA's statutory and regulatory framework. The generation and use of health information extends beyond covered entities. Even as mobile devices proliferate through society, the use of apps by users to monitor their own health, increase their exercise performance, or store other sensitive health information still is not covered by HIPAA.[39] Similarly, at-home paternity tests, genetic testing like 23andMe, and online repositories also fall outside the scope of jurisdiction of the Department of Health and Human Services ("DHHS"), which meant that when a woman found the results of her at-home paternity test easily accessible in a directory online, DHHS could do nothing about it.[40] Thus, in its current state, the bulk of privacy regulation for these services falls to the FTC.

---

[35] 45 C.F.R. § 164.520(a)(1) (2019).
[36] 45 C.F.R. § 164.522 (2019).
[37] *Id.*
[38] *See* Karen Colorafi & Bryan Bailey, *It's Time for Innovation in the Health Insurance Portability and Accountability Act (HIPAA)*, JMIR MED. INFORMATICS, Oct.–Dec. 2016, at e34.
[39] Latena Hazard, *Is Your Health Data Really Private? The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U. J. L. & TECH. 447, 457–58 (2017).
[40] Charles Ornstein, *Privacy Not Included: Federal Law Lags Way Behind New Health-Care Technology,* PAC. STANDARD MAG. (June 14, 2017), https://.com/social-justice/privacy-not-included-federal-law-lags-way-behind-new-health-care-technology ; Letter from Kurt T. Temple, Assoc. Deputy Dir. for Reg'l Operations, Dep't. of Health & Hum. Serv., to Jacqueline Stokes (June 5, 2015), *available at* https://.documentcloud.org/documents/2511636-hhs-stokes.html.

B. The Federal Trade Commission as a Catch-All

i. The Federal Trade Commission as a Regulator

The mission of the FTC is to protect "consumers and competition by preventing anticompetitive, deceptive, and unfair business practices" through legal action, promote consumer choice, and increase education while encouraging business activity.[41] The roles privacy and security play in commerce have grown tremendously with the advent of information technology. In the past decade, the FTC has sought to address this through § 5 of the FTC Act, which enforces a company's privacy policies through its ability to regulate unfair and deceptive trade practices.[42] Misleading statements or omissions to consumers, including statements about data privacy, may expose the company to litigation or action from the FTC.[43]

In 2013, for example, the FTC filed suit against LabMD, asserting that a lapse in security measures allowed an employee to install an external peer-to-peer file-sharing program called LimeWire on a company computer.[44] A LabMD company computer's "My Documents" folder contained the personal information of approximately 9,300 consumers and was available to LimeWire.[45] While the FTC ultimately lost on appeal in 2018 for reasons related to the scope of the FTC's order,[46] the case serves as an example of the FTC using its authority to enforce privacy policies against HIPAA-covered entities.[47]

Given the FTC's role in enforcing and administering more than 70 laws, including the Children's Online Privacy Protection Act ("COPPA"),[48] the Fair Credit Reporting Act ("FCRA"),[49] and the Identity

---

[41] *About the FTC*, FED. TRADE COMM'N, https://.ftc.gov/about-ftc (last visited Apr. 2, 2020).
[42] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583, 599 (2011).
[43] Hazard, *supra* note 39, at 464.
[44] *In re* LabMD, Inc., No. 9357 (F.T.C. Nov. 13, 2015) (initial decision), https://.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.
[45] *Id.* at 24–25.
[46] Diane Bartz, *U.S. Agency Loses Appeal Over Alleged LabMD Data Security Lapses*, REUTERS (June 6, 2018, 4:43 PM), https://.reuters.com/article/us-ftc-datasecurity-labmd/u-s-agency-loses-appeal-over-alleged-labmd-data-security-lapses-idUSKCN1J22XD.
[47] Kirk Nahra, *Takeaways from the 11th Circuit FTC v. LabMD Decision,* IAPP (June 7, 2018), https://.org/news/a/takeaways-from-the-11th-circuit-ftc-vs-labmd-decision.
[48] Children's Online Privacy Protection Act § 1302, 15 U.S.C. §§ 6505(a) (2020).

Theft Act,[50] as well as its use of the FTC Act to enforce privacy policies, the FTC is the primary source of regulation for this area.[51] The vast majority of actions brought against companies for violations of their own privacy policies settle, but the settlement agreements nevertheless form a unique body of law and standards, not unlike common law.[52] Companies look to these settlement agreements to guide their actions, enabling the FTC to become the "most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort."[53]

ii. Privacy Policies as Enforcement Mechanisms and Consumer Education

Privacy policies typically focus on the disclosure of how an entity handles consumer data by making certain representations and promises to consumers; unlike an entity's terms of use, which are contracts of adhesion, privacy policies are rarely enforced as contracts.[54] While some laws require certain institutions to provide privacy policies to consumers,[55] the bulk of privacy policies arose through norms and consumer expectations as consumers began to worry about the use of their data online.[56] Privacy policies were a way to maintain self-regulation in light of Congressional attention.[57] In 1998 "only 2% of all websites had some form of privacy policies," and by 2001, "virtually all of the most popular commercial websites had privacy notices, with the number continuing to increase through 2005."[58] Within these policies, the issue is largely a matter of "procedure rather than substance."[59] The question is whether the company properly disclosed its policy to the consumer, not if the company

---

[49] Fair Credit Reporting Act § 601, 15 U.S.C. § 1681 (2018).
[50] 18 U.S.C. § 1001 (2018).
[51] *See Enforcement,* FED. TRADE COMM'N, https://.ftc.gov/enforcement (last visited Apr. 2, 2020).
[52] Solove & Hartzog, *supra* note 42, at 586.
[53] *Id.* at 587.
[54] *Id.* at 589.
[55] *Id.* at 587.
[56] *See id.* at 593–94.
[57] *Id.*
[58] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control of Personal Information?*, 111 PENN. ST. L. REV. 587, 593 (2007).
[59] *Id.* at 597 n.57 (citing Juliet M. Moringiello & William L. Reynolds, *Survey of the Law of Cyberspace: Internet Contracting Cases 2004-2005*, 61 BUS. LAW. 433, 434 (2005)).

can sell or manage data the way it currently does.[60] There are no laws that "regulate the substance of that policy" unless it pertains to a specific type of data or institution, such as HIPAA,[61] COPPA,[62] GLBA,[63] FCRA,[64] and the California Online Privacy Act.[65]

One argument in favor of privacy policies and self-regulation, that the business provides notice and choice to the consumer, is known as the "notice and choice model." The business gives the customer notice by communicating their information disclosure and management practice through their privacy policy. Then, customers can make informed choices about whether to purchase products, visit websites, or trust businesses. This argument favors self-regulation and is inherently skewed in favor of the business. Consumers rarely take the time to read the privacy policies, terms and conditions, or other documents associated with the websites, products, or other services they utilize. In 2008, scholars estimated that it would take the average American 244 hours per year to read all of the privacy policies on the websites they visited.[66] But that was at a time when Facebook only had 100 million users,[67] smartphones were just taking off,[68] and IoT devices had not entered mainstream adoption.[69] Today, in *Contracting for the Internet of Things,* Guido Noto La Diega and Ian Walden highlight that a consumer purchasing a Nest digital thermostat would have to read 13 different legal documents in order "to have a comprehensive picture of the rights, obligations and responsibilities of the various parties in the supply chain."[70] Yet, once Nest discloses information to a third party, the use of the information "will be governed by the third party's privacy policy and not by Nest's privacy documenta-

---

[60] *See id.* at 597.
[61] *See* 42 U.S.C. § 1320d (2018).
[62] *See* 15 U.S.C. §§ 6501–6506.
[63] *See* Gramm-Leach-Bliley Act §§ 501–509, 15 U.S.C. §§ 6801–6809 (2018).
[64] *See* 15 U.S.C. § 1681.
[65] James Graves, *An Exploratory Study of Mobile Application Privacy Policies*, TECH. SCI. (Oct. 30, 2015), https://.org/a/2015103002.
[66] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. L. & POL'Y. FOR INFO. SOC'Y. 543, 563 (2008).
[67] Jefferson Graham, *5 Top Ways Tech Has Changed Since 2008,* USA TODAY (Nov. 13, 2016, 10:32 AM), https://.usatoday.com/story/tech/2016/11/13/5-top-ways-tech-has-changed-since-2008/93527624.
[68] *Id.*
[69] *Internet of Things (IoT) History,* POSTSCAPES, https://.postscapes.com/internet-of-things-history (last visited Apr. 2, 2020).
[70] Guido Noto La Diega & Ian Walden, *Contracting for the 'Internet of Things': Looking into the Nest,* 7 EUR. J. L. & TECH., no. 2, 2016, at 1, 6.

tion."[71] In essence, the resulting web of documents necessary to understand the obligations, responsibilities, and rights of the relevant parties continues to expand. With no limitations on reselling information, the difficulties faced by consumers are highlighted when trying to understand how their data is collected, managed, and protected.

The effort to understand a company's disclosure practices is further complicated by the choice of language used in the policies. Phrases like "affiliates" or "third parties" are littered throughout privacy policies, but "only 7% define them."[72] Conditional language, such as "may" or "might" further obfuscates the meaning and intentions of the privacy policies and presents a challenge in understanding a company's information management practices.[73] Even if a consumer were to develop an adequate understanding of the legal obligations in the web of privacy policies, a review of practices within businesses "points to a sustained failure of business to provide reasonable privacy protections" or comply with their own privacy policies.[74]

In many instances, businesses do not adequately or accurately describe their data-sharing habits in their privacy policies. So even if a consumer were to read them, the consumer would still not be aware of the degree to which information is being shared. In 2013, Privacy Rights Clearinghouse conducted a study of 43 different health and fitness apps. They found that "the majority of the technical practices that [they] considered a risk to users' privacy were not accurately disclosed,"[75] and "39% of the free apps and 30% of the paid apps sent data to someone not disclosed by the developer either in the app or in any privacy policy . . . ."[76] In *Automated Analysis of Privacy Requirements*, researchers ana-

---

[71] NEST, TERMS OF SERVICE § 3(c) (last updated Mar. 5, 2020), https://.com/legal/terms-of-service.

[72] Florencia Marotta-Wurgler, *Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies* 5 (Univ. of Mich. L. Sch., L. & Econ. Workshop, Apr. 16, 2015), *available at* https://.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf.

[73] *Id.*

[74] Haynes, *supra* note 58, at 610.

[75] LINDA ACKERMAN, PRIVACY RIGHTS CLEARINGHOUSE, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY: REPORT TO CALIFORNIA CONSUMER PROTECTION FOUNDATION 22 (July 15, 2013), *available at* https://.org/sites/default/files/pdfs/mobile-medical-apps-privacy-consumer-report.pdf.

[76] *Id.* at 5.

lyzed 9,050 mobile apps, and they found that only 1,461 adhered completely to their policy.[77]

Despite the lack of compliance or legal requirements on the substance of privacy policies, consumers often believe that privacy policies protect them, rather than just disclose specific practices.[78] For example, a report from the Annenberg Public Policy Center of the University of Pennsylvania "found that 75% of consumers believed that just because a site ha[d] a privacy policy, it is not allowed to sell to others the personal information customers disclosed to it."[79] A 2014 poll by Pew Research Center gave the following proposition on a survey: "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."[80] Fifty-two percent of those surveyed responded that this statement was true.[81] This misconception is likely "compounded by the fact that most people skip over the privacy policies or take too little time to read them in enough depth to extract their intended meaning."[82]

Though our current notice and choice paradigm has its benefits, it succeeds only when two conditions are satisfied. First, consumers need to be aware of how their information is being collected, managed, and sold to others. A companies' lack of transparency makes it difficult, and when companies make disclosures, the disclosures are not effective. The disclosures need to be accurate, clear, concise, and readable for the consumer. The complexity of modern data collection practices presents a unique problem, and the challenge of providing enough understandable, accurate information to make an informed decision without exhausting the reader is difficult even for the best drafters. However, thinking about

---

[77] Sebastian Zimmeck et al., *Automated Analysis of Privacy Requirements for Mobile Apps*, 2016 AAAI FALL SYMP. SERIES, 2016, at 286, 294, *available at* https://.aaai.org/ocs/index.php/FSS/FSS16/paper/download/14113/13704.

[78] *See* Haynes, *supra* note 58, at 611.

[79] *Id.* (citing JOSEPH TUROW ET AL., ANNENBERG PUB. POLICY CTR., UNIV. OF PA., OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005)).

[80] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is,* PEW RESEARCH CTR. (Dec. 4, 2014), https://.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is.

[81] *Id.*

[82] Joseph Turow et al., *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015*, 62 J. BROAD. & ELEC. MEDIA 461, 463 (2018).

privacy from the outset can provide huge returns in consumer education, such as through "just-in-time" disclosures.[83]

Second, notice and choice relies on the availability of actual choice in making the decision to utilize the service or not. Companies typically rely on a zero-sum approach to the use of data in which the protection or benefit of one party occurs at the expense of another.[84] In other words, choice, either to enable sharing or restrict certain uses, is viewed as a cost to the company because the company benefits from the ability to use the consumer's data. Companies then predicate the use of the product on the transfer of information in order to maximize their potential gain. When market competition is vibrant, this may not be an issue, as consumers can factor privacy into their choice of companies. However, network effects tend to reduce market competition,[85] and the commercialization of information incentivizes developers to monetize the information they can collect.[86] As more consumers gravitate towards a single platform, device, or app, the bargaining power of consumers to gain substantive privacy protections tends to decrease because the platform's utility increases, and consumers are less likely to leave.[87] Factoring in the lack of transparency in data collection and the lack of bargaining power inherent in the market, it is incredibly unlikely that there will be a substantive change absent any policy changes. In order to see the extent of data collection taking place through the user's apps and devices, many think-tanks, university researchers, and government agen-

---

[83] Just-in-time disclosures are disclosures presented to the consumer at the point of data collection, where the consumer immediately sees information about how the information they enter will be used. This provides information in discrete portions, rather than an aggregated form common in typical privacy policies. *See* FED. TRADE COMM'N, STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15–16 (Feb. 2013), *available at* https://.ftc.gov/sites/default/files/documents/reports /mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[84] *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 3 (2011), http://.industries/wp-content/uploads/2017/10/privacy-by-design.pdf.

[85] *See* Justus Haucap, *Competition and Competition Policy in a Data-Driven Economy*, 54 INTERECONOMICS REV. EUR. ECON. POL'Y 201, 202 (2019); *see also* David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses* 14 (Nat'l Bureau of Econ. Research, Working Paper No. 18783, 2013).

[86] *See* Suketu Gandhi et al., *Demystifying Data Monetization*, MIT SLOAN MGMT. REV. (Nov. 27, 2018), https://.mit.edu/article/demystifying-data-monetization.

[87] *See generally* Haucap, *supra* note 85.

cies conduct studies to shed light on this complex, rapidly expanding ecosystem.

III. Data Collection and Sharing Practices

With the rise in connected devices and software apps that accompany them, data is being collected and distributed as never before. In each smart device, data can be collected from consumers themselves through direct entry, the sensors present in the device, and the network the device is connected to. The sensors present in smart watches may include accelerometers, Wi-Fi sensors, heart rate sensors, GPS, gyroscopes, microphones, barometers, altimeters, cameras, thermometers, compasses, and others.[88] Although the specific collections will vary between app and device, the key data components, in addition to consumer-entered information, can broadly be categorized into five types, as stated by Ann Cavoukian and Abhik Chaudhuri:

> (a) Data collected by edge devices like wireless sensors, IP camera, barcode readers, RFID readers, GPS devices.
> (b) Data at the gateway devices flushed periodically from the edge devices by wired and wireless network
> (c) Data sent to the cloud by gateway devices for analytical processing, storage and application based output
> (d) API based data interchange for various smart service offerings between machine to machines (M2M) and between machines and users
> (e) 'Control' data sent back to the edge devices and sensors for controlling or fine-tuning the context of data gathering.[89]

This data can then be transferred to a number of different systems from the smart watch, including smartphones, devices, computers, and

---

[88] *See* Kyle Wiggers, *Apple Watch Series 4 Can Detect Falls, Take ECGs, and Lead You Through Breathing Exercises,* VENTUREBEAT (Sept. 12, 2018, 10:54 AM), https://.com/2018/09/12/apple-watch-series-4-can-detect-falls-take-ecgs-and-lead-you-through-breathing-exercises.

[89] Abhik Chaudhuri & Ann Cavoukian, *The Proactive and Preventative (3P) Framework for IoT Privacy by Design,* 57 EDPACS 5 (2018).

servers/cloud services.[90] This is further distinguished between proprietary systems of the wearable vendor's own apps and data and third-party systems, which are developed and maintained by external entities to provide specific functionalities.[91]

To fully grasp how difficult it is to follow from a consumer's perspective, it is important to understand how the apps collect data from a technical viewpoint. At a basic level, consumers would expect data to be transmitted from their phones for the performance of the app unless the app is known to be independent. A running app, for example, may send the consumer's location to a server run by the developers or the phone's manufacturer, and from there, use either that location information in conjunction with its own service or a vendor to map the running route, calculate calories burned, and suggest exercise routines for an upcoming race. However, beyond how companies handle consumer data rests the issue of how revealing that data can be for consumers.

A. Information Entered by Consumers Can Be Revealing

After downloading an app, consumers are often prompted to enter account information, shopping habits, or exercise routines, and apps can share this information as allowed by their privacy policy.[92] In 2013, the FTC conducted a study of consumer-generated and controlled data in various health apps that were available to the general public, using twelve apps, two wearables, and one primary device, such as a phone, specifying that it only surveyed data available to the consumer.[93] In reviewing the apps, the FTC discovered data was sent to 76 third parties.[94] For example, one third party received information from four different apps in the study, and one app transmitted data to 18 third parties.[95] While the customer can restrict certain types of data by not giving the app permission,

---

[90] Francisco de Arriba-Pérez et al., *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios,* SENSORS, Sept. 2016, at 1, 5.
[91] *Id.*
[92] *See*, *e.g.*, Zack Whittaker, *Fitness App PumpUp Leaked Health Data, Private Messages,* ZDNET (May 31, 2018, 6:56 PM), https://.zdnet.com/article/fitness-app-pumpup-leaked-health-data-private-messages (describing the data points entered by consumers that were exposed in a breach).
[93] FED. TRADE COMM'N, SPRING PRIVACY SERIES: CONSUMER GENERATED AND CONTROLLED HEALTH DATA (May 2014), https://.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf.
[94] *Id.*
[95] *Id.*

"[P]ermissions generally don't apply to the information users supply directly to the apps, which is sometimes the most personal."[96] As will be seen, consumer-entered information can trigger certain events causing sensitive data to be sent to third parties.

B. Excessive Permissions Can Undermine Privacy

When a consumer installs an app from a marketplace, such as the App Store or Google Play, the app requests certain permissions from the user.[97] App permissions are the privileges an app has to operate within the device, such as when Instagram gains access to a user's photos to upload them.[98] Generally, well-known developers try not to access more than they need for the app's service operations, which may include advertising, voice communication, or payment.[99] For consumers to really understand what the developers intend to use the data for in the app, they would need to turn to the app's privacy policy and its associated documents; but in doing so consumers will run into the same challenges discussed above.

These permissions can vary in the type of data accessed and potential threat levels. Determining permission trends within the two major mobile OS platforms may be accomplished using available research. While Apple and Google make up approximately 96.3% of the smartphone market, 81.5% of devices shipped in 2014 had Android OS.[100] This consolidation is projected to continue as Android takes more of the market.[101] Accordingly, the vast majority of data covers Android

---

[96] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.,* WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[97] *See* David Nield, *How to See Everything Your Apps Are Allowed to Do,* WIRED (July 5, 2018, 7:00 AM), https://.wired.com/story/how-to-check-app-permissions-ios-android-macos-windows.

[98] *Id.*

[99] *See* Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED (Apr. 14, 2018, 7:00 AM), https://.wired.com/story/app-permissions/(discussing Apple and Google app permission guidelines and enforcement with developers).

[100] John Kennedy, *Android and iOS Dominate Smartphone Economy – Own 96.3pc of Overall OS Market,* SILICON REPUBLIC (Feb. 25, 2015), https://.siliconrepublic.com/companies/android-and-ios-dominate-smartphone-economy-own-96-3pc-of-overall-os-market.

[101] Melissa Chau & Ryan Reith, *Smartphone Market Share,* INT'L DATA CORP. (updated Apr. 2, 2020), https://.idc.com/promo/smartphone-market-share/os.

devices,[102] so more research may need to be done to evaluate permission habits within iOS devices. In *Android Permissions Demystified* (2011), the authors explain that Android gives apps access to system resources at the time of installation.[103] Google only recently announced a departure from all-or-nothing permissions for an app, which allows consumers to have more control over permissions given to an app.[104] Android "defines 134 permissions" that are placed into one of the following three threat levels: Normal, Dangerous, and Signature/System permissions.[105] Developers declare the permissions their app will use when they submit it to the app store.[106] The study reviewed 940 apps from the Google Play store, and "identified 323 apps (35.8%) as having unnecessary permissions."[107] Within that subset, "9% of the overprivileged app[s] request unneeded Signature or SignatureOrSystem permissions."[108]

In *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis,* the authors identified 24 apps available on the Google Pixel that pertained to medicine information, dispensing, administration, or prescribing.[109] They analyzed the permissions requested and the data sent from the app.[110] Using the developer self-report on Google Play, the researchers found that the apps requested four permissions that involved a user's private information, stored data, or ability to affect other app operations, such as determining precise location (25% of the apps), reading, and editing device storage (79% of the apps), or receiving the phone's identity, including phone number and network information (29% of the apps).[111] In their

---

[102] *See* Gabriella M. Harari, *Using Smartphones to Collect Behavioral Data in Psychological Science: Opportunities, Practical Considerations, and Challenges*, 11 PERSP. ON PSYCHOL. SCI., Nov. 2016, at 838, *available at* https://.ncbi.nlm.nih.gov/pmc/articles/PMC5572675/pdf/nihms862908.pdf.

[103] Adrienne Porter Felt et al., *Android Permissions Demystified*, CCS' 11 Proc. 18th ACM Conf. Computer & Comm. Security 627, 628 (2011).

[104] Ben Smith, *Project Strobe: Protecting Your Data, Improving Our Third-Party APIs, and Sunsetting Consumer Google+,* GOOGLE (Oct. 8, 2018), https://.blog.google/technology/safety-security/project-strobe.

[105] Felt et al., *supra* note 103, at 628.

[106] *Declare Permissions for Your App,* GOOGLE, https://.google.com/googleplay/android-developer/answer/9214102 (last visited Apr. 16, 2020).

[107] Felt et al., *supra* note 103, at 634.

[108] *Id.* at 636.

[109] Quinn Grundy et al., *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis,* BMJ, Mar. 20, 2019, at 1, 4.

[110] *Id.*

[111] *Id.* at 4.

study, over 67% of the entities that data was sent to were "analysis providers," which include those responsible for collecting, collating, analyzing, or commercializing user data.[112]

C. Third-Party Libraries and Software Development Kits Have Access to Data

When an app receives permissions from the user, those permissions are passed down to all the components of the apps, and because apps are usually developed with the assistance of third parties, this transfer of permissions can provide ways for third parties to collect data. Combining code from other sources enables the developers to save time, use pre-tested code and modular code (where a function is in an independent module from the rest of the code).[113] Modular code can provide a specific function, such as targeted ads, app maintenance, social network integration, or user engagement,[114] rather than being interwoven with the rest of the app.[115] To this end, developers often use third-party libraries and software development kits for modular code, and, in addition to the immense benefits these libraries provide, the libraries are also able to collect sensitive data from consumers through the code that is implemented.[116] Because the libraries are used by various apps,[117] different apps may receive different sets of permissions from a single device; developers can utilize the diversity of apps to create digital profiles of the users.[118] The library or third-party services receive the same set of permissions the parent app receives, receiving large amounts of data usually beyond what was needed to provide a specific service to the app devel-

---

[112] *Id.* at 5.
[113] *See, e.g.*, Uroosa Sehar, *Third Party SDKs Used By Top Mobile Apps,* VIZTECK SOLUTIONS (Sept. 26, 2016), https://.com/blog/third-party-sdk-used-by-top-mobile-apps; *Importance of Modularity in Programming*, ASPECT-ORIENTED SOFTWARE DEV. (Jan. 18, 2018), http://.net/importance-of-modularity-in-programming.
[114] Abbas Razaghpanah et al., *Apps, Trackers, Privacy, and Regulators,* NETWORK & DISTRIBUTED SYSTEMS SECURITY SYMP. 1 (2018), https://.mobi/papers/ndss18_ats.pdf.
[115] *See generally* Saksham Chitkara et al., *Does this App Really Need my Location? Context-Aware Privacy Management on Smartphones,* PROC. ACM ON INTERACTIVE MOBILE WEARABLE & UBIQUITOUS TECHNOLOGIES, Sept. 2017, at 42:1 (2017).
[116] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data With Third-Party Services,* CONVERSATION (May 29, 2017, 9:48 PM), http://.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404.
[117] Chitkara et al., *supra* note 115, at 42:2.
[118] Vallina-Rodriguez & Sundaresan, *supra* note 116.

oper.[119] The specific device can then be identified through a unique device identification number.[120] Based on the top 1,000 apps in the App Store and Google Play, the average number of Software Development Kits per app was 19 for iOS and 28 for Android. 17.6% of those apps on the App Store and 25.4% of those on Google Play had at least one Facebook Software Development Kit.

In, *Does this App Really Need My Location? Context-Aware Privacy Management for Smartphones,* Yuvraj Agarwal et al. analyzed 1,321 users and found that the "most popular 30 libraries account for more than half of all private data accesses, while the top 100 account for 70%."[121] When incorporating ad-technology code or analytics packages, developers may not be aware of the details collected by the packages, and consumers are usually not provided any notice inside the app that it is "effectively tracking users without their knowledge or consent while remaining virtually invisible."[122] Often, when data is sent to a third party that is identifiable, the third party only functions as a subsidiary of another, and data is shared between the subsidiary and the parent, which further complicates those trying to piece together a map of how data is transmitted.[123] For example, Yahoo owns Flurry, Flickr, and Interclick,[124] and AOL owns Convertro and Gravity Insights.[125] Both Yahoo and AOL

---

[119] Razaghpanah et al., *supra* note 114, at 1.
[120] Chitkara et al., *supra* note 115, at 42:7.
[121] *Id.* at 4
[122] Razaghpanah et al., *supra* note 114, at 1.
[123] *See* Reuben Binns et al., *Third Party Tracking in the Mobile Ecosystem,* WEBSCI '18 10TH ACM CONF. ON WEB SCI., Oct. 8, 2018, at 1, 3, *available at* https://.org/pdf/1804.03603.pdf.
[124] Ingrid Lunden, *Yahoo Buys Mobile Analytics Firm Flurry For North of $200M,* TECHCRUNCH (July 21, 2014, 1:55 PM), https://.com/2014/07/21/yahoo-is-buying-mobile-analytics-firm-flurry-for-north-of-200m/; Mat Honan*, The Most Fascinating Profile You'll Ever Read About a Guy and His Boring Startup*, WIRED (Aug. 7, 2014, 6:38 AM), https://.wired.com/2014/08/the-most-fascinating-profile-youll-ever-read-about-a-guy-and-his-boring-startup; Leena Rao, *Yahoo To Buy Data-Driven Advertising Network Intercick For $270 Million*, TECHCRUNCH, (Nov. 1, 2011, 8:10 AM), https://.com/2011/11/01/yahoo-buys-data-driven-ad-company-interclick-for-270-million.
[125] Kara Swisher, *AOL Buys Personalization Startup Gravity for $90 Million in Cash*, VOX (Jan. 23, 2014, 4:31 AM), https://.vox.com/2014/1/23/11622610/aol-buys-personalization-startup-gravity-for-90-million-in-cash; Ingrid Lunden, *AOL Buys Marketing Analytics Company Convertro for $101M*, TECHCRUNCH (May 6, 2014, 3:36 PM), https://.com/2014/05/06/aol-buys-marketing-analytics-company-convertro-for-101m-memo.

are owned by Oath (now Verizon Media),[126] which is owned by Verizon, the "root parent."[127] The root parent has access to the data gathered by the subsidiaries; it can aggregate and manage the data as it sees fit.[128] In February of 2019, Sam Schechner and Mark Secada reported on how Flo Health Inc.'s "Flo Period and Ovulation" tracker, which claims to have over 25 million active users, informed Facebook when a user was having her period or was intending to get pregnant.[129] Their analytics kit, which is built into "thousands of apps," uses a tool called "App Events," which "allows developers to record their users' activity and report it back to Facebook regardless of whether users log in via Facebook or even have a profile."[130] Similarly, HR Monitor, a heart-rate app on Apple's iOS, sent a user's heart rate to Facebook immediately after it was recorded.[131] In a written statement, Flo remarked that the data sent to Facebook is "depersonalized," yet testing by the Wall Street Journal revealed that unique advertising identifiers, which can be matched to a device or profile, were sent with the sensitive information.[132] For an Android app, the Wall Street Journal commissioned a cybersecurity firm named Defensive Lab Agency ("DLA") to determine what an app, called BetterMe: Weight Loss Workouts, was sending.[133] BetterMe, immediately after a consumer entered the information, sent a users' weight and height to Facebook.[134]

D. Cross-device Tracking is Difficult to Detect and Can Link Consumer Data

These examples are just a few highlights.[135] Dozens of other examples in news stories are available across the internet, and new exam-

---

[126] Brian Heater, *Oath Officially Becomes Verizon Media Group on January 8*, TECHCRUNCH (Dec. 18, 2018, 4:38 PM), https://.com/2018/12/18/oath-officially-becomes-verizon-media-group-on-january-8.
[127] Nick Turner, *Verizon Kills Oath Brand After It Fails to Enliven Yahoo and AOL*, BLOOMBERG (Dec. 18, 2018, 4:46 PM), https://.bloomberg.com/news/articles/2018-12-18/verizon-kills-oath-brand-after-it-fails-to-enliven-yahoo-and-aol.
[128] Razaghpanah et al., *supra* note 114, at 2.
[129] Schechner & Secada, *supra* note 96.
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *See also* Dave Muoio, *Most Popular Health Apps Routinely Share Data with Little Transparency*, MOBI HEALTH NEWS (Mar. 22, 2019), https://.mobihealthnews.com/content/most-popular-health-apps-routinely-share-data-little-transparency.

ples arise every day.[136] The real concern with data comes with the collation of the data in third and fourth parties since they can use cross-device tracking to track users across platforms and devices, creating increasingly invasive and revealing profiles of individuals who are unaware of them.[137]

"Cross-device tracking occurs when platforms, publishers, and ad tech companies try to connect a consumer's activities across her smartphones, tablets, desktop computers, and other connected devices."[138] As with most technologies, tracking can provide a number of benefits to consumers, such as logging into a social media account across devices, "maintain[ing] state" to pick up where the user left off in a book, or preventing fraud.[139] However, tracking also allows companies that aggregate the data to create an entire device map and analyze "an individual consumer's activities based not only on her habits on one browser or device," but also on all the devices linked to the consumer.[140] Combining this with data about a consumer's offline behavior collected from physical stores that sell their data sets, companies can create a more revealing picture of a person than just one app or device alone can.[141]

When engaging in cross-device tracking, companies use both "deterministic" and "probabilistic" techniques.[142] Deterministic techniques usually involve some form of consumer-identifying characteristic, like a login; typically, a consumer will log in on each device or app they use.[143] Probabilistic techniques require a company to infer which consumer uses

---

[136] *See* Sam Schechner, *Eleven Popular Apps That Shared Data With Facebook*, WALL ST. J. (Feb. 24, 2019, 7:45 PM), https://.wsj.com/articles/eleven-popular-apps-that-shared-data-with-facebook-11551055132.

[137] *See* Samantha Cole, *Health Apps Can Share Your Data Everywhere, New Study Shows*, VICE (Mar. 20, 2019, 5:30 PM), https://.vice.com/en_us/article/pan9e8/health-apps-can-share-your-data-everywhere-new-study-shows (citing a number of health apps that sent data to Facebook).

[138] FED. TRADE COMM'N, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT i (Jan. 2017), https://.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [hereinafter CROSS-DEVICE TRACKING FTC REPORT].

[139] *Id.*

[140] *Id.*

[141] *See* Linda Carroll, *Your Health App Could Be Sharing Your Medical Data*, REUTERS (Mar. 22, 2019, 11:51 AM), https://.reuters.com/article/us-health-apps-privacy-idUSKCN1R326W.

[142] CROSS-DEVICE TRACKING FTC REPORT, *supra* note 138, at 2.

[143] *Id.* at 2–3.

a device.[144] This often happens through IP tracking or geolocation information, and because consumers do not have to take any affirmative identification action, it is less apparent to consumers.[145] Combining these two techniques results in more accurate information, so companies often work together to merge data sets. With the popularity of connected devices, the scope of this tracking may extend to include smart televisions, health data from wearable devices, and shopping habits collected through retail IoT practices, yet companies are usually not explicit in discussing these practices.[146] The FTC, in reviewing 100 privacy policies, only found three policies that reference "enabling third-party cross-device tracking . . . ."[147]

Cross-device tracking presents concerns about transparency, choice, and security—themes that have been recurring through this paper so far. Between consumer-entered information, excessive permissions, third party development kits, and cross-device tracking, the challenge to increase company transparency, consumer understanding, and data security will only become more difficult. When we consider the ways data can be used to increase our quality of life, it is apparent that we need to work towards a solution that is both conducive to the use of data as well as the safety and choice of consumers.

IV. The Impact of Health-Related Data

At first glance, the data collected from connected devices that companies use largely appears to be limited to advertising and software companies, but on closer inspection, there is a deeper trend of data usage. Through the power of machine learning, large companies are able to sort through incredible amounts of data to reveal insights about each person. These analytic services are able to be employed by companies for a variety of purposes, such as identifying the onset of disease before the symptoms become critical or evaluating the health risk of a patient to make changes to their insurance plan. When looking at the impact of health-related data on consumers, it is important to broaden the scope to include targeted advertising, algorithmic processing, and the potential for combination with other readily available data sources.

---

[144] *Id.* at 3.
[145] *Id.*
[146] *Id.* at 7.
[147] *Id.* at 8.

A. Targeted Advertising Can Pose Substantial Risks

According to a report discovered by *The Australian*, Facebook's algorithms can enable advertisers to determine precisely when a teenager has low self-esteem, insecurity, depression, or lack of confidence.[148] Though Facebook claims the report has been misleading,[149] it has been corroborated by others who have felt first-hand how advertisers can prey on vulnerable individuals.[150] While the report should come as no surprise given Facebook's 2014 study where it claimed it could "make people feel more positive or negative through a process of 'emotional contagion,' "[151] it highlights the role data analytics can play in determining things the users themselves are not aware of or would not want to be shared. More importantly, it illustrates the detrimental effects that careless advertising can bring to an individual, particularly for vulnerable populations. When Kari Paul interviewed Caroline Sanders, a machine learning designer, Sanders commented that "while algorithmically they may seem related to what was served up before, there is a lot of harm in the causal effects of how these things manifest."[152] Having these advertisements escalate from promoting "meditation apps" to asking users " 'are you bipolar' is really dangerous."[153]

In other cases, the harm from targeted advertising can arise from violations of privacy, errors in attribution, or directed political messaging at vulnerable populations. Facebook showed gay conversion therapy ads to young LGBT users on their network, which Facebook attributed to a "micro-targeting" blunder, despite the "evidence of the damage conversion therapy does to LGBT people's health and well-being."[154] The well-known story of Target predicting the pregnancy of a high school teenager

---

[148] Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless,"* ARS TECHNICA (May 1, 2017, 2:00 AM), https://.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless.

[149] Press Release, Facebook, Comments on Research and Ad Targeting (Apr. 30, 2017), *available at* https://.fb.com/news/h/comments-on-research-and-ad-targeting.

[150] *See, e.g.*, Kari Paul, *When Facebook and Instagram Think You're Depressed,* VICE (May 5, 2017, 11:16 AM), https://.vice.com/en_us/article/pg7d59/when-facebook-and-instagram-thinks-youre-depressed.

[151] Robert Booth, *Facebook Reveals News Feed Experiment to Control Emotions,* GUARDIAN (June 29, 2014), https://.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds.

[152] Paul, *supra* note 150.

[153] *Id.*

[154] Helena Horton & James Cook, *Facebook Accused of Targeting Young LGBT Users with 'Gay Cure' Adverts*, TELEGRAPH (Aug. 28, 2018, 12:00 PM), https://.tele-

based on her purchase history serves as another example of how data analytics have the potential to overstep boundaries, reveal personal information, and incentivize secrecy.[155] In the Target example, the company sent a coupon booklet for baby items to a high school girl whose father had not yet been told of her pregnancy.[156] After Target developed their pregnancy-prediction model, they sought to obfuscate their discovery by "piggyback[ing] on existing habits" and inserting baby items in other ads to make it look like they were "chosen by chance."[157] In a similar vein, Copley Advertising LLC was pursued by the Massachusetts Attorney General after they used geofencing technology to deliver targeted advertisements of anti-abortion messages to over 800,000 vulnerable women[158] as they visited abortion clinics. In the subsequent settlement, Copley agreed "not to use [geofencing] technology at or near Massachusetts healthcare facilities to infer the status, medical condition, or treatment of any person."[159]

B. Automated Decision Making and Data Brokers Can Harm Consumers

Though they operate mostly out of the public eye, data brokers collect data about consumers from hundreds of different public and proprietary sources in order to make, analyze, package, and sell said data or insights derived from the data to other companies. These companies almost never have direct relationships with the subjects of the data they collect; as discussed earlier, it is remarkably difficult to track the data to

---

graph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts.

[155] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[156] *Id.*

[157] *Id.*

[158] *See* Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, REWIRE.NEWS (May 25, 2016, 6:52 PM), https://.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits; Press Release, Office of Mass. Att'y Gen., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), *available at* https://.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts.

[159] Nate Raymond, *Firm Settles Massachusetts Probe Over Anti-Abortion Ads Sent to Phones*, REUTERS (Apr. 4, 2017), https://.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX.

the brokers. As a result, most consumers are not even aware these brokers have data on them or that their data is being collected. Generally, brokers can be divided into four types: people search sites, like Spokeo and ZoomInfo; advertising and marketing, like Acxiom; credit reporting, like Experian and Equifax; and risk mitigation, like LexisNexis Risk Solutions.[160] Each purchases data sets, scrapes public records, and/or participates in app-centric data collection. Acxiom, for example, provides "up to 3,000 attributes on 700 million people," and in 2018, "10,000, on 2.5 billion consumers."[161]

These companies often develop "risk scores" based on consumer data which can then be sold to doctors, insurance companies, and hospitals to identify at-risk patients.[162] In the process, these data brokers have partnered with health-insurance companies to process data on hundreds of millions of Americans.[163] LexisNexis Risk Solutions advertises its services by stating that it offers health risk prediction scores separate from protected health information covered under HIPAA.[164] ProPublica reported that LexisNexis "uses 442 non-medical personal attributes to predict a person's medical costs. Its cache includes more than 78 billion records from more than 10,000 public and proprietary sources . . . ."[165] Lexis went so far as to "validate[ ] its scores against insurance claims and clinical data. But it won't share its methods and hasn't published the work in peer-reviewed journals" to be verified.[166] Milliman MedInsight, one of the world's largest actuarial firms, is now using Lexis's scores, "[M]atch[ing] patient and member lists sent by healthcare organizations

---

[160] Steven Melendez & Alex Pasternack, *Here are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST COMPANY (Mar. 2, 2019), https://.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[161] *Id.*

[162] *See, e.g.*, Mohana Ravindranath, *How Your Health Information is Sold and Turned into 'Risk Scores'*, POLITICO (Feb. 3, 2019, 6:56 AM), https://.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978.

[163] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You – And It Could Raise Your Rates,* PROPUBLICA (July 17, 2018), https://.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[164] *See id;* U.S. DEP'T OF HEALTH & HUMAN SERVS., NAT'L COMM. ON VITAL AND HEALTH STATISTICS, HEALTH INFORMATION PRIVACY BEYOND HIPAA: A 2018 ENVIRONMENTAL SCAN OF MAJOR TRENDS AND CHALLENGES 23 (Dec. 2017) [hereinafter DHHS BEYOND HIPAA].

[165] Allen, *supra* note 163.

[166] *Id.*

to approximately 280 million identities."[167] Marcos Dachary, Director of Product Management for Milliman, acknowledged that "there could also be negative potential."[168] In other words, it could be used to discriminate.

Similarly, Aetna purchased data on millions of Americans from a data broker that contained hundreds of details about each person, including a person's hobbies, such as whether they ride bikes or run marathons.[169] Frank Pasquale, a University of Maryland law professor who specializes in issues relating to machine learning, comments that the "health privacy machine" is in crisis, stating that while the United States has "a law that only covers one source of health information," and that there is rapid development of data from other sources.[170] He suggests that health-risk scores should be treated like credit scores, for "[t]he risk of improper use is extremely high. And data scores are not properly vetted and validated and available for scrutiny."[171] This trend appears to have no sign of abating. Similarly, Optum, owned by UnitedHealth Group, was issued a patent in 2016 for an invention that links what consumers share on social media to their clinical and payment information.[172]

Certainly, this data could help patients get appropriate care, but "the industry has a history of boosting profits by signing up healthy people and finding ways to avoid sick people—called 'cherry picking.'"[173] Despite the Affordable Care Act, which prevents denials based on pre-existing conditions and is currently the subject of litigation,[174] insurance companies could still use the data to determine the prices of certain plans, which drugs to include in a plan, or which providers to limit from their network.[175]

---

[167] *Milliman MedInsight to Use LexisNexis Risk Solutions Socioeconomic Health Attributes to Help Enhance Healthcare Intelligence,* LEXISNEXIS RISK SOLUTIONS (Oct. 24, 2017, 9:00 AM), https://.prnewswire.com/news-releases/milliman-medinsight-to-use-lexisnexis-risk-solutions-socioeconomic-health-attributes-to-help-enhance-healthcare-intelligence-300541930.html.
[168] Allen, *supra* note 163.
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] U.S. Patent No. 9,300,676B2 (filed Mar. 17, 2014) (issued Mar. 29, 2016).
[173] Allen, *supra* note 163.
[174] *See* Ailsa Chang & Sabrina Corlette, *How a Lawsuit Challenging Obamacare Could Affect People with Pre-Existing Conditions,* NPR (Mar. 28, 2019, 5:03 PM), https://.npr.org/2019/03/28/707722585/how-a-lawsuit-challenging-obamacare-could-affect-people-with-pre-existing-condit.
[175] Allen, *supra* note 163.

Using these data sources, companies can utilize automated decision making with little to no transparency to make eligibility decisions for loans, provide less favorable services, increase interest rates, fees, and insurance premiums, or reject applicants for employment opportunities.[176] At any point in the process, automated decision making could filter out individuals with problematic characteristics; without a human participating in the process, the filtered individual would have little to no idea why they faced negative consequences.[177]

If regulators manage to prevent insurers' efforts to avoid certain patients, "[E]mployers may adopt pretextual tactics to drive them away as employees," and these methods won't be easy to detect.[178] Within the black box of an algorithm, it can be notoriously difficult to detect where the line is between one category and another.[179] If an employer was made aware of certain sensitive "health-related topics or conditions, such as 'Expectant Parent,'" which can be triggered from their purchase patterns, browsing history, or other seemingly unrelated pieces of data, they could use this information for their hiring or firing decisions without the individual being aware.[180] Generally, the Americans with Disabilities Act prohibits an employer from investigating an employee's medical condition beyond what is necessary to assess the employee's ability to perform their occupational duties, because the introduction of varied sources of data and their associated insights can obfuscate the lines of legality and reduce employers' chances of being caught.[181]

To use Pasquale's example, an employee would be hard-pressed to know that the algorithm was being used at all, much less whether or not the algorithm was "characterizing a potential employee as 1) diabetic, 2) in a 'diabetic-focused household' . . . . , 3) concerned about diabetes, [or] 4) having a demanding home life . . . ."[182] Determining whether element (4) applies would likely require insight into the attributes of the algorithms of the first three elements.[183] Using an algorithm to ascertain

---

[176] DHHS BEYOND HIPAA, *supra* note 164, at 23.
[177] *Id.*
[178] *See* Pasquale, *Redescribing Health Privacy*, *supra* note 12, at 107.
[179] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY 9 (Harv. Univ. Press 2015).
[180] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 5 (2014), https://.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[181] *See* Pasquale, *Redescribing Health Privacy supra* note 12, at 124.
[182] *Id*. at 107 (internal parentheticals removed).
[183] *See id.* at 107.

indirectly that which the employer could not ask directly is certainly illegal,[184] but applicants will have a more difficult time discovering and litigating which characteristics were used to make an employment decision.[185] This is because applicants would need to review information from different data sources which have a correlation with a medical condition, such as exercise data, internet searches, or purchase history and determine that these sources critically affected the hiring decision.[186] Therefore, any effort to expand employment protections beyond the first box would run into challenges from businesses and analytics firms because it would "require extensive auditing of business records" to figure out.[187]

Because the data is collected from so many different sources, advertising companies, data brokers, and those who receive risk scores have no obligation and little incentive to allow consumers to rectify incorrect data points that could lead to incorrect conclusions, which could unknowingly affect how they live their lives.[188] As Samuel Finlayson of Harvard Medical School points out, in the context of artificial intelligence and automated decision making, "the inherent ambiguity in medical information, coupled with often-competing financial incentives, allows for high-stakes decisions to swing on very subtle bits of information."[189]

As algorithms become more prominent, transparency will become more difficult. While HIPAA requirements have been clarified through litigation, "[D]ata brokers continue gathering information, and making

---

[184] *See* U.S. EQUAL EMP'T OPPORTUNITY COMM'N, ADA ENFORCEMENT GUIDANCE: PREEMPLOYMENT DISABILITY-RELATED QUESTIONS AND MEDICAL EXAMINATIONS 2 (1995), https://.eeoc.gov/policy/docs/preemp.html.

[185] *See* Pasquale, *Redescribing Health Privacy supra* note 12, at 124.

[186] *See* DHHS BEYOND HIPAA, *supra* note 164, at 49 (discussing hypothetical data company that can use data, such as food purchase and biofeedback information, to reasonably identify whether a person is diabetic).

[187] Pasquale, *Redescribing Health Privacy supra* note 12, at 107.

[188] *See* Cade Metz & Craig S. Smith, *Warnings of a Dark Side to A.I. in Health Care*, N.Y. TIMES (Mar. 21, 2019), https://.nytimes.com/2019/03/21/science/health-medicine-artificial-intelligence.html.

[189] *Id*; Milena A. Gianfracesco et al., *Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data*, JAMA INTERNAL MED., Nov. 2018, at 1544 , *available at* https://.ncbi.nlm.nih.gov/pmc/articles/PMC6347576; Carolyn Y. Johnson, *Racial Bias in a Medical Algorithm Favors White Patients over Sicker Black Patients*, WASH. POST (Oct. 24, 2019), https://.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients.

predictions based on it, entirely outside the HIPAA-protected zone."[190] The inferences from this data will become even more influential. These algorithms can make decisions about real-life people who are entirely unaware of how these decisions are being made.[191] Despite anti-discrimination statutes, individuals may be concerned that algorithms may make discriminatory decisions that are either not covered by statute, cannot be proven, or are undetectable by workers.[192]

V. Conclusion

In the three decades since Internet adoption began to climb, technology has changed dramatically, computing power has increased exponentially, and data is being generated at rates never before seen. The ability to process large amounts of data will be the hallmark of the 21st century; artificial intelligence and machine learning will revolutionize the way society operates. Not so long ago, mobile phones were reserved for the wealthy, and Facebook was "merely a database of profile pages of other people at Harvard."[193] Now, there are more mobile devices than people,[194] and Facebook has over 2 billion users.[195] As these technologies evolve, it will be vital to realize that, given the advent of machine learning and vast data generation, even the most innocuous pieces of data can be combined with others to generate new types of inferences previously thought impossible. Merely because information did not originate with a covered entity does not mean it cannot have dramatic impacts on the well-being of individuals or in the innovation of products.

Yet, the task of defining what constitutes health data is difficult, because data ostensibly unrelated to a person's health may ultimately be used to craft new conclusions about that person's sensitive health status; this can be considered a byproduct of a sectoral privacy regime based on

---

[190] Pasquale, *Redescribing Health Privacy supra* note 12, at 108.
[191] *See generally* Sean Illing, *How Algorithms are Controlling Your Life*, VOX (Oct 1, 2018, 8:10 AM), https://.vox.com/technology/2018/10/1/17882340/how-algorithms-control-your-life-hannah-fry.
[192] Sharona Hoffman*, Employing E-health: The Impact Of Electronic Health Records On The Workplace,* 19 KAN. J.L. & PUB. POL'Y 409, 416 (2010).
[193] Alexis Madrigal, *Before It Conquered the World, Facebook Conquered Harvard,* ATLANTIC (Feb. 4, 2019), https://.theatlantic.com/technology/archive/2019/02/and-then-there-was-thefacebookcom/582004.
[194] Zachary Davies Boren, *There Are Officially More Mobile Devices Than People in the World,* INDEP. (Oct. 7, 2014), https://.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html.
[195] Madrigal, *supra* note 193.

data source and data type.[196] A particular data point may be used as health data in the evaluation of a person's exercise habits and medical screening; that same data point may also be processed as part of a rideshare service.[197] The development of new apps and products that use this data to diagnose and treat illnesses and conditions can benefit consumers and society at large, but companies may use this same data to engage in discriminatory practices without ever notifying the consumer.

Looking forward, companies, regulators, and legislators will need to develop a framework that encourages innovation, evaluating the purposes of processing, informing consumers, incentivizing business transparency, and protecting the security, privacy, and freedom of individuals. Further research should explore possible solutions, which educate consumers and give them more control over their data while promoting ethical innovation.

---

[196] *See* O'Connor, *supra* note 21.
[197] *Id.*

Lies, Sex and Shaming: An Essay Reflecting on the Beginning of the Call-Out Culture and the Legal Response

Connie Davis Powell Nichols*, Mia Moody-Ramirez** & Tonya B. Hudson***

Keywords: freedom of speech, libel, new media, social media, privacy, defamation, Internet shaming, online gossip, the Communications Decency Act, user-generated content.

Table of Contents

---

* Connie Davis Nichols is a Professor of Law at Baylor Law School where she teaches intellectual property courses, and she is the Director of the Baylor Law School Intellectual Property Law and Entrepreneurship Clinic. Professor Nichols is also Of Counsel with the Houston-based law firm Gray Reed. Professor Nichols earned her J.D. cum laude from Maurer School of Law at Indiana University-Bloomington in 2000 after receiving her B.A. in Biology from the University of North Carolina at Chapel Hill in 1997. Professor Nichols' research focuses on the impact of new technology on traditional concepts of intellectual property.

** Mia Moody-Ramirez, Ph.D., is Professor and Chair of the Baylor University Department of Journalism, Public Relations and New Media. She joined Baylor in 2001 and has maintained an active research portfolio in addition to her teaching and leadership roles. Her research emphasizes media framing of people of color, women and other underrepresented groups. The author or co-author of four books, Dr. Moody-Ramirez has also been widely published in a variety of academic and industry journals and. She was honored with the Outstanding Woman in Journalism award by the Association for Education in Journalism and Mass Communication, and this summer received the organization's Lionel Barrow Jr. Award for Distinguished Achievement in Diversity Research and Education. She is also a 2019 Fellow in the AEJMC Institute for Diverse Leadership.

*** Tonya B. Hudson serves as Director of Strategic Communications in the Media and Public Relations Office at Baylor University. Before working at Baylor, Tonya was the Public Information Officer for the City of Duncanville for five years. She earned a

I. Introduction

Social media has provided a platform for users to document their lives and seamlessly share content with the world. As a consequence, social media has also provided users the ability to digitally document the lives of others without their permission and to make embarrassing content accessible on a variety of platforms. The nature of social media—mass communication with relative anonymity—has enabled the adoption of practices that mirror those offline (such as shaming, dating, fundraising, etc.), but with an online global audience. The Internet has become the stage of choice to shame, troll, or simply harass individuals for various reasons owing to the ease of posting content to social media sites.[1] Individuals use social media platforms to take embarrassing as well as mundane, everyday content out of personal spaces and place them center stage for the public to view. Cyberbullying, Internet shaming and trolling have become commonplace in today's world of social media activity. Users routinely seek revenge in a unique way that does not require personal confrontation, but enables the users seeking revenge to enlist an army of supporters.[2]

The introduction of online-gossip-magazines offered a different venue for gossip. Gossip content providers began posting stories loosely based on truth with little attribution, which reaches well beyond the grocery store checkout aisle of its brick and mortar counterpart.[3] Trends like "slut shaming" in which individuals post and repost raunchy pictures of individuals on social media platforms such as Facebook, Twitter, and Instagram have become commonplace.[4] So commonplace that the now

---

bachelor's degree in Journalism from the University of Oklahoma and a master's degree in Journalism from Baylor University. As a Director of Strategic Communications, Tonya focuses on crisis communications, strategic messaging, issues management, interview coaching, and is a University spokesperson.

[1] Danielle Keats Citron, *How Cyber Mobs and Trolls Have Ruined the Internet—and Destroyed* Lives, NEWSWEEK (Sept. 19, 2014, 12:56 PM), https://www.newsweek.com/internet-and-golden-age-bully-271800; *see* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 86–87 (2007); *see* Mike Young, *Name and Shame Websites: Free Speech or Defamation?*, MIKE YOUNG LAW FIRM, http://mikeyounglaw.com/internet-defamation (last visited Jan. 14, 2021).

[2] Citron, *supra* note 1.

[3] *How the Supermarket Tabloids Stay Out of Court*, NY TIMES (Jan. 4, 1991), https://www.nytimes.com/1991/01/04/news/how-the-supermarket-tabloids-stay-out-of-court.html.

[4] *See Teen Shaming the Latest Rage on Social Media*, ABC NEWS (Jan. 7, 2013, 4:13 AM), https://abcnews.go.com/Technology/teen-shaming-latest-rage-social-media/story?

defunct website "Is Anyone Up," invited bitter former lovers to submit nude photos and videos of their former partners, along with that former partner's Facebook profile or other social media identity.[5] In the same vein, some teenagers videotape, photograph, and share online the sexual assaults of victims who are intoxicated or in states of undress, sometimes without remorse.[6] While the aforementioned uses of social media highlight some extreme behaviors that are widely viewed as problematic, these uses have provided a blueprint for other uses that on the surface seem less problematic. Indeed, today's so-called "call-out culture" includes many of the same elements.[7]

While privacy, defamation, and changes in media are all in the forefront of today's scholarship, there is seemingly a gap in the scholarship on the counter-cultures developed on social media as a result of these changes.[8] As society's communication platforms have changed, so has the need to expand the existing scholarship to address how these trends begin and proliferate. At a glance, communications and mass media literature reveal various articles on courts' handling of cases based on the type of content posted, the platform, and the person who posted the content.[9]

---

id=18148546; *see* Sophie Sills et al., *Rape Culture and Social Media: Young Critics and a Feminist Counterpublic*, FEMINIST MEDIA STUD. 936, 941 (2016).

[5] *See* Kashmir Hill, *IsAnyoneUp Is Now Permanently Down*, FORBES (Apr. 19, 2012, 5:52 PM), https://www.forbes.com/sites/kashmirhill/2012/04/19/isanyoneup-is-now-permanently-down/#72c3540d450a.

[6] Katie McDonagh, *The birds, the bees and their boundaries*, SONOMA STATE STAR (Sept. 24, 2013), https://www.sonomastatestar.com/opinion/2014/10/23/the-birds-the-bees-and-their-boundaries.

[7] *See* Adrienne Matei, *Call-Out Culture: How to Get it Right (and Wrong)*, THE GUARDIAN (Nov. 1, 2019), https://www.theguardian.com/lifeandstyle/2019/nov/01/call-out-culture-obama-social-media (Discussing call-out culture is a form of public shaming that seeks to hold individuals accountable for actions by bringing attention on social media. Generally, the individual faces some sort of consequence as a result of the behavior).

[8] *See* Daniel J. Solove, *Do Social Networks Bring the End of Privacy?*, 299(3) SCI. AM. 100, 100-106 (2008), https://www.scientificamerican.com/article/do-social-networks-bring; *see also* Young, *supra* note 1.

[9] *See id*; *see, e.g.*, R. Post, *Three Concepts of Privacy*, 89 GEO. L. J. 2087, 2089–90 (2001) (discussing the logic of judicial decisions excluding inflammatory evidence); Lemi Baruh, *Read at your own risk: shrinkage of privacy and interactive media*, 9(2) NEW MEDIA & SOC'Y 187, 205 (2007) (discussing in a legal environment how interactive media threaten informational privacy); SOLOVE, *supra* note 1, at 101, 113, 137, 143, 146, 148; Nicole B. Cásarez, *Dealing with Cybersmear: How to Protect Your Organization from Online Defamation*, 47(2) PUB. REL. Q. 40, 41–43 (2002)

This Review Essay examines three prominent U.S. lawsuits that involved the use of social media in ways not contemplated by the social media platform or the law, in an effort to provide an in-depth understanding of the ways in which social media platforms have facilitated the growth of new countercultures. This Essay seeks to establish that as new communication patterns develop, the laws are consistently playing catch-up by reviewing three of the first cases to address cybertorts: (1) *United States v. Drew*[10]*;* (2) *Todd Hollis v. Tasha C. Joseph-Cunningham*[11] (DontDateHimGirl.com); and (3) *Sarah Jones v. Dirty World Entertainment Recordings, LLC*.[12]

II. Defining Privacy

Defining personal privacy has a storied history.[13] To date, a precise definition continues to be elusive.[14] In 1890, Justices Warren and Brandeis wrote the influential article "Right to Privacy" in which privacy was defined as the "right to be let alone."[15] Inspired by the intrusive technology of the time, instant photography, Warren and Brandeis believed it was necessary to preserve "the right to an inviolate personality."[16] Brandeis continued to advocate for this definition in his famous dissent in *Olmstead v. United States*, defining the "right to be let alone" as "the most comprehensive of rights and the right most valued by civilized men."[17] Contemporary scholars have defined privacy as a right to be let alone, of personhood, secrecy, limited access to self, and control over the dissemination of information about one's self.[18] In *Three Concepts of Privacy*, Robert Post asserts that "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so

---

(discussing procedural obstacles to forcing identification of anonymous online critics) ; VALERIE C. BRANNON, FREE SPEECH AND THE REGULATION OF SOCIAL MEDIA CONTENT 4–9 (2019) (discussing legal barriers to private lawsuits against social media providers).

[10] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[11] Hollis v. Cunningham, 2008 WL 11417652 (S.D. Fla. Feb. 6, 2008).

[12] Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398 (6th Cir. 2014).

[13] *See generally* S. Warren & L. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[14] *See generally* Alice E. Marwick, Diego Murgia-Diaz & John G. Palfrey, *Youth, Privacy, and Reputation (Literature Review)* (Harvard Pub. L. Working Paper No. 10–29, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163.

[15] Warren & Brandeis, *supra* note 13, at 193.

[16] *Id.* at 210–11.

[17] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[18] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1092 (2002).

engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[19] Notwithstanding the inherent issues of pinpointing a single definition of privacy, the concept of privacy continues to be one that the public demands and technology obscures.

Privacy studies from the 1960s through the 1980s often focused on television, radio, and telephone communication.[20] This focus shifted with the arrival of computers and subsequently the internet.[21] "Studies of computing in the 1950s and 1960s concluded that new technologies exacerbated privacy as a social problem. . .."[22] Studies of the 1980s and 1990s focused on topics such as newsroom issues, equality disputes, and computer surveillance.[23]

Scholars such as Marwick, Murgia-Diaz & Palfrey, Friedman, and Solove pondered the impact of culture, media, and technology on privacy.[24] Friedman argues that we are "living in a Peeping Tom society," and even refers to it as "a prying, gossiping society."[25] Solove added to this narrative of modern privacy concerns the use of the Internet to shame individuals for personal wrongdoings.[26] Websites such as BitterWaitress.com, which provides servers the opportunity publish information about poor tippers, and DontDateHimGirl.com, a website that lets women publish information about men who cheated on them,

---

[19] Robert Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001).
[20] *See, e.g.*, Robert Mills, *Radio, Television and the Right of Privacy,*13 J. OF BROAD. 51 (1968); John Wegner, *Home Interactive Media: An Analysis of Potential Abuses of Privacy,* J. OF BROAD. & ELEC. MEDIA, 29, 51–63 (1985); Oscar Gandy, and Charles E. Simmons, *Technology, Privacy and the Democratic Process,* 3(2) CRITICAL STUD. IN MASS COMM. 155, 155–68. (1986).
[21] *See* Sandra Braman, *Privacy by Design: Networked Computing, 1969–1979*, 14 NEW MEDIA & SOC'Y 800 (2012).
[22] *Id.*
[23] *See e.g.*, Louise M. Benjamin, *Privacy, Computers, and Personal Information: Toward Equality and Equity in an Information Age*, COMM. & THE LAW 3 (1991); Richard P. Cunningham, *Privacy and the Electronic Newsroom*, COLUM. JOURNALISM REV., 32 (1984); Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J., 17–18 (1988).
[24] Alice E. Marwick, Diego Murgia-Diaz & John G. Palfrey, *Youth, Privacy, and Reputation (Literature Review)* (Harvard Law Sch. Pub. Law. & Legal Theory Working Paper Series, Paper No. 10-29, 2010); LAWRENCE FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 259 (2007); SOLOVE, *supra* note 1, at 76–102.
[25] FRIEDMAN, *supra* note 24, at 259.
[26] *See* SOLOVE, *supra* note 1, at 76.

took center stage in Solove's commentary on the use of social media for righting perceived personal wrongs.[27] Solove likened these websites to tools for social control reminiscent of past public punishments methods, such as Hawthorne's scarlet letter; internet shaming creates a permanent record of a person's alleged transgressions.[28]

Indeed, in "You Already Have Zero Privacy. Get over it! Would Warren and Brandeis Argue for Privacy for Social Networking?," C. Powell advanced that social media is akin to the technology that motivated Warren and Brandeis to pen *The Right to Privacy*.[29] Powell puts forward the view that privacy torts specifically designed to regulate social media posts could be on the horizon.[30] Several concerns arose in 1890 as the result of the advent of new technology capable of widespread dissemination of personal or isolated information.[31] These concerns still exist today in a world of social media, where posts on social media are generated to garner both positive and negative reactions.[32] Who should be held accountable for the exposure of private information through social media, and under what legal theory?

Traditionally, an individual sought redress for damage to one's reputation through a defamation action. Defamation is generally defined as the act of harming the reputation of another individual or entity by making a false or defamatory statement to a third party.[33] In general, a statement is "defamatory 'if it tends to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.'"[34] With limitations, the tort of defamation "attempts to do that by protecting us from the utterance of false factual assertions that would besmirch our reputations within our communities."[35]

---

[27] *Id.* at 87–90.
[28] *Id.* 90–91, 94–95.
[29] Connie Davis Powell, *"You Already Have Zero Privacy. Get over It!" Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146–47 (2011).
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *See* 28 U.S.C. § 4101(1) (2018).
[34] Walleri v. Fed. Home Loan Bank, 83 F.3d 1575, 1583 (9th Cir. 1996) (citing RESTATEMENT (SECOND) OF TORTS § 559 (1977)).
[35] Amy Kristin Sanders, *Defining Defamation: Community in the Age of the Internet*, 15 COMM. L. & POL'Y 231, 232 (2010).

While defamation provides an opportunity for redress to the damage of reputation, the First Amendment right to freedom of speech limits defamation torts.[36] For instance, public figures cannot successfully maintain a defamation action unless they can clearly and convincingly demonstrate that the statement was made with "actual malice."[37] In *New York Times v. Sullivan*, a landmark defamation decision by the U.S. Supreme Court on First Amendment protections of petition and public speech, the Court held that safeguarding freedom of speech and the press requires that a public official who brings a libel action against critics of his official conduct must prove "actual malice" by the defendants.[38] Similarly, limitations were placed upon the tort of defamation by Congress with Section 230 of the Communications Decency Act.[39] In the early 1990s, courts were uncertain whether to treat Internet Service Providers (ISPs) as publishers of libelous posts or distributors in early defamatory cases.[40] However, Congress resolved this issue when it passed the Communications Decency Act in 1996. Section 230(c)(1) of the Communications Decency Act reads: "No 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."[41]

This immunity does not apply if the provider "creates or develops" the information.[42] Section 230 immunity was intended to protect "Good Samaritan" Internet service providers from civil liability for blocking or screening objectionable online material.[43] However, Section 230 has been criticized for its use to shield websites that house such content.[44] According to Solove, "courts are interpreting Section 230 so broadly as to provide too much immunity, eliminating the incentive to foster a balance between speech and privacy. The way courts are using Section 230 exalts free speech to the detriment of privacy and

---

[36] *See* Curtis Pub. Co. v. Butts, 388 U.S. 130, 152 (1967).
[37] *See id.* (defining actual malice as a statement made "with knowledge that it was false or with reckless disregard of whether it was false or not"); *see also* New York Times Co. v. Sullivan, 376 U.S. 254, 262 (1964) (describing how "actual malice" has been defined by state courts more generally).
[38] *New York Times Co.,* 376 U.S. at 279–80.
[39] *See* 47 U.S.C. § 230 (2018).
[40] Cásarez, *supra* note 9, at 41.
[41] 47 U.S.C. § 230(c)(1) (2018).
[42] Directory Assistants v. SuperMedia, LLC, 884 F. Supp. 2d 446, 451 (E.D. Va. 2012).
[43] Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1045 (9th Cir. 2019).
[44] *See* SOLOVE, *supra* note 1, at 159.

reputation."[45] Consequently, "a host of websites have arisen that encourage others to post gossip and rumors as well as to engage in online shaming."[46] As practices such as gossip and shaming have moved online, information that was once forgettable and localized within groups has become widespread, permanent, and searchable, with broad privacy agreements that facilitate dissemination of the information.[47]

The rules have changed as online and social network communities grow in popularity.[48] And as technology continues to evolve over time, defamation law will change.[49] Sanders asserts that scholars generally "discuss two key areas in the context of online defamation: jurisdiction and anonymity. . .."[50] Moreover, "a number of articles have touched on the jurisdictional complications associated with online defamation lawsuits, including determining whether a court can exercise authority over a defendant and what state's laws should apply to a particular case."[51] For instance, traditionally, "courts typically relied upon geographic factors, including where a plaintiff lived or worked," in defamation cases.[52] However, with the popularity of the internet, citizens are automatically connected geographically, which enables the increased spread of information through various channels.[53] This loosening of geographic boundaries has challenged the traditional

---

[45] *Id.*
[46] *Id.*
[47] *See* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 30, 69 (2008) (discussing how changes in technology have resulted in new versions of existing problems); SOLOVE, *supra* note 1, at 200–01 (addressing the broad privacy agreements that insulate social media websites).
[48] *See* Matthew E. Kelley & Steven D. Zansberg, *A Little Birdie Told Me, "You're a Crook": Libel in the Twittersphere and Beyond*, 30 COMM. L. 34, at 34 (2014); Amy Kristin Sanders & Natalie Christine Olsen, *Re-Defining Defamation: Psychological Sense of Community in the Age of the Internet*, 17 COMM. L. & POL'Y. 355, at 355 (2012); Amy Kristin Sanders, *Defining Defamation: Community in the Age of the Internet,* 15 COMM. L. & POL'Y. 231, at 231 (2008).
[49] Kelley & Zansberg, *supra* note 48, at 39.
[50] Amy Kristin Sanders, Defining Defamation: Community, Harm and Plaintiff Status in the Age of the Internet 227 (2007) (unpublished Ph.D. dissertation, University of Florida) (on file with the University of Florida Libraries, University of Florida).
[51] *Id.*
[52] Sanders & Olsen, *supra* note 48, at 357–58.
[53] *Id.* at 358.

media model centered on editorial judgment and ethics.[54] The internet allows users build relationships across the globe.[55]

The type of social media platform is also a concern in this area of research. Kelley and Zansberg write that as communications are increasingly conducted via social media platforms, judges are beginning to confront the question of how to apply the law of defamation to these web-based platforms.[56] Websites such as Facebook, Amazon, Twitter, and Yelp, "have given individuals a global platform on which to air their grievances with companies."[57] The popularity of such sites has given rise to situations where business owners may take legal action over critical posts.[58]

However, those subject to shaming have little to no recourse against the social media platform enabling the dissemination of what could be damaging to their reputation. Indeed, at least one court has opined that "the average reader would know that the comments are 'emotionally charged rhetoric' and the 'opinions of disappointed lovers,'" [59] thus precluding the defamation because the statements did not satisfy the threshold requirement of a false statement of fact. A false statement of fact is a statement that the average reader would not interpret as a statement of opinion, but rather a factual assertion that is capable of being substantiated as either true or false.[60] Truth serves as an "absolute defense" to a defamation cause of action.[61] As such, many of the shaming defamation cases end at this stage.[62] Notwithstanding the lack of a cause of action for defamation, many of these cases implicate the privacy torts that were advocated for in 1890 by Warren and Brandeis and developed by William Prosser.[63]

---

[54] See *id.* at 357–58.
[55] *See id.* at 358.
[56] Kelley & Zansberg, *supra* note 48.
[57] Dan Frosch, *Venting Online, Consumers Can Find Themselves in Court*, N.Y. TIMES (May 31, 2010), http://www.nytimes.com/2010/06/01/us/01slapp.html.
[58] *See id.*
[59] Couloute v. Ryncarz, 2012 WL 541089, at *6 (S.D.N.Y. Feb. 17, 2012).
[60] *Id.* at *5.
[61] Curtis Pub. Co. v. Butts, 388 U.S. 130, 151 (1967); RESTATEMENT (SECOND) OF TORTS § 581A (AM. LAW INST. 1977).
[62] Guccione v. Hustler Magazine, Inc., 800 F.2d 298, 304 (2d Cir. 1986); Atlantis Int'l, Ltd. v. Houbigant (In re Houbigant, Inc.), 95 Civ. 9541 (JSM), 1996 U.S. Dist. LEXIS 13424, at *17 (S.D.N.Y. Sep. 13, 1996).
[63] William L. Prosser, *Privacy,* 48 CALIF. L. REV. 383, 389 (1960).

III. Privacy Laws

The digital era has given rise to cybertorts that are akin to and implicate traditional privacy torts as possible remedies to the dissemination of information that is private and/or harassing. However, commentary by scholars suggests that these torts failed to effectively combat internet intrusions.[64] The four privacy torts that establish a "right to be let alone" as envisioned by Warren and Brandeis and later developed further by William Prosser in *Privacy* and in the Restatement Second of Torts are:

(1) Intrusion upon the solitude, seclusion or private affairs;
(2) Public disclosure of private facts;
(3) Publicity which places one in a false light; and
(4) Appropriation of name and likeness.[65]

In *Prosser's Privacy Law: A Mixed Legacy*, Neil Richards and Daniel Solove argue that the "rigid" structure of the above listed privacy torts developed by Prosser "stripped privacy law of any guiding concept to shape its future development."[66] As such, Richards and Solove conclude that privacy gained prominence in tort law during the life of Prosser, but "froze" after their codification into distinct categories.[67] Privacy tort law's growth in the absence of Prosser's advocacy faded, thereby deferring the development of privacy torts to the future.[68] In *Prosser's Privacy Law: A Mixed Legacy*, the authors recount the development of privacy law and how the rigid structure and lack of flexibility in development resulted in the law's inability to keep up with the Information Age, which was the article's overarching conclusion.[69] The inability of privacy law to effectively address the growing digital cybertorts is all too apparent in a review of the cases that brought media attention to the use of social media as a way to expose, deride, and harass.

---

[64] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 89 (2009) (examining traditional tort effectiveness).
[65] Prosser, *supra* note 63, at 389.
[66] Neil Richards and Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1890 (2010).
[67] *Id.* at 1924.
[68] *See id.* at 1890.
[69] *Id.* at 1890–91.

A. *United States v. Drew*

One of the first prominent cases to address the newfound uses of social media was *United States v. Drew*.[70] *Drew* brought attention to cyberbullying.[71] Around October 16, 2006, Megan Meier, a 13-year-old girl, killed herself after receiving cruel Myspace messages from a fake account whom she thought was a 16-year-old boy named Josh Evans.[72] As the story unfolded, "Josh" turned out to be an account created by Lori Drew (and other members of the conspiracy to create the Josh Evans account), the mother of Megan's classmate.[73] The account was used for several weeks to flirt with Megan before it was turned against her.[74] Drew, an advertising-magazine publisher, claimed she used the fake profile to find out what Megan was telling other friends about her daughter after the teenagers had a falling out.[75]

In mid-September of 2006, Megan's Myspace page was contacted by the fictitious "Josh Evans."[76] According to a *People* article, "Josh's" Myspace page "was enough to get the pulse of any teen girl racing."[77] Drew stated that she used "Josh Evans" to find out whether Megan was talking about her daughter, whom Megan had allegedly "called a lesbian."[78] For several weeks, the ruse continued with "Josh Evans" sending flattering statements to Megan.[79] Abruptly, the tone of the fictitious boyfriend, "Josh Evans," turned from flattering to insulting.[80] The Myspace message from "Josh Evans" stated that "the world would be a better place without you."[81] After this interaction, Megan hanged herself in her bedroom closet.[82] The Missouri state harassment law in 2006 did not pro-

---

[70] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
[71] Brandon Darden, *Definitional Vagueness in the CFAA: Will Cyberbullying Cause the Supreme Court to Intervene*, 13 SMU SCI. & TECH. L. REV. 329, 347–48 (2010).
[72] *Drew*, 259 F.R.D. at 452.
[73] Bill Hewitt, *Did a Cruel Hoax Lead to Suicide*?, PEOPLE (Dec. 3, 2007, 12:00 PM), https://people.com/archive/did-a-cruel-hoax-lead-to-suicide-vol-68-no-23; Alex Tresniowski, *A Cyberbully Convicted*, PEOPLE (Dec. 15, 2008, 12:00 PM), https://people.com/archive/a-cyberbully-convicted-vol-70-no-24.
[74] *Drew*, 259 F.R.D. at 452.
[75] Tresniowski, *supra* note 73.
[76] *Drew*, 259 F.R.D. at 452.
[77] Hewitt, *supra* note 73.
[78] Lauren Collins, *Friend Game*, NEW YORKER (Jan. 21, 2008), https://www.newyorker.com/magazine/2008/01/21/friend-game.
[79] *Drew*, 259 F.R.D. at 452.
[80] *See id.*
[81] Hewitt, *supra* note 73.
[82] *Id.*

vide a way to prosecute Lori Drew.[83] Federal prosecutors, using jurisdiction provided by the location of Myspace servers in Los Angeles county, attempted to hold Drew responsible for the results of her social media conduct.[84]

The Computer Fraud and Abuse Act (CFAA) was utilized as the vehicle to prosecute Drew for her social media conduct.[85] "Prosecutors charged Drew with violating the Myspace terms of service (TOS), which required truthful and accurate registration, refraining from using information from Myspace to harass others, refraining from solicitation of information from a minor, and refraining from promoting false or misleading information" and with three counts of "accessing protected computers to obtain information" under the CFAA.[86] At trial, Drew was acquitted of the three charges regarding unauthorized computer access.[87] The jury was deadlocked with regard to the conspiracy charge, leaving an opportunity for a retrial upon that issue.[88] Ultimately, Drew was found guilty of a misdemeanor violation of the CFAA.[89] Drew filed a Rule 29 motion for directed acquittal,[90] and the court held that she was entitled to such relief because the creation of a fictitious account could not satisfy the CFAA requirement of an unauthorized access or access that exceeded authorization.[91]

After the unfortunate incident that preceded this case and the failure of Missouri law to hold Drew responsible for the results of her behavior online, Missouri amended its state harassment law.[92] The amended statute redefined "harassment" in Section 565.090 of the Revised Statutes of Missouri to incorporate electronic communication that "frightens, in-

---

[83] *Cyberbullying,* 24 BERKELEY TECH. L.J. 659, 659 (2009).
[84] *See id.*
[85] Gov't's Trial Mem., *supra* note 82, *passim*; *Cyberbullying*, *supra* note 83, at 659.
[86] *Cyberbullying*, *supra* note 83, at 659; Indictment, United States v. Drew (C.D. Cal 2009) (No. CR08-00582), 2008 WL 2078622.
[87] United States v. Drew, 259 F.R.D. 449, 451 (C.D. Cal. 2009); A. Tresniowski, *A Cyberbully Convicted*, PEOPLE (Dec. 15, 2008, 12:00 PM), https://people.com/archive/a-cyberbully-convicted-vol-70-no-24/.
[88] *Drew*, 259 F.R.D. at 453.
[89] *Id.* at 452.
[90] Rule 29 Mot. for J. of Acquittal at 1, United States v. Drew, 259 F.R.D 449 (C.D. Cal. 2009) (No. CR-08-582-GW), 2008 WL 5041979; *see also* Suppl. to Rule 29 Mot. at 1, United States v. Drew, 259 F.R.D 449 (C.D. Cal. 2009) (No. CR-08-582-GW), 2008 WL 5381025.
[91] *Drew*, 259 F.R.D. at 461.
[92] *Compare* MO REV. STAT. § 565.090 (2008), *with* MO REV. STAT. § 565.090 (2005).

timidates or causes emotional distress to [another] person."[93] Under the Missouri statute as amended in 2008, the penalty for harassment was imprisonment for up to one year, unless a person age 21-years-old or older committed the offense upon a person younger than or equal to 17-years-old, in which case the sentence is carried out for up to four years.[94]

While cyberbullying was being addressed nationwide through state legislation, another online phenomenon was gaining traction—shaming. Online shaming, a form of public shaming in which individuals are humiliated online, frequently involves the publication of private information online, which often produces social ridicule of the individual shamed. Such ridicule often includes hate messages, death threats, and employment terminations.[95]

B. *Todd Hollis v. Tasha C. Joseph-Cunningham*

The concept of public shaming is not new. Public shaming served as a source of punishment throughout the 1700s to mid-1800s, until legislation began abolishing the practice.[96] For example, Massachusetts abolished public stocks in 1804.[97] Throughout the early 1900s there was a continued decline in the use of public shaming as punishment.[98] However, in the mid-1970s, shaming saw a resurgence.[99] In 1998, a Harris County, Texas, district court judge gained notoriety for his use of public shaming as punishment.[100] Indeed, Judge Ted Poe indicated that over a three-year period he had issued fifty-nine shaming sentences, which were successful in decreasing recidivism.[101] As early as the Colonial days, shaming has been used as punishment.[102] Since that time, courts in many

---

[93] MO REV. STAT. § 565.090 (2008).
[94] MO REV. STAT. § 565.090 (2008); MO REV. STAT. § 558.011 (2003).
[95] Kate Klonik, *Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age*, 75 MD. L. REV. 1029, 1034 (2016).
[96] Peter Sterns, *A History of Shaming in America and its Modern Revival*, BREWMINATE (Nov. 6, 2017), https://brewminate.com/a-history-of-shaming-in-america-and-its-modern-revival.
[97] *Id.*
[98] *Id.*
[99] Aaron S. Book, *Shame On You, an Analysis of Modern Shame Punishment as an Alternative to Incarceration*, 40 WM. & MARY L. REV. 653, 660 (1999).
[100] Kate Shatzkin, *Judges Are Resorting to Shame in Sentencing Criminals*, L.A. TIMES (Apr. 26, 1998, 12:00 AM), https://www.latimes.com/archives/la-xpm-1998-apr-26-mn-43159-story.html.
[101] *Id.*
[102] E.B. v. Verniero, 119 F.3d 1077, 1115 (3d Cir. 1997); Smith v. Doe, 538 U.S. 84, 98 (2003).

states determined that public shaming should not be used and that it did little to combat recidivism.[103] Many courts decided shaming is not appropriate to use in sentencing for criminal conduct for purposes of humiliation or embarrassment.[104]

While courts have frowned upon the use of public shaming for punishment, there has been a rise in the use of social media for public shaming.[105] In *Hollis v. Cunningham*, a plaintiff sought to hold a social networking site operator liable for online public shaming.[106] Cunningham tried to use Section 230 of the Communications Decency to act as a shield, stating in her Amended Answer and Defenses to the Amended Complaint that she was not a content provider as defined by the Act.[107] *Hollis* involved a former-lover-shaming site, DontDateHimGirl.com, that allowed individuals to post photos of ex-lovers and personal details about the relationship.[108] This case was the first of many in which a plaintiff sought damages for online shaming from a website operator.[109] The plaintiff in *Hollis* sought to hold the site operator liable under the theory that the site operator allowed and categorized anonymous posts by users.[110] Therefore, the theory is that liability should rest with the site operator, since there was no way to hold an anonymous poster liable.

The plaintiff in *Hollis* alleged that the posts made by several different women were false and defamatory, characterizing him as "cheater," and that "he wears dirty clothes."[111] Comments about Hollis included, "Chocolate Attorney Hollis: This jerk gave me herpes . . . He

---

[103] State v. Scott, 961 P.2d 667, 675 (1998); *Smith*, 538 U.S. at 98.
[104] *See, e.g.*, Aaron S. Book, *Shame On You: An Analysis of Modern Shame Punishment as an Alternative to Incarceration*, 40 WM. & MARY L. REV. 653, 667 (1999).
[105] *See* David Reutter, *For Shame! Public Shaming Sentences on the Rise*, PRISON LEGAL NEWS (Feb. 4, 2015), https://www.prisonlegalnews.org/news/2015/feb/4/shame-public-shaming-sentences-rise.
[106] Second Am. Compl. at 9, Hollis v. Cunningham, No. 07-23112 CIV-ALTONAGA/ Turnoff, 2008 WL 11417652 (S.D. Fla. Feb. 6, 2008) (No. 07-23112), 2008 WL 2472888.
[107] Defs.' Am. Answer and Defenses to the Am. Compl. at 2, Hollis v. Cunningham, 2008 WL 11417652 (S.D. Fla. Feb. 6, 2008) (No. 07-23112), 2008 WL 2472887.
[108] Second Am. Compl., *supra* note 106.
[109] *See, e.g.*, Sabbato v. Hardy, No. 2000CA00136, 2000 WL 33594542 (Ohio Ct. App. Dec. 18, 2000); Tabor v. Willey, No. C01-1002 MJM, 2001 WL 34152085 (N.D. Iowa May 3, 2001); Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003); Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006); Dimeo v. Max, 433 F. Supp. 2d 523 (E.D. Pa. 2006), *aff'd*, 248 F. App'x 280 (3d Cir. 2007).
[110] Second Am. Compl., *supra* note 106, ¶ 12.
[111] Second Am. Compl., *supra* note 106, ¶ 4.

tried to pay me to have sex after we broke up, what a jerk . . . Beware girlfriends. He is no chocolate, but rather poo-poo."[112]

Hollis contended that the site operator created categories, "actively participated in the writing and preparation of the profiles," and added additional content for the fabricated postings.[113] In response to the suit, Cunningham argued that the Section 230 of the Communications Decency Act, which immunizes website hosts against liability for messages posted by others, protected her.[114] She added that DontDateHimGirl.com is no different from any other site on the web that provides information and that the website gives people the perfect platform to disclose whatever information they see fit.[115] In June of 2008, the case was settled by the parties and the judge dismissed the case.[116]

C. *Sarah Jones v. Dirty World Entertainment Recordings, LLC*

TheDirty.com, a gossip website that allows users to post photos, anecdotes, and rumors about everyday people or celebrities, is the defendant in the last of the trilogy of cases reviewed in this essay.[117] TheDirty.com became the subject of a lawsuit by one of the targets of a third-party post.[118] Jones, a high school teacher at the time, sued the operators of TheDirty.com after the gossip website posted that she contracted sexually transmitted diseases from her ex-boyfriend and that he had bragged about having sex with her on the football field and in her classroom.[119] The excerpt below is what sparked Jones' outrage:

> Nik, here we have Sarah J, captain cheerleader of the playoff bound cinci bengals. . Most ppl see Sarah has [*sic*] a gorgeous cheerleader AND highschool teacher. . . yes she's also a teacher. . but what most of you don't know is. . Her ex Nate. . . cheated on her with over 50 girls in 4 yrs. . . in that time he tested positive for Chlamydia Infec-

---

[112] Leslie Yeransian, *Women Rat, Man Sues*, ABC NEWS (July 18, 2006, 9:27 AM), http://abcnews.go.com/US/LegalCenter/story?id=2184494&page=1.
[113] Second Am. Compl., *supra* note 106, ¶ 35.
[114] Defs.' Am. Answer and Defenses to the Am. Compl., *supra* note 107, ¶ 140.
[115] Defs.' Am. Answer and Defenses to the Am. Compl., *supra* note 107, ¶ 65.
[116] *Hollis v. Cunningham*, DIGITAL MEDIA LAW PROJECT (June 20, 2008), http://www.dmlp.org/threats/hollis-v-cunningham.
[117] Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398 (6th Cir. 2014).
[118] *Id.*
[119] *Id.* at 403.

> tion and Gonorrhea. . . so i'm sure Sarah also has both. . . whats worse is he brags about doing sarah in the gym. . football field. . her class room at the school she teaches at DIXIE Heights.[120]

Hooman Karamian, the founder of TheDirty.com and better known as Nik Richie, then added his own comment to the post: "Why are all high school teachers freaks in the sack? — nik."[121] This case truly pushed the limits of the protections afforded by Section 230 of the Communications Decency Act. The case sought to determine whether a website operator like Richie could establish immunity under Section 230 of the Communications Decency Act for objectionable posts by third parties that contained commentary by the website operator.[122]

Jones argued that the posts were false and malicious and that they caused her severe mental anguish.[123] Richie denied any malice and indicated that he did not write the false posts.[124] Jones requested that the post be removed by sending over twenty-seven emails to Richie.[125] She stated that she was concerned about how it would affect her job.[126] Richie told her that the posts would not be removed.[127] Richie's lawyers contended that the Communications Decency Act protects Richie as the operator of a website that allows third-party posts and that holding him responsible for such posts, "would have a negative impact on free speech" and on other websites that host forums of discussion.[128] Further, Richie's lawyers argued that this type of liability is precisely what Section 230 of the Communications Decency Act guards against.[129] An initial trial resulted in a hung jury.[130] Later, a jury of eight women and two men found that the

---

[120] *Id.*
[121] *Id.* at 404.
[122] *Id.* at 402.
[123] *Id.*
[124] Appellant's Opening Br. at 9, Jones v. Dirty World Entm't Recordings LLC, 965 F. Supp. 2d 819 (E.D. Ky. 2013), r*ev'd and vacated*, 755 F.3d 398 (6th Cir. 2014).
[125] *Jones*, 755 F.3d at 404.
[126] *See* Appellee Sarah Jones's Resp. Br. at 4, Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398 (6th Cir. 2014) (No. 13-5946) 2013 WL 6823689.
[127] *Id.* at 403.
[128] Lisa Cornwell, *Jury Finds Website Defamed Ex-Bengals Cheerleader*, AP NEWS (July 11, 2013), https://apnews.com/article/46bbb7d094ce4381bbb8a0c2a74f2232.
[129] Jones v. Dirty World Ent. Recordings, LLC, 965 F. Supp. 2d 818, 819 (E.D. Ky. 2013).
[130] *Id.*

posts were false and Richie was guilty of libel.[131] The jurors also found Richie acted with malice or reckless disregard in the case by posting anonymous submissions.[132]

The district court ruled that the website was not shielded from liability by Section 230 of the Communications Decency Act because Richie invited people to post "dirt" and comments on the submitted posts.[133] The district court opined that the Communications Decency Act "was intended only to provide protection for site owners who allow postings by third parties without screening them and those who remove offensive content."[134] The court concluded that although the immunity provided by Section 230 of the Communications Decency Act is broad, there are certain circumstances under which the immunity may be lost.[135] The district court concluded that Richie's commentary was one of such circumstances.[136]

On appeal, the Sixth Circuit Court of Appeals found that while the content published by the third-party user-generated online tabloid was defamatory, neither Richie nor TheDirty.com were the creators nor the developers of the defamatory content at issue.[137] The court opined that Jones' tort claims were "grounded on the statements of another content provider" yet sought to impose liability on the hosts "as if they were the publishers or speakers of those statements."[138] The court reasoned that because the comments could not be attributed to Richie or TheDirty.com, Section 230(c)(1) of the Communications Decency Act barred Jones' claims.[139] The Sixth Circuit reversed "the district court's denial of Dirty World's and Richie's motion for judgment as a matter of law with instructions to enter judgment as a matter of law in their favor."[140]

---

[131] Cornwell, *supra* note 128.
[132] *Id.*
[133] Jones v. Dirty World Entm't. Recordings, LLC, 840 F. Supp. 2d 1008, 1012–13 (E.D. Ky. 2012).
[134] *Jones*, 956 F.Supp.2d at 822; David Klein, *Court of Appeals Reverses Decision: Website "Thedirty.Com" Entitled To CDA § 230 Immunity*, MONDAQ.COM (Aug. 5, 2014), https://www.mondaq.com/unitedstates/it-and-internet/332594/court-of-appeals-reverses-decision-website-thedirtycom-entitled-to-cda-230-immunity?type=mondaqai&score=67&signup=true.
[135] *Jones*, 840 F. Supp. 2d at 1011.
[136] *See id.* at 1013.
[137] Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 402 (6th Cir. 2014).
[138] *Id.*
[139] *Id* at 417.
[140] *Id.*

Without question, new media types have transformed privacy expectations. This invites the question of whether traditional rules of ethics and tort law apply to new media platforms. All three cases in this essay featured examples of cybertorts that used shaming and ridicule to exact revenge. The individuals who posted the content wanted to make a point or to embarrass. However, the circumstances surrounding each case led to varying results. In these three case studies, while the internet enabled greater exposure to content posted about the victims and potentially increased the impact they may have on each person, the platform did not change the underlying nature of the comments, photos, or videos themselves.

These cases provide the means to explore the distinction between publishing platforms. The key idea here is that Internet intermediaries are "platforms," whereas newspapers are "publishers"—a distinction that has significant legal consequences, particularly as to the applicability of CDA 230 as a defense to a defamation claim. In each case, individuals used social media to post or to disseminate unflattering information. In all three studies, the content posted on third-party websites attacked the person's character and depicted him or her in an unflattering manner.

GirlDontDateHim.com, Myspace, and TheDirty.com are all social media platforms that allow users to post. The facts of each case reviewed in this essay, involving these platforms, gave rise to a cybertort. Jones and Hollis argued that the owners of websites that published content about them created headlines and additional content for the defamatory postings.[141] They also stated that the postings about them were false and had hurt them personally and professionally.[142] Hollis also provided the rationale that because Joseph-Cunningham's company put headings on the false statements, she effectively vouched for the content.[143] In Jones' case, her attorney stated that Richie selected certain posts and added his own commentary to the defamatory comments.[144] At first, the district court judge rejected Richie's Section 230 claim.[145] Jurors concluded that Richie acted with malice or reckless disregard in posting anonymous sub-

---

[141] *Id.* at 403; *See* Am. Compl. ¶ 31, Hollis v. Cunningham, (S.D. Fla. Feb. 6, 2008) (No. 07-23112-CIV), 2008 WL 538857.
[142] *Jones*, 755 F.3d at 405; *See* Am. Compl. ¶ 71, Hollis v. Cunningham, (S.D. Fla. Fedb. 6, 2008) (No. 07-23112-CIV), 2008 WL 538857.
[143] Pl.'s Resp. in Opp'n to Def. the Cavelle Company, Inc.'s Mot. to Compel, Hollis v. Cunningham, (S.D. Fla. Feb. 6, 2008) (No. 07-23112-CIV), 2008 WL 2200984.
[144] Appellee Sarah Jones's Resp. Br, *supra* note 126, at 13.
[145] *Jones*, 965 F. Supp. 2d 818, 823 (E.D. Ky. 2013).

missions.[146] Richie argued that he was not required to fact-check anonymous submissions before posting them because such websites are protected under the federal Communications Decency Act.[147] Richie argued further that holding the site operator responsible for posts created by a third party would have a negative impact on free speech for other people and other websites.[148]

In addition to the platform on which the comments were published, judges also took into consideration the content of the posts.[149] The circumstances were different in the case studies. For instance, former lover shaming websites allow individuals to post information about other people. However, audiences know the websites are created specifically for shaming. In our case studies, individuals posted content on the former-lover websites that a court would likely find to be mere opinion because readers of the content could more than likely than not ascertain that the posts were from an angry former girlfriend or spouse.[150]

Hollis alleged defamation, intentional infliction of emotional distress, and false light invasion of privacy.[151] Defendants in *Hollis* argued they were entitled to summary judgment on several of the plaintiff's claims because certain examples of the disputed content were true and certain examples were entitled to protection under Section 230 of the Communications Decency Act.[152] The merits of the Defendants' arguments in *Hollis* ultimately were not decided.[153] Hollis and Cunningham reached a settlement and the judge dismissed the case with prejudice.[154]

In *Jones*, Richie, the website owner, did substantially more than provide the platform for third parties to post. Richie selected certain posts and added his own commentary.[155] Indeed, one such post was alleged to be defamatory.[156] At first, the court rejected Richie's claim of immunity

---

[146] Appellee Sarah Jones' Resp. Br., *supra* note 126, at 12.
[147] Appellant's Opening Br., *supra* note 124, at 50.
[148] *See id.* at 24.
[149] *See* Jones v. Dirty World Entertainment Recordings LLC., 755 F.3d 398, 410 (6th Cir. 2014).
[150] *See id.* at 403; *See* Hollis v. Cunningham, No. 07-23112-CIV, 2008 WL 11417652, at *2 (S.D. Fla. Feb. 6, 2008).
[151] Second Am. Compl., *supra* note 106, at 2.
[152] Defs.' Am. Answer and Defenses to the Am. Compl., Hollis v. Cunningham, No. 07-23112-CIV, 2008 WL 2472887, ¶¶ 140, 147.
[153] *See Hollis v. Cunningham, supra* note 116.
[154] *Id.*
[155] Jones v. Dirty World Ent., 755 F.3d 398, 402 (6th Cir. 2014).
[156] *Id.* at 403.

under Section 230 of the Communications Decency Act.[157] The court concluded that Richie acted "with malice or reckless disregard" in posting anonymous submissions and commenting without first fact checking.[158]

Critics agreed with Richie's assertions. For instance, while describing TheDirty.com as "a tasteless website," The Citizen Media Law Project suggested the ruling could have a "chilling effect" for online speech, which is fairly common with these types of cases.[159] Robinson writes:

> In the Internet context, Section 230 was enacted to prevent a "chilling effect" that the threat of litigation would have on discussion on the Internet . . . . In Sarah Jones' case against TheDirty.com, there may indeed be disputed evidence of the website's involvement in soliciting tortious statements from users; and perhaps enough evidence for Section 230 to not apply. But courts should tread a cautious line here, and not turn Section 230 into a paper tiger that does not impose any real impediment to plaintiffs' lawsuits against web sites.[160]

It is worth noting that the Communications Decency Act does not always provide immunity to content hosts. *Fair Housing Council v. Roommates.com, LLC*, explores the Communication Decency Act in a context of disclosure of personal information that might be used to discriminate and/or shame.[161] Roommates.com operates a web-based business designed to match roommates.[162] Before a subscriber to Roommates.com's services could search listings or post housing availabilities on the website, they were required to create a profile containing basic information about themselves, such as their name, the location of the property, and their email address.[163] In addition, Roommates.com required the disclosure of sex, sexual orientation, and whether there would

---

[157] *Id.*
[158] Cornwell, *supra* note 128.
[159] Eric P. Robinson, *Sixth Circuit's 'Dirty' Decision Sends a Chill*, DIGITAL MEDIA LAW PROJECT (June 7, 2012), http://www.dmlp.org/blog/2012/sixth-circuits-dirty-decision-sends-chill.
[160] *Id.*
[161] Fair Hous. Council of San Fernando Valley v. Roommate.Com, L.L.C., 521 F.3d 1157 (9th Cir. 2008).
[162] *Id.* at 1161.
[163] *Id.*

be children in the household.[164] These same questions were included in the subscriber's preference.[165] The site also allowed for additional comments from the users.[166]

The Fair Housing Councils of San Fernando Valley and San Diego sued Roommates.com alleging that the website's questionnaire, requiring the disclosure of sex, sexual orientation, and family status violated the Fair Housing Act, 42 U.S.C. § 3601 and California's housing discrimination laws.[167] The district court initially dismissed the claims against Roommates.com, finding that the company was immune under Section 230 of the Communications Decency Act.[168] Specifically, the district court found that Section 230 of the Communications Decency Act immunized website operators who do not provide the content.[169]

The case on appeal to the Ninth Circuit turned on whether the required questionnaire and answers, once selected by users, constituted content provided by Roommates.com or by "another information content provider" as required under Section 230 of the Communications Decency Act in order to qualify for immunity.[170] Roommates.com argued that it was not responsible for the information on the page because the subscriber's actions led to the publication of the information.[171] However, a look at Roommates.com's use of service requirements revealed that, as discussed above, the website required the initial disclosures prior to use of the services, which could not be refused if the subscriber wished to use the services.[172] With this information, the Court of Appeals reasoned that by requiring information as a condition of service Roommates.com was acting as more than a passive website.[173] In other words, providing a prepopulated set of answers that are selected by users does not constitute information provided by "another information content provider," but rather content developed by the website.[174] This type of content develop-

---

[164] *Id.* at 1165.
[165] *Id.* at 1161–1162.
[166] *Id.* at 1161.
[167] *Id.* at 1162.
[168] *Id.*
[169] *Id.*
[170] *Id.* at 1162–64.
[171] *Id.* at 1166.
[172] *Id.*
[173] *Id.*
[174] *Id.*

ment, the court reasoned, is not subject to immunity under the Communications Decency Act.[175]

Section 230 of the Communications Decency Act has at least allowed the creation of modern digital countercultures that are responsible for the use of social media platforms in ways that are tortious. Because many social media sites have taken a hands-off approach to moderating their platforms, the tortious actions of users continue with impunity. In enacting Section 230 of the Communications Decency Act, Congress left room for moderating to decrease the behavior that we see today and relied on self-governance to police bad behavior online. It is highly likely that the absence of Section 230 of the Communications Decency Act would not change the behavior that has developed online, but would go a long way to hold sites responsible for some of the tortious conduct. Ultimately, cybertorts are traditional torts on a digital platform. Likewise, these harassment behaviors that exist in the physical world proliferate in the digital world, but their roots are the same. And while we can attempt to make such acts more difficult, the law cannot cure human nature.

IV. Conclusion

Today, user-generated content and social media sites provide users the chance to have their voices heard about topics that they may feel strongly about. Messages of today are not confined to small circles or groups of friends and acquaintances. Instead, messages of today are spread among large social media networks that amplify them, in some cases exponentially (i.e., "going viral"). Sites such as GirlDontDateHim.com, Facebook, Twitter, TheDirty.com, and LiarsandCheatersRUs.com have become a platform for expression. Posting comments on a page can be cathartic and offer a safe haven for individuals to express themselves in an environment without feeling someone may retaliate against them publicly. The nature of online posting and commenting provides a buffer from face-to-face confrontations. However, as the case studies presented in this Essay demonstrate, posting online does not fully insulate or protect individuals from the scathing critiques or cyberbullying of others.

The three cases highlighted in this Essay exemplify forms of cybertorts that have developed as a result of the rise in popularity of public shaming in social media. While these cases do not represent all

---

[175] *Id.*; *See also* 47 U.S.C.A. § 230(f)(3) (West). (providing the statutory definition of internet content provider).

privacy cases, they are nonetheless valuable in providing insight into the problems faced with "cybertorts." Indeed, these cases point to how computer, defamation, and privacy regulations have been inadequate in addressing these new "cybertorts." Notwithstanding, these "cybertorts" should have legal repercussions. All states have laws addressing forms of bullying in the physical world.[176] As an example, assault, battery, and intentional infliction of emotional distress are widely recognized causes of action. In the digital world since *Drew*, 48 states have specifically included cyberbullying in their bullying laws, and most of them have introduced criminal sanctions for such behavior.[177]

Similarly, anti-stalking laws and recognized privacy torts, such as intrusion upon seclusion, should be similarly applied to their digital counterpart of cyberstalking. Doxing is merely the digital manifestation of public disclosure of private facts. Texas has enacted statutes which forbid stalking through digital means.[178] Cyberstalking can be prohibited through anti-harassment legislation even in jurisdictions that lack specific cyberstalking laws.[179] In the absence of any uniform laws addressing these concerns, we propose that a uniform code of these cybertorts be presented to the states in favor of consistency and predictability. State borders do not exist in the digital world, yet state laws can vary. Functioning like a Restatement, this uniform proposal would leave the states with the option to adopt the provisions they each feel would be appropriate within its own statutory scheme and case law. Meanwhile, users and ISPs would benefit from consistent, expressly-stated policies across jurisdictions.

Another proposed solution to the apparent gaps in Section 230's legislation is to amend the statute with notice and takedown procedures. In her article "The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given," Patricia Spiccia proposes legislation which would require ISPs to follow specific procedures set out by

---

[176] *See Bullying Laws Across America*, CYBERBULLYING RES. CTR., https://cyberbullying.org/bullying-laws (last visited Jan. 2, 2021).
[177] *Id.*
[178] TEX. PEN. CODE ANN. § 33.07 (West 2011); TEX. PEN. CODE ANN. § 42.07 (West 2017).
[179] Ashley Perna, *Cyberstalking: Definition, Laws, and How to Stay Safe*, PRIVATEINTERNETACCESS: PRIVACY NEWS ONLINE (Jan. 5, 2019), https://www.privateinternetaccess.com/blog/2019/01/cyberstalking-definition-laws-and-how-to-stay-safe.

Congress in order to earn Section 230's protection.[180] One requirement would be that a given ISP must have a set take-down procedure in place, much like the requirements that exist for the Digital Millennium Copyright Act.[181] Further, she proposes a division of the Federal Communications Commission be solely dedicated to analyzing, evaluating upon notice, and notifying parties of defamatory material.[182] This model is a good solution because it requires ISPs to have a minimum threshold of self-moderation in order to receive the benefits of Section 230.[183]

Unfortunately, neither proposal is a perfect solution. Spiccia's proposal does not specifically address the fact that it is still difficult to impose liability on the poster of such content. However, her proposed legislation would at a minimum provide some redress to the symptoms of these "cybertorts," even if it does not solve the overall problem. Using this system to address these problems lessens the need to use a case-by-case analysis each time an incident occurs. Prospective plaintiffs should be given more tools to prepare and adjudicate their claims within existing legal procedures. While the law will continue to evolve and attempt to fix such issues, it is unlikely that any total, all-encompassing solution exists—at least not one that does not infringe on First Amendment protections. On the other hand, our proposal lacks the guarantee that any state would actually adopt it. There are plenty of proposed codes that have been adopted by only one or two states, but ignored by the others. In addition, even if every state adopts such a code or restatement, that does not mean they will each apply it consistently.

Undoubtedly, we will see more cases like these as new social media platforms are developed and continue to grow in popularity. Eventually, each case highlighted above dropped out of the news cycle. However, they served to stimulate ongoing and ever-evolving discussions on the topic. Although privacy might be a problem "for anyone who leads a life mediated in part by digital technologies," the

---

[180] Patricia Spiccia, Note, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given*, 48 VAL. U.L. REV. 369, 411 (2013).
[181] *Id.* at 411–12; Digital Millennium Copyright Act 17 U.S.C. § 512(c) (2018).
[182] Spiccia, *supra* note 180, at 411–12.
[183] *Id.*

problem is said to be more acute for young people because "we are just at the beginning of the digital age."[184]

[184] JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 61–62 (2008).

Product Liability's Amazon Problem

Sean M. Bender*

Throughout its rise from a startup bookseller to the world's most valuable company, Amazon has managed to disrupt nearly every aspect of the twentieth-century retail model. Its website now accounts for over half of all online shopping in the United States, acting as a literal "Everything Store" for the millions of customers who browse its virtual catalog each day. But Amazon is more than just a store—in addition to selling its own products, its marketplace lists the goods sold by hundreds of thousands of independent merchants. By some estimates these third-party sellers now account for over 60% of Amazon's transactions, while the fees collected from these sales now make up one of the company's most important revenue streams.

As Amazon has reinvented retail, tort law has struggled to keep up. Modern product liability doctrines were developed at a time when supply chains were linear and market participants could be neatly cabined into roles like "seller" or "manufacturer." By design, Amazon's business model disrupts that paradigm, removing the middlemen between manufacturers and consumers while reducing the friction that might keep foreign (or otherwise judgment-proof) manufacturers from putting dangerous products on the market. And while courts have readily held its third-party merchants strictly liable when they sell defective products through Amazon's website, Amazon's own role in these transactions is far less clear.

This Article proceeds in three parts. Part I begins with an overview of contemporary product liability law,

---

* Class of 2021, University of Pennsylvania Law School. My thanks to Professors Tom Baker and Tess Wilkinson-Ryan for their feedback and support, and to Jacob Marsh for his helpful suggestions. All errors are my own.

discussing the origins of the strict liability rule and the rise of the Restatement (Second)*'s approach to no-fault recovery. Part II focuses on the doctrine's application to Amazon, tracking the outcome of every product liability lawsuit filed against the company between January 2015 and December 2020. Finally, Part III is prescriptive, discussing both why and how courts should respond to Amazon's disruption of product liability law.*

"Precedents drawn from the days of travel by stagecoach do not fit the conditions of travel today."[1]

– BENJAMIN CARDOZO, *MacPherson v. Buick Motor Co.*

"Third-party sellers are kicking our first party butt. Badly."[2]

– JEFF BEZOS

Introduction

In 1957, when William Greenman decided to buy a lathe attachment for his Shopsmith combination power tool, he went to his local

[1] MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916).
[2] Amazon.com, Inc., 2018 Letter to Shareholders (Form 8-K) (Apr. 11, 2019).

retail merchant: a hardware store called The Hayseed.[3] Had Mr. Greenman made a similar purchase in 2020, he may instead have turned to Amazon.com, the e-commerce juggernaut that last year captured nearly half of all online spending in the United States.[4] Back in 1957, when the lathe's defective design landed Mr. Greenman in the hospital, the identity of the tool's manufacturer (Yuba Power Products, Inc.) and seller (The Hayseed) were readily apparent, allowing him to target both in his ensuing product liability lawsuit.[5] But today, for the Amazon-purchased power tool, it might not be so simple.

Amazon is often thought of as an online retailer, and that was an apt enough description when the site launched in 1995. Beginning with a single product line (books) before eventually expanding into dozens of others, the company's initial business model consisted of purchasing bulk inventory from distributors at wholesale prices and then reselling these goods through its website at retail prices.[6] In that way, it was no different from a digital version of The Hayseed or any other twentieth-century retail establishment. But since the early aughts, Amazon's business model has changed considerably; now when customers make purchases through its digital storefront, "odds are, [they] aren't buying it from Amazon at all."[7] Last year, third-party merchants who use the website as a sales platform accounted for more than 60% of the website's total transactions, bringing in more than $200 billion in revenue.[8] And beyond volume, the service fees paid by these third-party sellers now constitute Amazon's second largest revenue segment, generating $53.76 billion in 2019.[9]

---

[3] Greenman v. Yuba Power Products, Inc., 377 P.2d 897, 897–98 (Cal. 1963).
[4] *Digital Investments Pay Off for Walmart in Ecommerce Race*, EMARKETER (February 14, 2019), https://www.emarketer.com/content/digital-investments-pay-off-for-walmart-in-ecommerce-race.
[5] *Greenman*, 377 P.2d at 898.
[6] BRAD STONE, THE EVERYTHING STORE: JEFF BEZOS AND THE AGE OF AMAZON 35–38 (2013); *see also* Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 985 (2019) [hereinafter Khan, *Separation*] ("In Amazon's early days, it operated primarily as an online retailer.").
[7] Josh Dzieza, *Prime and Punishment: Dirty Dealing in the $175 Billion Amazon Marketplace*, THE VERGE (Dec. 19, 2018), https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appeal-reinstatement.
[8] *Sellers on Amazon*, MARKETPLACE PULSE, https://www.marketplacepulse.com/marketplaces-year-in-review-2019.
[9] AMAZON.COM, INC., ANNUAL REPORT (FORM 10-K) 92 (Jan. 31, 2020) [hereinafter AMAZON'S ANNUAL REPORT].

The rise of these third-party sellers has tested the limits of product liability law, much of which was developed at a time when supply chains were linear and actors could be neatly cabined into roles like "seller," "distributor," or "manufacturer."[10] By design, e-commerce has disrupted that retail model, "cut[ting] out the middlemen between manufacturers and consumers, reducing the friction that might keep foreign (or otherwise judgment-proof) manufacturers from putting dangerous products on the market."[11] Amazon's website now allows users to browse products sold by more than one million sellers, purchase these products using Amazon's payment system, and receive them two days later in Amazon Prime shipping containers.[12] But if the products turn out to be defective and as a result injure their purchaser, Amazon is almost always able to avoid legal consequences by arguing that its role in these sales is merely that of a facilitator—connecting independent sellers with customers in a manner that does not create liability.[13]

Amazon's near immunity from liability for its customers' injuries poses a problem to product liability doctrine. Since the "fall of the citadel"[14] more than fifty years ago, it has been black letter law that product liability operates through a strict liability regime, permitting consumers to recover damages without proving either a breach of warranty or fault.[15] This is not to say that strict liability is uncontroversial; to the contrary, its critics are legion, and the litigious behavior this system is said to inspire has been a frequent target of industry lobbying and legislative tort-reform efforts.[16] Still, it remains the case that the law on the books in almost

---

[10] *See* Benjamin Edelman & Abbey Stemler, *From the Digital to the Physical: Federal Limitations on Regulating Online Marketplaces*, 56 HARV. J. ON LEGIS. 141, 143 (2019) ("Historically, most businesses followed a linear business model, focused primarily on creating goods and services to sell to distributors or customers.").

[11] Erie Ins. Co. v. Amazon.com, 925 F.3d 135, 144 (4th Cir. 2019) (Motz, J., concurring).

[12] Amy Elizabeth Shehan, Note, *Amazon's Invincibility: The Effect of Defective Third-Party Vendors' Products on Amazon*, 53 GA. L. REV. 1215, 1218 (2019).

[13] *Id*. at 1224–25.

[14] William L. Prosser, *The Fall of the Citadel (Strict Liability to the Consumer)*, 50 MINN. L. REV. 791 (1966) [hereinafter Prosser, *Fall*].

[15] JOHN C.P. GOLDBERG ET AL., TORT LAW: RESPONSIBILITIES AND REDRESS 893-94 (4th ed. 2016).

[16] *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 1 cmt. e, reporters' note 1 (AM. L. INST. 1998) ("The legislative response to the common-law rule has been varied. . . . A host of statutes bar an action for strict liability depending on whether jurisdiction may be obtained against the manufacturer and whether the manufacturer is able to satisfy a judgment.").

every state envisions some degree of no-fault recovery when consumers are injured by defective products.[17] Yet when these defective products are purchased from the website of one of the country's largest and most profitable companies, the law in action plays out quite differently.

This Article proceeds in three parts. Part I begins with an overview of contemporary product liability law, discussing the origins of the strict liability rule and the rise of the *Restatement (Second)*'s approach to no-fault recovery. It then outlines the debates that have surrounded this regime ever since, noting both the policy justifications used to support strict liability's extension and some of the ways in which courts and legislatures have acted to constrain its reach.

Part II of this Article is descriptive. After briefly outlining Amazon's history and business model, it reviews an original, hand-coded dataset assembled to track the outcome of every product liability lawsuit filed against the company between January 2015 and December 2020. This review confirms what has long been reported anecdotally: Amazon's customers are rarely successful in holding the company liable for defective products sold by its third-party vendors, even when those vendors cannot be sued directly because of insolvency, extraterritoriality, or both. Amazon has achieved these outcomes by wielding two primary arguments: its role as a sales platform (vice retail merchant), and its supposed immunity under Section 230 of the Communications Decency Act.[18] And as the data make clear, Amazon has litigated these questions almost exclusively in federal forums, "arguably stunt[ing] the development of state law."[19] This Part concludes by using *Erie Insurance Company v. Amazon.com*[20] as a case study for the typical progression of these lawsuits.

Finally, Part III is both normative and prescriptive. It first makes the case that Amazon should be strictly liable for defective products sold by its third-party sellers. Amazon's role in these transactions is certainly an awkward fit within the existing product liability doctrine, but "doctrinal analysis is essentially static—an organizing tool but little more—unless it is attentive to the policy concerns that channel discretion in one

---

[17] 1 DAVID OWEN & MARY DAVIS, OWEN & DAVIS ON PROD. LIAB. § 5:7 (4th ed. 2020).
[18] 47 U.S.C. § 230 (2018).
[19] Erie Ins. Co. v. Amazon.com, 925 F.3d 134, 145 (4th Cir. 2019) (Motz, J., concurring).
[20] Erie Ins. Co. v. Amazon.com, No. 16-02676-RWT, 2018 WL 3046243 (D. Md. Jan. 22, 2018), *aff'd in part, rev'd in part*, 925 F.3d 135 (4th Cir. 2019).

direction or another."[21] Amazon plays just as integral a role in placing goods into the stream of commerce as did its twentieth-century retail counterparts. And just as courts once abandoned the privity rule and then later embraced strict liability, tort law must once again evolve to meet the challenges of a changing economy. Thus, this Article concludes by discussing both how and why courts should respond to "Amazon's invincibility."[22]

I. The Fall of the Citadel and the Rise of Strict Liability

For more than half a century, the manufacturers, sellers, and distributors of defective goods have been subject to a special set of tort doctrines grouped together under the banner "product liability law." This Part begins by reviewing the origins and development of those doctrines, noting some of the theoretical and policy justifications that have helped ensure their widespread acceptance. It then briefly surveys some of the ways in which states have departed from those common law doctrines through various statutory enactments.

A. Liability Without Fault

Suppose you decide to purchase a car. After researching makes and models, you visit a dealership, examine its inventory, and perhaps take a car or two out for a test drive. Then, satisfied with the appearance and performance of your choice, you negotiate an acceptable price, arrange for financing, sign the title, and drive the car off the lot. Now suppose that unbeknownst to you, and far beyond your ability to inspect, there is a small defect in the car's steering column that has weakened the metal's integrity. The car drives fine for several months, but one day while you are driving down the highway, the column finally fails, snapping in two and spinning you off the road. As a result of the crash, the car is totaled, and you find yourself in the hospital facing serious medical bills.[23] What happens next?

If the crash had taken place before the 1960s, American law would have provided you with two avenues for recovering monetary damages. First, under the original language of U.C.C. § 2-314 (and to

---

[21] Robert L. Rabin, *The Duty Concept in Negligence Law: A Comment*, 54 VAND. L. REV. 787, 794 (2001).
[22] *Cf.* Shehan, *supra* note 12.
[23] These facts were loosely adopted from Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960).

some degree, under the preceding Uniform Sales Act),[24] every sale was accompanied by an implied warranty that the purchase was "fit for the ordinary purposes for which such goods are used."[25] This created a kind of strict liability in contract: regardless of the care exercised by the merchant, a product defect constituted a breach and gave rise to a cause of action.[26] However, this theory of liability suffered from several key limitations. For one, because the implied warranty was said to arise from a contractual relationship, it could only be asserted by parties in privity with one another.[27] Thus, while you would have been able to sue the dealer for selling you a lemon, any passengers in the car could not have joined the lawsuit, nor could you have pursued a parallel claim against the automaker or its vendors. Additionally, both the U.C.C. and the Uniform Sales Act permitted retailers to disclaim any implied warranties and obviate any chance of recovery through careful contract drafting.[28] Finally, warranty law's strict notice requirements would have presented you with significant procedural barriers.[29]

---

[24] *See* SAMUEL WILLISTON, THE LAW GOVERNING SALES OF GOODS AT COMMON LAW: AND UNDER THE UNIFORM SALES ACT 439 (2d ed. 1924) ("An implied warranty or condition as to quality or fitness for a particular purpose may be annexed by the usage of trade.").

[25] U.C.C. § 2-314(2)(c) (AM. L. INST. & UNIF. L. COMM'N 1952).

[26] *See* Kyle Graham, *Strict Products Liability at 50: Four Histories*, 98 MARQ. L. REV. 555, 571 (2014) ("Liability under an implied-warranty theory was therefore 'strict' in a manner that negligence liability was not."); *see also* Marc A. Franklin, *When Worlds Collide: Liability Theories and Disclaimers in Defective-Product Cases*, 18 STAN. L. REV. 974, 990 (1966) ("The contract-warranty doctrine amounted to liability without fault for product defects.").

[27] *See* William L. Prosser, *The Assault Upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099, 1117–18 (1960) [hereinafter Prosser, *Assault*] ("[S]o long as the privity wall stands firm, these warranties are of no avail against the wholesaler . . . .").

[28] U.C.C. § 2-316(2)(a) (AM. L. INST. & UNIF. L. COMM'N 1952) ("[A]ll implied warranties are excluded by expressions like 'as is', 'as they stand', 'with all faults', or other language which in common understanding calls the buyer's attention to the exclusion of warranties and makes plain that there is no implied warranty."); WILLISTON, *supra* note 24, at 475 ("[A] seller may by appropriate words exclude all liability."). *See, e.g.*, Allis-Chalmers Mfg. Co. v. Hawhee, 105 P.2d 410, 412 (Okla. 1940) ("Both under the Uniform Sales Act and in states not having that provision, stipulations negativing implied warranties have been held valid and effective by the courts almost unanimously . . . .").

[29] Richard E. Speidel, *The Virginia "Anti-Privity" Statute: Strict Products Liability Under the Uniform Commercial Code*, 51 VA. L. REV. 804, 834 (1965) ("Any attempt to use Article 2 of the Uniform Commercial Code as a vehicle for imposing strict liabil-

Alternatively, you might have been able to bring a tort action, arguing that the steering column was defective because it had been cast, assembled, or installed in a negligent manner. Unlike your warranty claim, this suit would have been brought against any party in the car's distribution chain; by the middle of the twentieth century, privity had long since faded as a requirement in negligence suits, "succumb[ing] eventually to the force of Cardozo's reasoning" from the landmark case *MacPherson v. Buick Motor Co*.[30] Yet this approach would have also had its downsides. Most significantly—the difficulty in proving fault. In many product liability cases, the evidence of the alleged defect (say, a small crack in a pressurized soda bottle) is destroyed in the event precipitating the lawsuit, leaving nothing but witness testimony of what happened.[31] You might nevertheless have been able to succeed on a theory like *res ipsa loquitur*,[32] but there would have been no guarantee that a jury would accept this claim. And because growing distributions chains placed ever more intermediaries between the manufacturer and consumer, you might also have struggled to identify exactly which of the possible defendants was actually at fault.[33]

The burdens these rules placed on injured plaintiffs were readily apparent, and by the mid-twentieth century courts had begun riddling them with exceptions.[34] First to go were consumables. American courts have always placed special duties on purveyors of food and drink, duties that were then gradually broadened to encompass not only the immediate purchasers of contaminated foodstuff but also any subsequent consumer.[35] In language that would be echoed in Justice Roger Traynor's opinions a generation later, courts spoke of the serious consequences of tainted food,[36] the demands of public safety,[37] and consumers' inability to

---

ity upon sellers of goods to remote users or consumers must be prepared to deal with . . . the requirement of timely notice of breach.").

[30] James Henderson, Jr., MacPherson v. Buick Motor Company: *Simplifying the Facts While Reshaping the Law*, in TORTS STORIES 41, 65 (Robert L. Rabin & Stephen D. Sugarman, eds., 2003).

[31] *See* Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 438 (Cal. 1944) ("Plaintiff testified that after she had placed three bottles in the refrigerator and had moved the fourth bottle about 18 inches from the case 'it exploded in my hand.'").

[32] *See id.* at 440.

[33] G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 171 (expanded ed. 2003).

[34] DAVID G. OWEN, PRODUCTS LIABILITY LAW 18–19 (3rd ed. 2014).

[35] *Id.* at 248–49; *see also* Prosser, *Assault*, *supra* note 27, at 1107–08 (collecting cases).

[36] *See, e.g.*, Parks v. G.C. Yost Pie Co., 144 P. 202, 203 (Kan. 1914) ("The degree of care required of a manufacturer or dealer in human food for immediate consumption is

independently verify the safety of their purchases.[38] By the 1940s and 50s, courts were expanding this exception even further to encompass other consumer goods, first stretching the definition of "food" to include products like dog food and cigarettes, and then again to include other "articles for intimate bodily use" like hair dye, soap, and cosmetics.[39]

Coincident with this common law development was an important shift in legal scholarship that laid the intellectual foundation for the eventual rise of strict product liability.[40] By the 1940s, the Legal Realists—who generally advocated for grounding law in human experience and the realities of public policy[41]—had begun to focus their anti-formalist critique on what they viewed as the outsized role of fault within tort law. This, they claimed, arose from "archaic notions of behavior," while failing to ensure an adequate distribution of risk.[42] In their view, tort law ought to act as a form of social insurance, assigning liability in the manner that would best distribute losses and ensure recovery by injured plaintiffs.[43] This meant that when injuries were caused by defective products, "all limitations imposed by the doctrine of privity should go," permitting injured parties to sue the most "financially responsible" actor.[44] Even as Realism began to fade from prominence, its ideas about risk allocation and loss spreading continued to drive tort law scholarship, setting the stage for the coming acceleration towards no-fault recovery.[45]

---

much greater by reason of the fearful consequences which may result from what would be slight negligence in manufacturing . . . .").

[37] *See, e.g.*, Eisenbeiss v. Payne, 25 P.2d 162, 166 (Ariz. 1933) ("[P]ublic safety demands that there should be an implied warranty of its fitness for human consumption . . . ."); Race v. Krum, 118 N.E. 853, 854 (N.Y. 1918) ("The rule is an onerous one, but public policy, as well as the public health, demand such obligation should be imposed.").

[38] *E.g.*, Jacob E. Decker & Sons v. Capps, 164 S.W.2d 828, 829 (Tex. 1942) ("It is usually impracticable, if not impossible, for the ultimate consumer to analyze the food and ascertain whether or not it is suitable for human consumption.").

[39] Prosser, *Assault*, *supra* note 27, at 1111-12; OWEN, *supra* note 34, at 251.

[40] For a comprehensive discussion of this topic, *see generally* WHITE, *supra* note 33; James R. Hackney, Jr., *The Intellectual Origins of American Strict Product Liability Law: A Case Study in American Pragmatic Instrumentalism*, 39 AM. J. LEGAL HIST. 443 (1995); George Priest, *The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law*, 14 J. LEGAL STUD. 461 (1985).

[41] *See* Joseph Singer, *Legal Realism Now*, 76 CALIF. L. REV. 465, 474 (1988).

[42] Priest, *supra* note 40, at 471.

[43] Hackney, *supra* note 41, at 494–95; *see also* WHITE, *supra* note 33, at 108–10.

[44] Fleming James, *General Products—Should Manufacturers be Liable Without Negligence?*, 24 TENN. L. REV. 923, 925 (1957).

[45] Priest, *supra* note 40, at 501; WHITE, *supra* note 33, at 158.

By 1960, it was clear that change was on the horizon; as William Prosser famously put it, "the storming of the inner citadel is already in full cry," and that "it needs no prophet to foresee" that the end of fault-based recovery was near.[46] It didn't take Prosser long to be proven right—within a year the New Jersey Supreme Court became the first in the nation to eliminate the privity requirement for warranty claims,[47] and not long after, California became the first to abandon the fault requirement for tort action against the manufacturers[48] and retailers[49] of defective products. This new doctrine of strict liability then "spread like wildfire across the nation,"[50] marking the judicial convergence of "once independent streams of contracts and torts scholarship."[51] It also represented a repudiation of prior theories of recovery—as Edward White has noted, the "triumph of strict liability" would not have occurred absent "a tacit consensus among academicians and courts that negligence theory was not performing satisfactorily in defective product cases."[52]

Strict liability's peak came in 1965 when the American Law Institute codified the rule in Section 402A of its *Restatement (Second) of Torts* (for which Prosser served as the Reporter). As articulated by the *Restatement*, the seller of "any product in a defective condition" is liable to the consumer for any "physical harm thereby caused," regardless of the degree of care exercised by the seller.[53] In the commentary accompanying this provision, Prosser clarified that the rule "applies to any person engaged in the business of selling products for use or consumption," including manufacturers, distributors, wholesalers, and retail dealers.[54] Despite "restating" almost no actual law, the project was an overwhelming success. Within a decade, the rule had been adopted in some form by the courts of almost every US jurisdiction, "a progression so rapid that it amazed even some of the judges who joined in the movement."[55] The citadel had fallen, and strict liability had arrived.

---

[46] Prosser, *Assault*, *supra* note 27, at 1113–14.
[47] *See* Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960).
[48] *See* Greenman v. Yuba Power Products, Inc., 377 P.2d 897, 900-01 (Cal. 1963) (recognizing strict liability on manufacturers of a broad range of goods).
[49] *See* Vandermark v. Ford Motor Co., 391 P.2d 168, 171 (Cal. 1964).
[50] OWEN, *supra* note 34, at 23.
[51] Priest, *supra* note 40, at 505.
[52] WHITE, *supra* note 33, at 171.
[53] RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965).
[54] *Id.* at § 402A, cmt. f.
[55] Graham, *supra* note 26, at 578–79.

B. Justifying Strict Liability

It may be, as Justice Holmes once wrote, that the common law develops by "decid[ing] the case first and determin[ing] the principle afterwards,"[56] but Prosser and his contemporaries had several key principles in mind as they ushered the modern product liability doctrine into existence.

First, borrowing from contract law's implied warranty, they argued that simply by placing goods into the stream of commerce, "the supplier . . . represents to the public that [the goods] are suitable and safe for use."[57] As with implied warranties, strict liability is the necessary corollary to a breach of this representation. After all, consumers only complete transactions when they have received some level of assurance their purchases will function as intended without injuring them or their property.[58] It should therefore come as no surprise when consumers actually do rely on those assurances, irrespective of the existence of contractual privity. "The supplier has invited and solicited the use; and when it leads to disaster, he should not be permitted to avoid the responsibility by saying that he has made no contract with the consumer."[59]

A second rationale was drawn directly from ideas about loss spreading and risk allocation pioneered by the Legal Realists in the decades prior. Injured people, the argument went, should be compensated not because of the blameworthiness of a tortfeasor, but rather "because their injuries affect[ ] society at large."[60] In this view, tort law is best understood as a type of public law: "a compensation system designed to distribute the costs of injuries throughout society efficiently and fairly."[61] Strict liability fits neatly within this paradigm by completely detaching compensation from negligence, ensuring that "victims who previously had to prove fault in this important area are now able to recover without such a showing."[62] Because manufacturers, distributors, and sellers are—as individuals and as an industry—best positioned to spread these costs,

---

[56] Oliver Wendell Holmes, *Codes, and the Arrangement of the Law*, 5 AM. L. REV. 1, 1 (1870), *reprinted in* 44 HARV. L. REV. 725, 725 (1931).
[57] Prosser, *Assault*, *supra* note 27, at 1123.
[58] *See* Speidel, *supra* note 29, at 811 ("These general representations mold consumer choice, create expectations of quality, and influence sales at retail.").
[59] Prosser, *Assault*, *supra* note 28, at 1123.
[60] WHITE, *supra* note 33, at 149.
[61] *Id*. at 150 (citing Leon Green, *Tort Law Public Law in Disguise*, 38 TEX. L. REV. 1 (1959)).
[62] Marc A. Franklin, *Replacing the Negligence Lottery: Compensation and Selective Reimbursement*, 53 VA. L. REV. 774, 785 (1967); *see also* WHITE, *supra* note 33, at

they "should absorb the inevitable losses which must result in a complex civilization from the use of their products."[63]

Finally, strict product liability was grounded in appeals to public safety. "As handicrafts have been replaced by mass production," Justice Traynor wrote in his famous *Escola* concurrence, "[t]he consumer no longer has means or skill enough to investigate for himself the soundness of a product."[64] For this reason, the public interest in protecting human life, safety, and health supports holding the product suppliers responsible for the harms they cause, regardless of any negligence on their part.[65] As with the law's treatment of tainted food products a generation prior, this liability should not be "based on negligence, nor on a breach of the usual implied contractual warranty, but on the broad principle of the public policy to protect human health and life."[66] The seller "has undertaken and assumed a special responsibility toward any member of the consuming public," and so must be responsible for the costs of even accidental injuries.[67]

While these policy justifications helped propel strict liability into existence, they were quickly challenged by the rising Law and Economics movement of the 1970s. In his seminal work *The Cost of Accidents*, Guido Calabresi argued that "the principal function of accident law is to reduce the sum of the costs of accidents and the costs of avoiding accidents."[68] In this view, loss spreading and victim compensation—ideas at the heart of product liability's recent expansion—were at most secondary goals of accident law better tackled using tools like social insurance programs.[69] Instead, liability rules should seek to discourage "accident

---

150. ("Today one can muster substantial evidence of society's desire to shift the focus from the defendant and his conduct to the victim and his plight.").

[63] Prosser, *Assault*, *supra* note 27, at 1120.

[64] Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 467 (Cal. 1944) (Traynor, J., concurring).

[65] Prosser, *Assault*, *supra* note 27, at 1122.

[66] *Decker*, 164 S.W.2d at 829; *see also* Note, *Strict Products Liability and the Bystander*, 64 COLUM. L. REV. 916, 930 (1964) (noting how this language "implies a connection between the marketer's moral obligation and the consumability of his product").

[67] RESTATEMENT (SECOND), *supra* note 53, § 402A, cmt. c.

[68] GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 26 (1970).

[69] *Id.* at 32, 46–47; *see also* Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499, 530 (1961) ("[I]f risk spreading is deemed crucial, enterprise liability could do only part of the job; the other part would have to be filled in by some social insurance scheme.").

prone" activities and encourage safer alternatives by allocating the costs of those accidents, "forc[ing] individuals to consider accident costs in choosing among activities."[70] And consistent with Law and Economics' general market-based approach, these costs should be directed towards the lowest-cost accident avoider, ensuring the greatest benefits to the society with the fewest transaction costs for the parties.[71]

Still, even within this deterrence-centric vision of tort law, Calabresi nevertheless recognized a role for no-fault recovery.[72] His reasoning centered on the question of efficiency. Rather than requiring judges and juries to make case-by-case determinations as to which party was the negligent lowest-cost avoider, strict liability permits ex ante determinations as to the nature of the injuring enterprise.[73] This means that the issue is "not whether avoidance is worth it, but which of the parties is relatively more likely to find out whether avoidance is worth it."[74] A far cry from "public law in disguise," this approach would have tort law filling a regulatory function by making decisions about loss allocation before the first case is even litigated.[75] Still, even under this approach, the answer is the same for most defective products: the corporations within the products' supply chains are almost invariably better positioned to make this cost-benefit determination than the consumers, irrespective of their degree of fault for any eventual injuries.[76]

A final justification for strict product liability can be found in the civil recourse theory most prominently advanced by John Goldberg and Benjamin Zipursky. In their view, tort law's primary normative function is neither to advance public policy nor to act as a cost-allocation mechanism, but rather to provide victims of legally-recognized wrongs with the means to obtain redress from their wrongdoers.[77] Product liability law is no different: the doctrine "allows victims who have been wrongfully injured by the seller of a defective product to invoke the legal system to

---

[70] CALABRESI, *supra* note 68, at 68–69.
[71] *Id.* at 135–36.
[72] Guido Calabresi & Jon T. Hirschoff, *Towards a Test for Strict Liability in Torts*, 81 YALE L.J. 1055, 1060 (1972).
[73] *Id.* at 1060.
[74] *Id.* at 1060–61.
[75] WHITE, *supra* note 33, at 221.
[76] Calabresi & Hirschoff, *supra* note 72, at 1064. *But see* Richard Posner, *Strict Liability: A Comment*, 2 J. LEGAL STUD. 205, 213-15 (1973) (describing Calabresi's view of strict liability as "inefficient" for failing to encourage safe behaviors by individual plaintiffs).
[77] JOHN C.P. GOLDBERG & BENJAMIN C. ZIPURSKY, RECOGNIZING WRONGS 6 (2020).

hold the seller accountable."[78] As well as promoting greater civil accountability, Goldberg and Zipursky argue that strict liability acts to empower victims by allowing them to demand a judicial recognition that they have, in fact, been victimized.[79] Its elimination, therefore, would disempower a broad swath of the citizenry, denying them a forum in which to demand that law take their individual interests seriously.[80]

C. Retrenchment and Reform

Even as its strict liability formulation achieved widespread adoption, the *Restatement (Second)*'s application of this doctrine to nonmanufacturing retailers became a flashpoint for controversy. The sellers of defective products, critics argued, are often not the lowest-cost avoider in the retail chain, nor are they the party best situated to ensure that defective products do not reach the consumer.[81] This is especially the case for complex or high-tech products shipped from manufacturers in sealed containers; in these cases, a retailer may be just as ill equipped as the consumer in identifying and mitigating harmful defects.[82] Neither are the sellers of defective products necessarily the best cost-bearing party. Not every retailer has the resources of Walmart, and a large damages award could bankrupt many mom-and-pop stores.[83] And while it is certainly possible (as some courts have argued) for nonmanufacturers to add indemnification agreements to their sales contracts, legal fees and other transaction costs make this an especially inefficient way to spread losses.[84]

---

[78] John C.P. Goldberg & Benjamin C. Zipursky, *The Easy Case for Products Liability Law: A Response to Professors Polinsky and Shavell*, 123 HARV. L. REV. 1919, 1944 (2010).
[79] *Id.* at 1946.
[80] *Id.* at 1946–47.
[81] *See* Frank J. Cavico, Jr., *The Strict Tort Liability of Retailers, Wholesalers, and Distributors of Defective Products*, 12 NOVA L. REV. 213, 227 (1987).
[82] *See id.* ("In the typical transaction, the retailer and wholesaler receive the goods in a sealed package and do nothing to contribute to the danger the goods may present to the consumer."); *see also* John G. Culhane, *Real and Imagined Effects of Statutes Restricting the Liability of Nonmanufacturing Sellers of Defective Products*, 95 DICK. L. REV. 287, 300–01 (1991) (noting that when retailers sell goods shipped in sealed containers, "the supplier is no more at fault than the consumer").
[83] *But see* Prosser, *Fall*, *supra* note 14, at 816 (noting that even in the mid-60s, the retailer of a defective product was far more likely to be "Safeway Stores, or some other nation-wide enterprise" than "the little corner grocery").
[84] *See* A. Mitchell Polinsky & Steven Shavell, *The Uneasy Case for Product Liability*, 123 HARV. L. REV. 1436, 1470 (2010) (discussing these costs and noting that, "[F]or

Beginning in the Ford Administration, the federal government took an intense interest in strict product liability and chartered an interagency task force to study its effects.[85] In addition to recommending legislation that would preempt several state insurance regulations,[86] the task force also proposed a model Uniform Product Liability Act (UPLA) to harmonize product liability law among the states.[87] Unlike the *Restatement (Second)*, the UPLA largely rejected nonmanufacturer strict liability, stating that "product sellers shall not be subject to liability in circumstances in which they did not have a reasonable opportunity to inspect the product . . . [for] the existence of the defective condition."[88] The only exceptions to this exclusion were for circumstances in which the manufacturer is effectively judgement-proof, either because it is not subject to service of process or is insolvent.[89]

With the UPLA serving "as model and incentive," many state legislatures have since acted to narrow strict liability's scope.[90] While these legislative enactments are varied and touch on a range of issues, they can generally be placed into four categories as they relate to nonmanufacturer liability.

First, a few states enacted absolute bars on holding nonmanufacturers strictly liable for product defects.[91] These laws contain no exceptions and have the practical effect of reversing decisions like *Vandermark v. Ford Motor Company*[92] and shifting all liability for defective products onto the manufacturers.[93] Thus, when consumers in these states are una-

---

each dollar that an accident victim receives in a settlement or judgment, it is reasonable to assume that a dollar of legal and administrative expenses is incurred.").

[85] Victor Schwartz & Mark Behrens, *The Road to Federal Product Liability Reform*, 55 MD. L. REV. 1363, 1365 (1996).

[86] Many of these recommendations were ultimately enacted into law, including most significantly the Product Liability Risk Retention Act of 1981, Pub. L. No. 97–45, 95 Stat. 949 (codified as amended at 15 U.S.C. §§ 3901–3904).

[87] Schwartz & Behrens, *supra* note 85, at 1366.

[88] Model Uniform Product Liability Act, 44 Fed. Reg. 62,714, 62,726 (Oct. 31, 1979).

[89] *Id.*

[90] Cavico, *supra* note 81, at 237.

[91] GA. CODE ANN. § 51-1-11.1 (1987); NEB. REV. STAT. § 25-221, 181 (1997); S.D. CODIFIED LAWS § 20-9-9 (1979); MISS. CODE ANN. § 11-1-63(h) (2014). Additionally, Louisiana's statute limits product liability to manufacturers unless "the seller is the alter ego of the alien manufacturer." LA. REV. STAT. ANN. § 9:2800.53 (1988).

[92] Vandermark v. Ford Motor Company, 391 P.2d 168, 171 (Cal. 1964).

[93] Adam Feeney, *In Search of a Remedy: Do State Laws Exempting Sellers from Strict Product Liability Adequately Protect Consumers Harmed by Defective Chinese-Manufactured Products?*, 34 J. CORP. L. 567, 573 (2009).

ble to recover from a judgement-proof manufacturer, they are left with no tort law remedy for their injuries.

Second, at the opposite end of the spectrum, another group of states enacted statutes that largely retain the general presumption of nonmanufacturer strict liability with an exception carved out for cases in which the products are distributed by the manufacturers in sealed containers.[94] Some of these statutes also require manufacturers to indemnify their retailers and distributors[95] (though this indemnification likely already existed at common law).[96] One state—North Carolina—has codified the sealed-container defense and also abolished strict liability as a theory of recovery against any defendant, whether manufacturer or seller.[97]

Third, another group of states adopted a presumption against permitting strict liability claims against nonmanufacturing sellers, though these suits are not barred outright. In these jurisdictions, plaintiffs are still permitted to hold sellers strictly liable in cases in which the manufacturer is either not subject to the jurisdiction of the state's courts or is insolvent (or both).[98] A slight variation of this idea is found in Colorado and Indiana's statutes, which only permit strict liability claims against the product's "manufacturer," but define the term to include the principle in-state distributor of the defective product in cases where the state lacks jurisdiction over the actual manufacturer.[99]

Finally, a few states enacted what is effectively a burden-shifting framework for allocating product liability.[100] In general, these statutes permit plaintiffs to sue retailers and distributors, who can then obtain

---

[94] KY. REV. STAT. ANN. § 411.340 (LexisNexis 1978); DEL. CODE ANN. tit. 18, § 7001(b) (1995); MD. CODE ANN., CTS. & JUD. PROC. §5-405(b) (LexisNexis 1997).
[95] ARIZ. REV. STAT. ANN. § 12-684A (1978); ARK. CODE ANN. § 16-116-207 (1979); OKLA. STAT. tit. 12, § 12-832.1(A) (2004); TEX. CIV. PRAC. CODE ANN. § 82.002(a) (1993).
[96] *See* Cavico, *supra* note 81, at 237 (describing these statutes as "merely codify[ing] basic common law indemnification principles").
[97] N.C. GEN. STAT. § 99B-1.1 (2020) ("There shall be no strict liability in tort in product liability actions.").
[98] IDAHO CODE ANN. § 6-1407 (2005); IOWA CODE § 613.18 (1986); KAN. STAT. ANN. § 60-3306 (2012); OHIO REV. CODE ANN. § 2307.78 (LexisNexis 2001); WASH. REV. CODE § 7.72.040 (1991); TENN. CODE ANN. § 29-28-106 (2011); WIS. STAT. § 895.047(2) (2019).
[99] COLO. REV. STAT. ANN. § 13-21-402(2) (2003); IND. CODE §34-20-2-4 (1998).
[100] 735 ILL. COMP. STAT. 5/2-621 (1995); MINN. STAT. § 544.41 (West 1980); MO. REV. STAT. § 537.762 (West 2019); N.J. STAT. ANN. § 2A:58C-9 (West 1995); N.D. CENT. CODE § 28-01.3-04 (West 1993).

dismissal of any strict liability claims by identifying the responsible manufacturer of the defective good. Once the manufacturer is identified, the burden shifts back to the plaintiff, who can stop this dismissal (or in some cases reinstate the nonmanufacturing seller) by demonstrating that the manufacturer's extraterritoriality or financial status makes recovery impossible.[101]

These and other "reform" statutes have transformed product liability law, signaling a retreat from the *Restatement (Second)*'s emphasis on risk-spreading and no-fault recovery. While a majority of jurisdictions continue to apply strict liability to the sellers of defective goods,[102] it is no longer the universal rule. These statutes mark a shift from the preceding purely common law rulemaking, often to the detriment of injured consumers.[103] Still, regardless of their merits, these statutes have shaped the field of product liability law, playing significant roles in cases like those filed against Amazon.

II. Amazon And Not-So Strict Liability

This Part turns from product liability generally to consider the doctrine's application to Amazon. After describing the company's history and structure, the article reviews six years of product liability litigation arising from third-party sales, noting the various arguments advanced by Amazon and the difficulties that consumers have faced in holding it liable. It then concludes with a case study of the typical progression of these lawsuits.

A. Building the "Unstore"

"[V]irtually all of us have some experience with Amazon,"[104] but that experience is now quite different than it was in the website's earliest days. Amazon launched in 1995 as one of the first attempts to capitalize

---

[101] § 13-21-402(2); §34-20-2-4; 5/2-621; § 544.41; § 537.762; § 2A:58C-9; § 28-01.3-04.

[102] RESTATEMENT (THIRD), *supra* note 16, at § 1, cmt. e.

[103] *See* GUIDO CALABRESI, A COMMON LAW FOR THE AGE OF STATUTES 243 (1982) (warning that these statutes "may be the start of a new and dominant (for me, undesirable) trend characterized by very low liability in tort conjoined with greater governmental compensation and regulation").

[104] Erie Ins. Co. v. Amazon.com, Inc., No. 8:16-CV-02679, 2018 WL 3046243, at *1 (D. Md. Jan. 22, 2018).

on the explosive growth of the World Wide Web.[105] Initially billing itself as "Earth's Biggest Bookstore," Amazon offered visitors a literary catalogue of more than one million titles coupled with advanced search capabilities and "consistently low prices."[106] Then, one-by-one, new product categories were added to the website: first CDs and DVDs in 1998, then tools, electronics, and children's toys the following spring.[107] But the company's ambitions were larger still—as Amazon's founder Jeff Bezos would tell senior executives, he viewed Amazon as not just a store but as an "unstore." And being the world's first "unstore" meant, in Bezos' view, "that Amazon was not bound by the traditional rules of retail."[108]

As its user base began to grow exponentially, Amazon was quickly forced to reassess its retail strategy. In its early days as a bookseller, the company maintained relatively little of its own inventory. Instead, when a customer ordered a book through its website, Amazon would purchase the book from one of the two national book distributors and then ship it to the customer.[109] While this was an effective way to save money as the website got off the ground,[110] an inventory-free model proved almost impossible to scale up, and Amazon soon began keeping a supply of its most-ordered books on hand so that they were available for immediate shipment.[111] What started as just the "top ten bestselling books" quickly grew to a standing inventory of thousands, and by 1996 Amazon had leased a 93,000 square foot warehouse that became the company's first fulfillment center.[112]

Meanwhile, Amazon's leadership was warily watching the rise of the rival e-commerce platform—eBay. Like Amazon, the online auction house had also launched in 1995, but unlike Amazon, it was turning a

---

[105] ROBERT SPECTOR, AMAZON.COM: GET BIG FAST: INSIDE THE REVOLUTIONARY BUSINESS MODEL THAT CHANGED THE WORLD 30 (2002).
[106] *Id.* at 70–71.
[107] STONE, *supra* note 6, at 84–87.
[108] *Id.*
[109] SPECTOR, *supra* note 105, at 68.
[110] In addition to saving on overhead, Amazon's initial strategy was also motivated by the fact that before 2018 online sellers were only required to collect sales taxes on items sold to customers in states where the seller maintained a physical presence (e.g., a fulfillment center), giving Amazon an important advantage over its retail competition. *See* South Dakota v. Wayfair, Inc., 138 S. Ct. 2080, 2087-88 (2018) (discussing this dynamic). This is also why Bezos chose to headquarter Amazon in Washington state and not with most other 90s tech companies in the far more populous California. STONE, *supra* note 6, at 31.
[111] SPECTOR, *supra* note 105, at 137.
[112] *Id.* at 138.

steady profit with a business model that produced brisk sales with almost no overhead.[113] It was after the acquisition efforts broke down that Amazon first tried to create its own platform for third-party sellers. In 1999, the company launched Auctions, an eBay clone which debuted that March, and then zShops, a fixed-price marketplace that opened its doors that September.[114] Neither platform was initially successful, receiving little traffic and failing to lure small merchants away from eBay. Still, Bezos was undeterred, telling executives that his vision was for Amazon's revenue to one day be split equally between its own products and commissions collected from third-party sellers using its site.[115]

The turning point for Bezos' vision came in the fall of 2000 when Amazon's leadership realized that almost all traffic to its third-party vendors originated from links embedded within the site's established product catalogue.[116] This, in turn, led to the realization that the best way to direct traffic to third-party sellers would be to immediately list their wares alongside Amazon's own inventory, thereby offering customers the choice of sellers.[117] Relaunched that winter as Amazon Marketplace, this new platform generated controversy almost immediately, with book publishers complaining that it was driving buyers away from new books and towards used books. Even Amazon's own management worried that the company's sales would be cannibalized by now-embedded rivals.[118] Still, Bezos held his ground, and Amazon Marketplace continued to expand every year since.[119]

While Amazon may have lost money in the short-term by listing its competitors' products directly alongside its own, it nevertheless gained three key benefits by operating its website as a fully integrated retail ecosystem. First, the addition of third-party sellers allowed Amazon to dramatically expand the scope of its offerings with little added

---

[113] *See* STONE, *supra* note 6, at 77 ("[eBay] had the perfect business model: it took a commission on each sale but had none of the costs of storing inventory and mailing packages.").
[114] Feng Zhu & Qihong Liu, *Competing with Complementors: An Empirical Look at Amazon.com*, 39 STRATEGIC MGMT. J. 2618, 2623–24 (2018).
[115] STONE, *supra* note 6, at 107.
[116] *Id.* at 115.
[117] *Id.*
[118] *Id.* at 116.
[119] *See* 2018 Shareholder Letter, *supra* note 5.

expense.[120] Bezos had long envisioned his company as a literal "everything store," and integrating the wares of thousands of independent merchants into the site's catalogue was key to achieving this goal. Second, increasing traffic to third-party sellers allowed Amazon to gather valuable data on sales trends and product popularity, informing the company's decisions about whether and how to enter a particular product market.[121] Finally, and most importantly, any short-term losses from this internal competition have been more than offset by the benefits from the increased customer base of Amazon's third-party sellers, as the fees generated by these transactions now constitute one of the company's largest and most important revenue streams.[122]

Even as it maintains its ostensible independence from third-party sellers,[123] Amazon's involvement in these transactions is extensive. Sellers pay Amazon various fees, including a subscription fee (either $39.99 per-month or $0.99 per-item) and a per-transaction fee.[124] Sellers then set their own prices and write their own product descriptions. But when multiple sellers offer the same product, Amazon displays the products on a single product detail page to "present customers with the best experience."[125] For these combined listings, Amazon uses its proprietary ranking algorithms to determine which seller's product appears in the page's "Buy Box," a designation that leads to 82% of the site's sales.[126] Amazon also serves as an intermediary for all communications between its cus-

---

[120] *See* SPECTOR, *supra* note 105, at 218 (describing third-party sellers as "a throwback to the original Amazon.com business model of selling merchandise on the Web without the hassle and expense of carrying inventory").

[121] *See* Zhu & Liu, *supra* note 114, at 2624–25. While beyond the scope of this Article, it should be noted that this data-collection process has raised significant antitrust concerns, as has Amazon's practice of using this data to develop and market its own private label brands. *See generally* Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017).

[122] *See Sellers on Amazon*, *supra* note 8; s*ee also* AMAZON'S ANNUAL REPORT, *supra* note 9.

[123] *See Amazon Services Business Solutions Agreement* ¶ 13, AMAZON.COM, https://sellercentral.amazon.com/gp/help/external/G1791?language=en_US (last visited Jan. 13, 2021) ("[Y]ou and we are independent contractors, and nothing in this Agreement will create any partnership, joint venture, agency, franchise, sales representative, or employment relationship between us.").

[124] *Let's Talk Numbers*, AMAZON.COM, https://services.amazon.com/selling/pricing.html (last visited Jan. 13, 2021); Khan, *Separation*, *supra* note 6, at 987 n.42.

[125] The Beginner's Guide to Selling on Amazon, AMAZON.COM, https://sell.amazon.com/beginners-guide.html (last visited Jan. 13, 2021).

[126] Khan, *Separation*, *supra* note 6, at 988.

tomers and sellers. It processes payments, communications, dispute adjudications, and refund requests.[127] For over 80% of sellers,[128] Amazon also acts as the logistics provider. Through its Fulfillment by Amazon program, the company stores third-party goods in its warehouses and handles all aspects of packaging, delivery, customer service, and returns.[129]

B. Prime and Punishment

It should come as no surprise that the world's largest retailer gets sued a lot. Bloomberg Law's Litigation Analytics tool lists 1665 lawsuits filed against Amazon between January 1, 2015, and December 31, 2020, while a Westlaw search shows more than 3000 cases within the same period. Filtering these searches by Case Type (Bloomberg) and Practice Area (Westlaw) produced lists of 88 and 101 product liability cases, respectively. These results were combined and then reviewed for relevance to create a dataset of 79 product liability lawsuits filed against Amazon involving third-party sales. Of these 79 suits, which are listed by filing date in Appendix, 22 remain pending, 35 were settled or otherwise voluntarily dismissed, and 22 were adjudicated through a case dispositive motion like a motion to dismiss or summary judgement.[130] There are two reasons to think that this dataset may be underinclusive. First, commercial databases like Bloomberg and Westlaw are notoriously incomplete when it comes to state court records, especially at the trial court level. Second, the dataset excludes cases where the pleadings and other docket entries are unclear as to whether the defective product was sold by Amazon or a third-party merchant.[131]

---

[127] *About Ordering from a Third-Party Seller*, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201889310 (last visited Jan. 13, 2021); About the Buyer-Seller Messaging Service, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html?nodeId=201889440 (last visited Jan. 13, 2021).

[128] *FBA Usage Among Amazon Marketplace Sellers*, MARKETPLACE PULSE, https://www.marketplacepulse.com/amazon/fulfillment-by-amazon-fba (last visited Jan. 13, 2021).

[129] Save Time and Help Grow Your Business with FBA, AMAZON.COM, https://sell.amazon.com/fulfillment-by-amazon.html?ref_=sdus_fulfill_fba_h (last visited Jan.13, 2021).

[130] *See* Appendix (for lawsuits whose appeals have been adjudicated, the dataset reflects only the decision of the appellate court, not the trial court).

[131] For example, the dataset excludes cases like *Nenninger v. Amazon.com, LLC*, in which the complaint describes Amazon as the "seller" of the product in question. Complaint ¶ 6, Nenninger v. Amazon.com, No. 2:17-cv-00171 (E.D.N.Y dismissed Feb. 2,

Nevertheless, focusing on these 79 cases reveals several important trends. Most importantly, their outcomes challenge some scholars' optimistic predictions about the law's capability to extend liability to online platforms.[132] Amazon has been spared in this aspect. Of the 22 lawsuits that have reached some form of adjudicative outcome, only six[133] have resulted in opinions even suggesting that Amazon might be strictly liable in tort, several of which are still being appealed as of this writing.[134] Even at a time when civil plaintiff success rates are approaching all-time lows,[135] winning just 7% of filed cases (and 27% of adjudicated cases) stands out as an especially dismal track record.

Additionally, these cases make clear that Amazon has a strong preference for litigating in federal courts. On the one hand, this is not so surprising, as it is a preference shared by many other well-resourced litigants.[136] Yet the numbers are still striking, especially considering state courts' central role in developing product liability doctrines. Out of the 79 cases identified in this review, 67 ultimately ended up in a federal court—over half because of removals initiated by Amazon. (Additionally, three others were removed to federal court before ultimately being remanded back to the original forum). The cases that remained in state

---

2018), the answer denied this assertion, Answer at 8, and the case settled with no adjudication of this factual dispute.

[132] *See* Rory Van Loo, *The Revival of Respondeat Superior and Evolution of Gatekeeper Liability,* 109 GEO. L.J. 141, 161 (2020) (suggesting that "the doctrine of *respondeat superior* may be evolving" to recognize the degree of control exercised by online platforms over activities taking place on their websites).

[133] The decisions are Oberdorf v. Amazon, 930 F.3d 136 (3d Cir. 2019); Papataros v. Amazon, 2019 WL 4011502 (D.N.J. Aug. 26, 2019); State Farm v. Amazon, 390 F. Supp. 3d 964 (W.D. Wis. 2019); McMillan v. Amazon.com, Inc., 433 F. Supp. 3d 1034 (S.D. Tex. 2020); Bolger v. Amazon.com, LLC, 267 Cal. Rptr. 3d 601 (Cal. App. Aug. 13, 2020); and State Farm Fire & Cas. Co. v. Amazon.com Servs., Inc., No. 008550/2019, 2020 WL 7234265 (N.Y. Sup. Ct. Dec. 8, 2020).

Two additional cases involving third-party defective products have advanced past the pleading stage, but neither asserts a strict liability claim against Amazon. In the first, *State Farm v. Amazon.com*, the plaintiff alleges that Amazon was negligent in the operation of its online marketplace. 414 F. Supp. 3d 870, 875 (N.D. Miss. 2019). In the second, *Love v. WEECOO(TM)*, the plaintiff is suing for negligent failure-to-warn, alleging that Amazon failed to pass on information it learned prior to the sale about the product's dangerousness. 774 F. App'x 519 (11th Cir. 2019).

[134] *Id.*

[135] See Alexandra D. Lahav & Peter Siegelman, *The Curious Incident of the Falling Win Rate: Individual vs System-Level Justification and the Rule of Law*, 52 U.C. DAVIS L. REV. 1371 (2019).

[136] *See infra* notes 141–143 and accompanying text.

courts appear to lack diversity jurisdiction, making removal impossible. In *Stiner v. Amazon.com*, for example, the plaintiffs were able to join another Ohio resident as a co-defendant alongside Amazon and the third-party merchant, thus destroying complete diversity.[137] Others were filed in Amazon's home state, and thus could not be removed regardless of the parties' citizenship.[138] But since most plaintiffs cannot properly join a home-state defendant or travel to Washington or Delaware to litigate their claims,[139] Amazon is able to steer much of this litigation into federal courts.

This is not to say that Amazon is necessarily acting with some nefarious purpose when it removes these product liability suits. Defendants have a range of reasons to prefer federal fora over litigation in state court. Federal judges are often seen as more competent;[140] they have more resources at their disposal and as a result generally draft more thorough opinions;[141] and their lifetime appointments tend to immunize them from public pressure on hot-button issues, especially compared to state judges who might face periodic reelection.[142] For their part, Amazon's attorneys have argued that federal courts are appropriate venues because of Amazon's assertion of immunity under federal telecommunications statutes—making these cases fully adjudicable on a federal level without having to reach any questions of state law.[143] Still, whatever Amazon's motivations, its strategy has left state judges on the sidelines of these legal fights. And

---

[137] Stiner v. Amizon.com, Inc., 120 N.E.3d 885, 887 (Ohio Ct. App. 2019).
[138] USAA General Indemnity Co. v. Amazon.com, Inc., No. 18-2-08310-4 (Wash. Super. Ct. filed May 24, 2018).
[139] *Cf.* 28 U.S.C. § 1441(b)(2) (2012) ("A civil action otherwise removable solely on the basis of the jurisdiction under section 1332(a) of this title may not be removed if any of the parties in interest properly joined and served as defendants is a citizen of the State in which such action is brought.").
[140] *See* Burt Neuborne, *The Myth of Parity*, 90 HARV. L. REV. 1105, 1121 (1977) ("Because it is relatively small, the federal trial bench maintains a level of competence in its pool of potential appointees which dwarfs the competence of the vastly larger pool from which state trial judges are selected.").
[141] *See* Benjamin C. Glassman, *Making State Law in Federal Court*, 41 GONZ. L. REV. 237, 277 (2005) (suggesting that federal courts are "institutionally advantaged" as compared to state courts); Neuborne, *supra* note 140, at 1122 ("[T]he caliber of judicial clerks exerts a substantial impact on the quality of judicial output.").
[142] *See* Neuborne, supra note 140, at 1127 ("Federal district judges, appointed for life and removable only by impeachment, are as insulated from majoritarian pressures as is functionally possible.").
[143] *See* Oral Argument at 16:20, Erie Insurance Co. v. Amazon.com, Inc., 925 F.3d 135 (4th Cir. 2019), https://www.ca4.uscourts.gov/OAarchive/mp3/18-1198-20190321.mp3.

this, as one judge put it, has "arguably stunted the development of state law," since federal courts sitting in diversity must proceed with caution in resolving questions of first impression.[144]

Once in federal court, Amazon deploys a two-fold defense strategy to avoid liability for the sale of the defective product. First, it asserts that it has immunity under Section 230 of the Communications Decency Act of 1996. By way of background, Section 230 was enacted in the mid-90s "to promote the continued development of the Internet and other interactive computer services and other interactive media . . . unfettered by Federal or State regulation."[145] To that end, Congress directed that no provider of an "interactive computer service" can be treated as the publisher of any content originating from a third-party user of their platform.[146] Thus, argues Amazon, courts need not reach the merits of the strict liability question all. Its role in third-party sales is merely allowing merchants to post their product offerings to its Marketplace, bringing it within the broad umbrella of Section 230's protections.[147]

While such a sweeping interpretation of Section 230 has its supporters,[148] it has found little traction in the courts so far. To date, no judge has taken Amazon up on its suggestion that these cases should be resolved on Section 230 grounds, and only two have even suggested (albeit in dicta) that Amazon's interpretation of Section 230 is correct.[149] The

---

[144] *Erie*, 925 F.3d at 145 (Motz, J., concurring); *see also infra* Part III.C.

[145] 47 U.S.C. § 230(b).

[146] *Id.* at § 230(c)(1); *see also* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1604–09 (2018) (discussing § 230's legislative and interpretive history).

[147] *E.g.*, Brief for Appellee at 39-40, Fox v. Amazon.com, Inc., 930 F.3d 415 (6th Cir. 2019) (No. 18-5661), 2018 WL 5784393 ("Amazon's conduct that supposedly constituted 'selling' was allowing a third-party to post a product offer online. But the CDA bars any claim seeking to treat the provider of an interactive computing service (such as Amazon) as the speaker or publisher of content provided by a third party.").

[148] *See* Shehan, *supra* note 12, at 1234 ("Amazon's argument that dismissal is mandated under § 230 of the CDA should prevail.").

[149] Eberhart v. Amazon.com, Inc., 325 F. Supp. 3d 393, 400 n.5 (S.D.N.Y. 2018) ("To the extent that Eberhart seeks to assert a claim that Amazon is liable, either directly or vicariously, for the content it permitted CoffeeGet to post on amazon.com, such a claim is preempted by § 230 of the Communications Decency Act."); Loomis v. Forrinx Tech. (USA) Inc., 2019 WL 2031430, at *9 (Cal. Super. Ct. March 15, 2019) ("The court further finds that defendant has established entitlement to claim immunity under the Communications Decency Act as to the product liability causes of action and counts.").

rest have either rejected this argument outright,[150] declined to weigh in on the question after resolving the case on different grounds,[151] or adopted a narrower reading of Section 230 which only immunizes Amazon from liability for suits based on a failure to warn theory but not when there is an alleged design or manufacturing defect.[152]

What these cases really turn on, then, is the second prong of Amazon's defense: that nonmanufacturer strict liability only extends to the "sellers" and "distributors" of defective products. This, in Amazon's telling, does not describe its role in these transactions. In Amazon's view, when goods are sold through its Marketplace, it acts merely as the facilitator to a private transaction between a consumer and a third-party merchant.[153] It does not create the product listing. It does not transfer title.[154] It does not even set the prices at which the goods are sold.[155] Its website merely acts as a platform to connect its third-party merchants to a base of customers, and after the sales are complete it provides those merchants with logistical support.[156] All this, Amazon has argued, means

---

[150] *See, e.g.*, *Erie*, 925 F.3d at 140 (rejecting Amazon's claim that Section 230 protects it "from liability as the seller of a defective product.").

[151] *E.g.*, Garber v. Amazon.com, Inc., 380 F. Supp. 3d 766, 782 (N.D. Ill. 2019) ("Because Amazon is entitled to judgment as a matter of law on the Garbers' claims, the Court need not reach the immunity provision in the Communications Decency Act.").

[152] *See* Oberdorf v. Amazon.com, Inc., 930 F.3d, 136 153 (3rd Cir. 2019) ("[T]o the extent that Oberdorf's negligence and strict liability claims rely on Amazon's role as an actor in the sales process, they are not barred by the CDA. However, to the extent that Oberdorf is alleging that Amazon failed to provide or to edit adequate warnings . . . these failure to warn claims are barred by the CDA.").

[153] Brief for Appellee at 17, Fox v. Amazon.com, Inc., 930 F.3d 415 (6th Cir. 2019), (No. 18-5661), 2018 WL 5784393.

[154] *Id.*; *cf.* U.C.C. § 2-106(1) (AM. L. INST. & UNIF. L. COMM'N 2002) ("A 'sale' consists in the passing of title from the seller to the buyer for a price.").

[155] Brief for Appellee, *supra* note 155, at 17. Indeed, major brands have complained for years that Amazon does little to prevent third-party merchants from listing their goods below the manufacturer's minimum advertised price. *See* Alistair Barr, *Brands Cry Foul Over Unauthorized Sellers on Amazon*, REUTERS (Oct. 23, 2012, 1:10 PM), https://www.reuters.com/article/us-amazon-sellers/brands-cry-foul-over-unauthorized-sellers-on-amazon-idUSBRE89M1CT20121023 ("The problem on Amazon is that while the goods are authentic, sellers often get them from leaks in supply chains, and then sell the products online at below the minimum advertised price set by the label.").

[156] Brief for Appellee at 22, Erie Ins. Co. v. Amazon.com, Inc., 925 F.3d 135 (4th Cir. 2019) (No. 18-1198).

that its role differs from that of a "seller" to whom state product liability laws apply.[157]

Unlike Amazon's claims about Section 230, its seller defense has been largely successful. Fourteen courts applying the substantive tort law of ten states have now agreed that Amazon's role in facilitating third-party transactions is insufficient to give rise to strict product liability.[158] Notwithstanding differences in the underlying state laws, there are a few points of commonality in these decisions. First, many courts have given significant weight to the fact that "title flows directly from third-party vendors to consumers,"[159] a fact that is held up as evidence of Amazon's peripheral role in these transactions. "[R]egardless of what attributes are necessary to place an entity within the chain of distribution," one court wrote, "the failure to take title to a product places that entity on the outside."[160] Other courts, while giving the transfer of title somewhat less weight, have nevertheless pointed to it as a significant factor in their analyses.[161] Only two courts appear to have explicitly rejected Amazon's claim that title transfer is a necessary condition for a classification as a "seller."[162]

But even when they reject Amazon's arguments about the necessity of title transfer, courts have largely accepted Amazon's claim that its role in third-party transactions is simply to "provid[e an] online marketplace and storefront for sellers to offer and buyers to purchase products,"

---

[157] *See, e.g.*, Brief for Appellee at 10, Oberdorf v. Amazon.com, Inc., 930 F.3d 136 (3d Cir. 2019), (No. 18-1041), 2018 WL 2973856 ("Amazon is a marketplace provider, not a seller, and it therefore falls outside the scope of Pennsylvania product-liability law.").

[158] Additionally, the Federal Circuit has held that "Amazon is not a seller . . . for the purposes of copyright infringement under 17 U.S.C. § 106." Milo & Gabby LLC v. Amazon.com, 693 F. App'x 879, 890 (Fed. Cir. 2017).

[159] State Farm v. Amazon.com, Inc., 407 F. Supp. 3d 848, 852 (D. Ariz. 2019).

[160] Eberhart v. Amazon.com, Inc., 325 F. Supp. 3d 393, 398 (S.D.N.Y. 2018); *see also Oberdorf*, 930 F.3d at 156–57 (Scirica, J., concurring in part and dissenting in part) (" '[S]elling' entails something Amazon does not do for Marketplace products: transferring ownership, or a different kind of legal right to possession, from the seller to the customer.").

[161] *E.g.*, *State Farm*, 407 F. Supp. 3d at 853 ("Whether title is transferred to an entity in the chain of production has never been a necessary prerequisite to holding that entity strictly liable . . . but it remains an important factor courts consider.").

[162] Garber v. Amazon.com, Inc., 380 F. Supp. 3d 766, 776 (N.D. Ill. 2019) ("[T]he Illinois Supreme Court has never limited its inquiry of whether a party is a 'seller' for strict liability purposes solely to the transfer of title."); Fox v. Amazon.com, Inc., 930 F.3d 415, 423 (6th Cir. 2019) ("[W]e are not persuaded that the Tennessee legislature intended such a limited construction [of the term 'seller']."). *See also infra* Part III.B.1.

similar to an auction house or flea market.[163] Courts have articulated this holding in various ways. Some have focused on the fact that Amazon does not inspect third-party products which are shipped directly from the seller to the consumer when a transaction is not fulfilled by Amazon.[164] Others (particularly in cases that advance a failure-to-warn theory of liability) note that third-party sellers write their own product descriptions with no involvement from Amazon.[165] For one court, the question of liability turned on the fact that "Amazon's conduct was [not] a 'necessary factor' in bringing [the defective product] to the initial consumer market."[166] At the end of the day, regardless of how these courts have structured their decisions, their conclusions have been the same: Amazon is not the "seller" or "distributor" of these defective products and as a result cannot be held strictly liable.

So, what about the handful of courts that have suggested that Amazon might be strictly liable? First, in these cases, the plaintiffs had the benefit of state court precedent explicitly disclaiming the requirement that a "seller" transfer title to the product. In *McMillan*, for example, the plaintiffs were able to cite to a decision from the Texas Supreme Court holding that "a seller does not need to actually sell the product" to incur product liability.[167] Likewise, the district court in *State Farm* stated that Wisconsin's case law "lays to rest" the argument that "a formal transfer of ownership is required to hold an entity strictly liable for a defective product."[168] This case law—together with Texas and Wisconsin's broadly-worded product liability statutes[169]—permitted the district courts

---

[163] Loomis v. Forrinx Tech.(USA) Inc., No. BC632830, 2019 WL 2031430, at *3 (Cal. Super. Ct. Mar. 15, 2019).

[164] *E.g.*, Stiner v. Amazon.com, Inc., 120 N.E.3d 885, 891 (Ohio App. 2019) ("Amazon did not install, repair, or maintain any aspect of a product and, therefore, did not fit the definition of a supplier . . . ."); *State Farm*, 407 F. Supp. 3d at 852 ("Even after receiving products from third-party vendors, Amazon still exercises only minimal control over those products such that it has little meaningful ability to inspect them.").

[165] *E.g.*, *Fox*, 930 F.3d at 425 ("Defendant did not choose to offer the hoverboard for sale, did not set the price of the hoverboard, and did not make any representations about the safety or specifications of the hoverboard on its marketplace.").

[166] Carpenter v. Amazon.com, Inc., 2019 WL 1259158, at *5 (N.D. Cal. Mar. 19, 2019).

[167] McMillan v. Amazon.com, Inc., 433 F. Supp. 3d 1034, 1041 (S.D. Tex. 2020) (citing Firestone Steel Prod. Co. v. Barajas, 927 S.W.2d 608, 613 (Tex. 1996)).

[168] State Farm v. Amazon.com, Inc., 390 F. Supp. 3d 964, 972 (W.D. Wisc. 2019) (citing Kemp v. Miller, 453 N.W.2d 872 (Wisc. 1990)).

[169] *See* TEX. CIV. PRAC. & REM. CODE § 82.001(3) (defining "seller" to mean "a person who is engaged in the business of distributing or otherwise placing, for any commercial purpose, in the stream of commerce for use or consumption a product or any component

to look more broadly at Amazon's relationships with its third-party merchants and conclude that its role "comported with the purposes of strict liability."[170]

In *Oberdorf* and *Bolger*, the Third Circuit and California Court of Appeal confronted a somewhat different situation. Neither Pennsylvania nor California has enacted a comprehensive product liability statute, and both states instead implement the *Restatement (Second)* as a matter of common law.[171] For the Third Circuit, this made its *Erie*-guess[172] significantly more challenging; for in the words of the state's Supreme Court: "language of an 'adopted' restatement provision is not 'considered controlling in the manner of a statute' " and must be "tested against the facts of each case."[173] Likewise, Court of Appeal found itself with no on-point precedent and only a mandate to "give the rule of strict liability a broad application."[174] Still, like in Texas and Wisconsin, both Pennsylvania and California's courts have applied the rule of strict liability to cases where there was no transfer of title.[175] Thus, because the Third Circuit and Court of Appeal both recognized that the facts in their cases "weigh[ed] in favor of imposing strict liability on Amazon,"[176] they did just that—hold-

---

part thereof"); *see also State Farm*, 390 F. Supp. 3d at 971 ("[N]othing in [Wisconsin law] restricts those liable for defective products to some narrow class of specially defined sellers or distributors.").

[170] *McMillan*, 433 F. Supp. 3d at 1044.

[171] Greenman v. Yuba Power Prods., Inc., 377 P.2d 897 (Cal. 1963); *see also* Webb v. Zern, 220 A.2d 853, 854 (Pa. 1966) (setting forth Section 402A of the RESTATEMENT (SECOND) OF TORTS and "adopt[ing] the foregoing language as the law of Pennsylvania").

[172] *See infra* notes 271–274 and accompanying text.

[173] Tincher v. Omega Flex, Inc., 104 A.3d 328, 354 (Pa. 2014); *see also id.* at 355 ("[W]e underscore the importance of avoiding formulaic reading of common law principles and 'wooden application of abstract principles to circumstances in which different considerations may pertain.' ") (quoting Scampone v. Highland Park Care Center, LLC, 57 A.3d 582, 605 (Pa. 2012)).

[174] Bolger v. Amazon.com, LLC, 267 Cal. Rptr. 3d 601, 612 (Cal. Ct. App. 2020) (cleaned up).

[175] *See, e.g.*, Hoffman v. Loos & Dilworth, Inc., 452 A.2d 1349, 1354 (Pa. Super. Ct. 1982) (holding that a "sales agent" who took a commission for accepting orders and arranging product shipment could be held liable as the "seller" of the product); Canifax v. Hercules Powder Co., 237 Cal. App. 2d 44 (Cal. Ct. App. 1965) (applying strict liability to a "jobber").

[176] Oberdorf v. Amazon.com, Inc., 930 F.3d 136, 147–48 (3d Cir. 2019).

ing that "Amazon is strictly liable for consumer injuries caused by defective goods purchased on Amazon.com."[177]

Although each of these decisions marked a setback for Amazon, it's unclear how lasting their consequences will be. As of this writing, the appeals for several of them remain pending, which creates some uncertainty as to the decisions' long-term status. And regardless, most plaintiffs suing Amazon won't be able to choose the law of states with such broad (or non-existent) product liability statutes. They also won't be able to rely on case law rejecting Amazon's title-based definition of "seller." Instead, without further action by state courts and legislatures, future litigation will likely play out much like the following case study, leaving the vast majority of the consumer class with no meaningful remedy.

C. "The Flaming Headlamp Case"[178]

The case of *Erie Insurance v. Amazon.com* began in April 2014 when a fire broke out in Mihn and Ahn Nguyen's Burtonsville, Maryland, home. After containing the blaze, which caused extensive damage to the house and surrounding property, investigators were able to trace its origins to a defective LED headlamp that the Nguyens had borrowed from a friend several days prior. That friend, in turn, had originally purchased the headlamp from a company called Dream Light operating through Amazon's online Marketplace.[179] The Nguyens' insurer paid out over $300,000 to cover the repairs and other fire related expenses, after which it exercised its right to subrogation and filed suit in a Maryland state court to recover some of these costs.[180]

---

[177] *Id.* at 151; see also *Bolger*, 267 Cal. Rptr. 3d at 624 ("[T]he novelty of these issues does not prevent us from applying the doctrine where, as here, it is warranted.").

Shortly after the decision in *Oberdorf*, a district court in New Jersey reached the same conclusion in a separate suit against Amazon. Papataros v. Amazon.com, Inc., No. 2:17-CV-09836 (Dkt. 38), 2019 WL 4011502, at *19 (D.N.J. Aug. 26, 2019). While this case nominally applied New Jersey's Product Liability Act, the opinion noted that its analysis was "fundamentally structured" by the *Oberdorf* decision. *Id.* at *1. And indeed, proceedings were stayed once the Third Circuit announced that it would be reconsidering that case *en banc*. *See* No. 2:17-CV-09836 (Dkt. 42), 2019 WL 4740669, at *1 (D.N.J. Sept. 3, 2019).

[178] Oral Argument at 0:20, Erie Insurance Co. v. Amazon.com, 925 F.3d 135 (4th Cir. 2019) (No. 18-1198), *available at* https://www.ca4.uscourts.gov/OAarchive/mp3/18-1198-20190321.mp3.

[179] Complaint at 2, Erie Ins. Co. v. Amazon.com, Inc., No. 8:16-CV-02679 (D. Md. July 25, 2016).

[180] *Id.*

From the start, *Erie Insurance* followed a familiar trajectory. Amazon first removed the case to a federal court.[181] Then, after several months of discovery, it filed a motion for summary judgement that raised both of its standard defenses: 1) "Amazon simply provided . . . an online marketplace for a buyer and a seller to consummate their own sale," and 2) its actions were "protected by Section 230 of the Communications Decency Act."[182] After several rounds of replies and sur-replies, the district judge issued a bench ruling that granted Amazon's motion on both grounds.[183] Making almost no reference to Maryland law, the judge rejected the plaintiff's argument that Amazon was either a seller or a middle-man in the transaction, instead finding that it merely provided a sales platform.[184] And "even if I am incorrect with respect to [Amazon's role]," the judge concluded, "[Section 230] would preclude the claims in any event."[185]

The insurer appealed to the Fourth Circuit, which affirmed the grant of summary judgement.[186] The panel's opinion began by observing that Maryland courts view all product liability claims—whether sounding in negligence, strict liability, or warranty—as largely coterminous; and that the focus in each is directed towards "the liability of a *seller* for a defective product."[187] The state's commercial code, for example, provides an implied warranty against the "seller" of goods,[188] and Maryland courts had fully adopted the *Restatement (Second)*'s formulation of strict liability as attaching to "one who *sells* any product in a defective condition. . . ."[189] Moreover, these courts have never indicated that the term "seller" carries anything but its ordinary meaning, and that the ordinary meaning involves "the transfer of ownership of and the title to prop-

---

[181] *See* Notice of Removal from Circuit Court for Montgomery County Maryland, Erie Ins. Co. v. Amazon.com, Inc., No. 8:16-CV-02679 (Dkt. 1) (D. Md. July 25, 2016).
[182] Motion for Summary Judgement by Amazon.com, Inc., Erie Ins. Co. v. Amazon.com, Inc., No. 8:16-CV-02679 (Dkt. 45), 2017 WL 8793493, at *6 (D. Md. Sept. 15, 2017).
[183] *See* Erie Ins. Co. v. Amazon.com, Inc., No. 8:16-CV-02679, 2018 WL 3046243, at *3 (D. Md. Jan. 22, 2018).
[184] *Id.*
[185] *Id.*
[186] Erie Ins. Co. v. Amazon.com, Inc., 925 F.3d 135, 144 (4th Cir. 2019) ("At bottom, we conclude that Amazon was not, in this particular transaction, a seller.").
[187] *Id.* at 141 (citing Miles Labs., Inc. v. Doe, 556 A.2d 1107, 1123 (Md. 1989)) (emphasis in original).
[188] MD. CODE ANN., COM. LAW § 2-315 (LexisNexis 2020).
[189] *Erie*, 925 F.3d at 141 (citing Phipps v. Gen. Motors Corp., 363 A.2d 955, 957 (Md. 1976)) (emphasis added).

erty. . . ."[190] Thus, concluded the Fourth Circuit, while no case was directly on-point, Maryland courts would be unlikely to view Amazon as the "seller" of the defective headlamp and therefore subject to a product liability claim.[191]

However, the panel did reject the district court's conclusion about the scope of Section 230. It first held that by the law's own terms, its grant of immunity only applies in cases where the claim is "based on the interactive computer service provider's publication of a third party's speech."[192] Yet, this was not the basis of the plaintiff's claims; they were premised on the contention that Amazon was "liable as the seller of a defective product."[193] The third-party merchant may have drafted a product description that appeared on Amazon's website, but the insurance company was not suing because that description was defamatory or misrepresented the product.[194] Therefore, while Section 230 may protect companies like Amazon from liability as a publisher of speech, "it does not protect them from liability as a seller of a defective product."[195]

While the panel was unanimous in its opinion on the present state of Maryland law, Judge Motz wrote separately to express her view that "this may not always be so."[196] After strongly implying that Amazon had deliberately structured its operations to avoid precisely the liability at issue in this case,[197] she observed that much of product liability law was developed to match the then-existing retail model, which ensured that consumers would always have some legal recourse if they purchased an injurious product.[198] Amazon's success, she noted, has come about pre-

---

[190] *Id.* (quoting MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1129, 1097 (11th ed. 2007)).

[191] *Id.* at 144. The court also rejected the insurer's arguments that Amazon was an "entrustee" or "distributor" under Maryland law. The former form of liability, it held, only applies when "a rightful owner attempts to sue a buyer after the buyer purchases goods from a merchant." *Id.* at 143 (quoting Great Am. Ins. Co. v. Nextday Network Hardware Corp., 73 F. Supp. 3d 636, 640 (D. Md. 2014)). As to the latter, it held that Amazon's logistical support made it no more liable than UPS Ground, which had delivered the headlamp. *Id.* at 142.

[192] *Id.* at 139.

[193] *Id.*

[194] *Id.* at 140.

[195] *Id.*

[196] *Id.* at 144 (Motz, J., concurring).

[197] *See id.* at 145 (noting that "[it] is surely no accident" that Maryland law resolved this case in Amazon's favor).

[198] *Id.* at 144 ("[S]ome entity in this linear supply chain is clearly a "seller" and available for service of process within the United States.").

cisely because it disrupted this traditional model by eliminating many of the logistical hurdles that once kept foreign or otherwise judgement-proof manufacturers from placing dangerous goods into the stream of commerce.[199] Still, while the common law can change, especially in light of public policy considerations, she concluded that this is the job of state courts. As such, absent a certification request from either party, all that federal courts can do is enforce the status quo, no matter how dated.[200]

III. Product Liability for an Age of Amazon

The previous Parts have discussed the ways in which courts have struggled to fit the round peg of Amazon into the square hole of product liability doctrine. But as Robert Rabin has argued, "doctrinal analysis is essentially static—an organizing tool but little more—unless it is attentive to the policy concerns that channel discretion in one direction or another."[201] This Part takes up those policy concerns, arguing that Amazon both can and should be liable for the defective products sold through its Marketplace. And as state courts are the best institutions to weigh these policy concerns and develop their common law, this Part argues for greater use of the certification process to ensure their involvement.

A. The Costs of Accidental Immunity

The law of strict product liability has always been grounded in what James Hackney described as "pragmatic instrumentalism": a blend of policy considerations, institutional economics, and other Realist concerns about the social significance of legal outcomes.[202] Even the doctrine's most vocal critics seem to accept this outcome-focused orientation, focusing their critiques on whether it is the most efficient or effective means to those ends.[203] Thus, when considering whether Ama-

---

[199] *Id.*
[200] *Id.* at 145.
[201] Rabin, *supra* note 21, at 794.
[202] Hackney, *supra* note 40, at 444–45. Hackney, in turn, credits the term to Robert Summers, who used it to define the general legal theory that viewed law as "a body of practical tools for serving specific substantive goals." Robert S. Summers, *Pragmatic Instrumentalism in Twentieth Century American Legal Thought—A Synthesis and Critique of Our Dominant General Theory About Law and Its Use*, 66 CORNELL L. REV. 861, 863 (1981).
[203] *See* Polinsky & Shavell, *supra* note 84, at 1472–76 (concluding that for many commonly sold products, the burdens imposed by a system of no-fault recovery outweigh its

zon *does* fall within the metes and bounds of product liability doctrine, courts ought to begin with the question of whether it *should*.

As discussed above, Prosser and his contemporaries relied on a trio of public policy arguments as they worked to usher strict liability into existence,[204] and each of these arguments, when considered today, weighs heavily in favor of extending liability to Amazon. Take their first justification: that "the supplier, by placing the goods upon the market, represents to the public that they are suitable and safe for use."[205] In Amazon's case, these representations aren't just implicit—the company expressly warrants the quality of third-party products as part of its A-to-Z Guarantee, promising consumers a full refund if they "received an order that is different than expected."[206] And it is in no small part because of these representations—along with the general imprimatur that being sold through Amazon's website provides—that customers choose to transact with many of these third-party merchants at all. In recent years, Amazon has aggressively recruited foreign companies into its Marketplace, promising to cut out the middlemen and bypass the regulations that separate these companies from American consumers.[207] The result of this growing cross-border e-commerce has been a breakdown in the layers of importers and inspections that once permitted greater policing of unsafe products entering the United States.[208] Yet for Amazon's users, these products appear in search results as just one option among many, allowing them to

---

benefits); William M. Landes & Richard Posner, *A Positive Economic Analysis of Products Liability*, 14 J. LEGAL STUD. 535, 566 (1985) (arguing that for a "significant though unknown fraction" of goods, strict products liability is not economically rational).

[204] *See supra* notes 57–67 and accompanying text.

[205] Prosser, *Assault*, *supra* note 27, at 1123.

[206] *About A-to-Z Guarantee*, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html?nodeId=201889410 (last visited Jan. 13, 2021). While a few courts have pooh-poohed this policy as nothing more than "occasional distribution of refunds to consumers," Amazon's assurances that it will serve as a financial backstop against unscrupulous sellers must surely be at least one reason that so many consumers have been willing to pay for what are effectively credence goods. State Farm Fire and Casualty Co. v. Amazon.com, Inc., 407 F. Supp. 3d 848, 852 (D. Ariz. 2019).

[207] Jon Emont, *Amazon's Heavy Recruitment of Chinese Sellers Puts Consumers at Risk*, WALL ST. J. (Nov. 11, 2019), https://www.wsj.com/articles/amazons-heavy-recruitment-of-chinese-sellers-puts-consumers-at-risk-11573489075.

[208] *Id.* ("It's not normal that a factory with 200 people manufacturing baby monitors in Dongguan can ship products directly to consumers in Minnesota.").

purchase a defective headlamp from a company whose identity is later impossible to determine with just one click.[209]

All this is, of course, assuming that customers are even aware that they are making a purchase from a third-party seller. In contrast to other online marketplaces, Amazon's user interface makes the information about the seller somewhat difficult to discern.[210] The site only displays the name of the actual seller "in small-type under the area indicating whether the item is in stock or not, buried in an information-dense area of the user-interface called the 'buy-box.'"[211] Thus, many consumers likely do not notice this information at all, instead assuming that they are buying their goods "from Amazon."[212] But even when the nature of the transaction is clear, Amazon does almost nothing to inform its customers about the actual identity of these companies or their trustworthiness. In many cases, the website provides users with just a seller's trade name,[213] making any research beyond the (not-infrequently fraudulent)[214] customer reviews posted to the site impossible.[215] Additionally, Amazon's practice of commingling inventory at its warehouses means that "a product or-

---

[209] *Cf.* Erie Ins. v. Amazon Inc., 925 F.3d 135, 144 (4th Cir. 2019) (No. 18-1198), 2018 WL 3070080 (Motz, J., concurring) (noting that Amazon's business model "reduc[es] the friction that might keep foreign (or otherwise judgment-proof) manufacturers from putting dangerous products on the market").

[210] Ryan Bullard, *Out-Teching Products Liability: Reviving Strict Products Liability in an Age of Amazon*, 20 N.C. J.L. & TECH. ONLINE 181, 208 (2019), https://ncjolt.org/wp-content/uploads/sites/4/2019/05/Bullard_Final.pdf.

[211] *Id.*

[212] *See, e.g.*, Allstate N.J. Ins. Co. v. Amazon.com, Inc., No. 17-CV-2738 (FLW)(LHG), 2018 WL 3546197, at *1 (D.N.J. July 24, 2018) (noting that the plaintiff, who purchased the defective product from a Hong Kong-based company through Amazon's Marketplace, was "under the impression that Amazon was the [ ] seller").

[213] In *Erie Insurance*, for example, the defective headlamp was sold by a company identified as "Dream Light" in Amazon's Marketplace. It was only during discovery that the plaintiffs identified the seller as a Chinese national named XiaoCong Chen. Brief for Appellant at 4-5, Erie Ins. Co. v. Amazon.com, Inc., 925 F.3d 135 (4th Cir. 2019) (No. 18-1198), 2018 WL 3070080.

[214] *See, e.g.*, Complaint ¶¶ 12–16, Fed. Trade Comm'n v. Cure Encapsulations, Inc., No. 1:19-cv-00982 (Dkt. 1) (E.D.N.Y. Feb. 19, 2019) (alleging that an Amazon merchant violated the FTC Act by paying for fake product reviews).

[215] *See* Emont, *supra* note 207 ("It is often hard to tell that an Amazon seller is based in China . . . [The website] shows no indication the products are Chinese and gives no store address.").

dered from a third-party seller may not have originated from that particular seller."[216]

Amazon fares no better under Prosser's second justification for strict liability. To the extent that cost spreading remains a legitimate goal of tort law, it seems evident that Amazon should play at least some role when the victim of a defective product seeks legal redress.[217] Not only is the company almost always the best financed out of the pool of potential defendants, it is also uniquely positioned to spread the costs of these claims. True, Amazon does not directly set the prices of third-party goods, but it still has tremendous latitude in "charging predictable fees that allow the third-party vendors to set the overall product price after taking into account Amazon's share and the third-party's desired markup."[218] Alternatively, the company could simply purchase more comprehensive liability insurance, spreading the cost of its increased premiums by incrementally raising the fees it charges its third-party sellers.[219] These sellers are, after all, already required to indemnify Amazon for the costs of product defect lawsuits.[220]

But the most persuasive of Prosser's policy rationales for applying strict liability to Amazon is his argument that "[t]he public interest in human life, health and safety demands the maximum possible protection that the law can give against dangerous defects in products . . . ."[221] In 1964, this meant applying strict liability to include not only manufacturers but also retailers, who constituted "an integral part of the overall producing and marketing enterprise" that led to a product's arrival in a consumer's home.[222] In 2020, this means applying the doctrine to Amazon. "It's not normal that a factory with 200 people manufacturing baby monitors in Dongguan[, China,] can ship products directly to consumers

---

[216] Serena Ng & Greg Bensinger, *Do You Know What's Going in Your Amazon Shopping Cart?*, WALL ST. J. (May 11, 2014, 8:31 PM), https://www.wsj.com/articles/on-amazon-pooled-merchandise-opens-door-to-knockoffs-1399852852.

[217] *Cf.* Edelman & Stemler, *supra* note 10, at 187 ("When objections to a marketplace are best addressed through a solution with large up-front costs but low marginal costs, it may be efficient to impose liability only on especially large marketplaces.").

[218] Bullard, *supra* note 210, at 221.

[219] *Id.* at 222–23.

[220] *See Amazon Services Business Solutions Agreement*, *supra* note 124, ¶ 6 (requiring third-party sellers to indemnify Amazon against any third-party claim or loss arising from the seller's products, including "any personal injury, death (to the extent the injury or death is not caused by Amazon), or property damage related thereto").

[221] Prosser, *Assault*, *supra* note 27, at 1122.

[222] Vandermark v. Ford Motor Co., 391 P.2d 168, 171 (Cal. 1964).

in Minnesota," yet that is exactly what Amazon's platform allows.[223] The result has been a Marketplace that contains thousands of defective, mislabeled, and occasionally outright illegal products, all just one click away from consumers who are unable to even guess at their quality.[224] Liability may be "a pillar of the law,"[225] but it is one that plays little role in regulating one of Amazon's most profitable business lines.

To be clear, a Wild West is not the inevitable state of affairs for an online marketplace, and to the extent that tort law is about efficient deterrence, Amazon is well-positioned to spread the costs of any safety improvements. It could, for example, require all of its third-party merchants to obtain comprehensive liability insurance, a requirement it already imposes on its largest sellers.[226] Alternatively, it could follow its rivals' lead and tighten the vetting process used to screen would-be sellers before they can access its platform.[227] It could even simply redesign its user interface to more prominently display the identity of the third-party seller, ensuring that customers fully understand that they are not making a purchase "from Amazon."[228] There is likely no silver bullet, and these or other changes to its Marketplace could well reduce its offerings or raise its prices while failing to deliver meaningful safety improvements. But Amazon is the best positioned actor to determine what solution could prove effective while weighing its costs-and-benefits; therefore, tort law should provide it with an incentive to do so.[229]

Finally, strict liability's application to Amazon finds strong support in Goldberg and Zipursky's civil recourse theory. For the vast ma-

---

[223] Emont, *supra* note 207.

[224] *See* Alexandra Berzon, Shane Shifflett, and Justin Scheck, *Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products.*, WALL ST. J. (Aug. 23, 2019, 9:56 AM), https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990?mod=article_inline.

[225] Van Loo, *supra* note 132, at 143.

[226] *See Amazon Services Business Solutions Agreement*, *supra* note 123, ¶ 9 (requiring sellers whose gross proceeds exceed $10,000 per-month over any three consecutive months to obtain at least $1 million of liability insurance).

[227] *See* Berzon, Shifflet & Scheck, *supra* note 224 (reporting that the application to become a seller on Walmart's platform "can take days for approval, and only a fraction of merchants applying make it through the vetting," while Target's platform is invitation-only).

[228] *See supra* note 212 and accompanying text.

[229] *Cf.* Calabresi & Hirschoff, *supra* note 72, at 1060–61 ("The issue becomes not *whether* avoidance is worth it, but which of the parties is relatively more likely to find out whether avoidance is worth it.").

jority of plaintiffs, a finding that Amazon cannot be held liable effectively ends their avenues for recovery. They cannot, as Amazon has repeatedly argued, simply redirect their claims towards the third-party seller, who in many cases are either extraterritorial, insolvent, or otherwise judgement-proof.[230] Nor can they sue the product's manufacturer, who—even assuming they can be identified[231]—is just as unlikely to be subject to service of process. For the victims of defective Marketplace products, a suit against Amazon is their only means of accessing tort law's grant of political power.[232]

B. Re-Felling the Citadel

Notwithstanding these policy justifications, Amazon has largely avoided liability when third-parties on its platform sell defective products that go on to injure their purchasers.[233] This section takes a more critical look at the company's legal arguments and offers several suggestions for how courts could once again re-fell the citadel whose downfall Prosser once celebrated.

1. On Sellers and Title

Surprisingly few states have actually defined the term "seller" in their product liability statutes, and those that have almost all adopted some variant of the UPLA's vague and somewhat recursive definition.[234] Indiana, for example, rather unhelpfully defines "seller" as "a person engaged in the business of selling or leasing a product,"[235] and this defini-

---

[230] *See, e.g.*, Oberdorf v. Amazon.com Inc., 930 F.3d 136, 142 (3rd Cir. 2019) ("Neither Amazon nor Oberdorf has been able to locate a representative of [the third-party seller], which has not had an active account on Amazon.com since May 2016.").

[231] *See* Allstate N.J. Ins. Co. v. Amazon.com, Inc., 2018 WL 3546197, at *11 (D.N.J. July 24, 2018) (noting that in that case, "Amazon admits that it does not know the manufacturer's identity").

[232] *See* Goldberg & Zipursky, *supra* note 78, at 1946 ("By empowering victims to demand a determination whether they have been victimized and, should they prove their cases, by entitling them to recourse, tort law grants to citizens an important political power.").

[233] *See supra* notes 132–134 and accompanying text.

[234] *See* Model Uniform Product Liability Act, 44 Fed. Reg. 62,714, 62,717 (1979) ("'Product seller' means any person or entity that is engaged in the business of selling products, whether the sale is for resale, or for use or consumption. The term includes a manufacturer, wholesaler, distributor, or retailer of the relevant product. The term also includes a party who is in the business of leasing or bailing such products.").

[235] IND. CODE ANN. § 34-6-2-136 (West).

tion is typical. Minor variations exist between jurisdictions, but none in any way ties the meaning of "seller" to the entity holding title to a defective product. Indeed, many states explicitly include bailors within the scope of the term "seller,"[236] and bailments—by definition—do not involve a transfer of title.[237] Only Texas appears to have meaningfully departed from the UPLA's model, but its definition of "seller" is even more capacious: "'Seller' means a person who is engaged in the business of distributing or otherwise placing, for any commercial purpose, in the stream of commerce for use or consumption a product or any component part thereof."[238] Case law is similarly unilluminating; to the extent that title transfer is referenced, it is "merely one factor among many in determining whether strict liability is appropriate."[239]

Amazon's move, then, has been to point courts away from the definition of "seller" in states' product liability statutes and towards the definitions of "seller" and "sale" in their U.C.C. provisions.[240] In *Erie Insurance*, for example, Amazon argued that "[u]nder Maryland law, a 'seller' is defined as 'a person who sells or contracts to sell goods,'" and that "a 'sale' consists in the passing of title from the seller to the buyer for a price."[241] Likewise in *Fox*, it argued that "[t]he ordinary meaning of the word 'sell,' from which 'seller' and 'selling' are derived, involves transferring a thing that one owns to another in exchange for something

---

[236] *E.g.*, MD. CODE ANN., CTS. & JUD. PROC. §5-405(5) (LexisNexis 2020) ("'Seller' means a wholesaler, distributor, retailer, or other individual or entity other than a manufacturer that is regularly engaged in the selling of a product whether the sale is for resale by the purchaser or is for use or consumption by the ultimate consumer. 'Seller' includes a lessor or bailor regularly engaged in the business of the lease or bailment of the product.").

[237] *Bailment*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[238] TEX. CIV. PRAC. & REM. CODE ANN. § 82.001(3) (West 2019).

[239] Bullard, *supra* note 210, at 214. The Supreme Court has recently weighed in on what it means to directly sell a good, albeit in a very different context. *See* Apple Inc. v. Pepper, 139 S. Ct. 1514, 1519 (2019) (holding that when iPhone users purchase applications from third-party developers through Apple's App Store, they become Apple's "direct purchasers" for purposes of federal antitrust law).

[240] *See* U.C.C. § 2-103(d) ("'Seller' means a person who sells or contracts to sell goods."); § 2-106 ("A 'sale' consists in the passing of title from the seller to the buyer for a price.").

[241] Brief for Appellee at 12, Erie Ins. Co. v. Amazon.com, Inc., 925 F.3d 135 (4th Cir. 2019), 2018 WL 3618157 (quoting MD. CODE ANN., COM. LAW §§ 2-103(1)(d) and 2-106(1)).

of value," and that "[t]he legal meaning of the term is the same."[242] As previously noted, most courts have either accepted this assertion as dispositive or at least as a significant factor weighing against finding Amazon liable.[243]

This argument might seem reasonable enough on its face; after all, looking to surrounding statutory provisions to discern the meaning of an ambiguous term is a well-trodden canon of statutory interpretation.[244] The problem, though, is that the U.C.C. uses the term "seller" to define the scope of its implied warranty of merchantability—the promise that goods sold by a merchant are "fit for the ordinary purposes for which such goods are used."[245] Yet an implied warranty necessarily attaches to a smaller class of defendants than does strict product liability; indeed, as discussed above, the doctrine of strict liability was developed in part because of limitations to recovery under the law of sales.[246] Thus, just because a defective product did not breach an implied warranty does not mean that the seller is off the hook. And by accepting Amazon's arguments to the contrary, courts disregard decades of precedent that undergird modern product liability doctrine.[247]

"Strict products liability," as the *Restatement (Third)* puts it, "is a term of art that reflects the judgment that products liability is a discrete area of tort law which borrows from both negligence and warranty. It is not fully congruent with classical tort or contract law."[248] The more plausible reading of these product liability statutes is that they use the term "seller" to mean something broader than the parties who would be liable under the U.C.C. The UPLA itself suggests as much, stating that "[t]his Act is in lieu of and preempts all existing law governing matters within its coverage, including the 'Uniform Commercial Code' and similar laws."[249] And it would go a long way towards explaining why the UPLA

---

[242] Brief for Appellee at 16, Fox v. Amazon.com, Inc., 930 F.3d 415 (6th Cir. 2019), (No. 18-5661), 2018 WL 5784393 (citing TENN. CODE ANN. § 47-2-106(1)).
[243] *See supra* notes 159–62 and accompanying text.
[244] *See* ANTONIN SCALIA & BRYAN GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS (2012).
[245] MD. CODE ANN, COM. LAW § 2-314(2)(c) (LexisNexis 2020); *accord* TENN. CODE ANN. § 47-2-314(2)(c) (West).
[246] *See supra* notes 23–28 and accompanying text.
[247] *See* Bullard, *supra* note 210, at 211 ("Any requirement for a retailer or distributor to hold title in a defective product in order for it to be subject to strict liability is absent from products liability statutes, from the *Restatement* and from relevant case law.").
[248] RESTATEMENT (THIRD), *supra* note 16, § 1, cmt. a.
[249] Model Uniform Product Liability Act, 44 Fed. Reg. 62,714, 62,720 (Oct. 31, 1979).

or state product liability acts did not just directly incorporate the U.C.C.'s title-based definition, which was already several decades old when these statutes were being drafted. Courts considering Amazon's liability should recognize these differences and maintain the distinction between the law of sales and product liability doctrine.

2. Auction Houses and Other Analogies

Precedent and analogy lie at the heart of legal reasoning, and courts have relied heavily on both as they have grappled with Amazon's place in the product liability doctrine. Amazon has been described in judicial opinions as an auctioneer, a flea market, a broker, and even a newspaper's classified-ads section.[250] Courts have reasoned from product liability precedent involving sales agents,[251] asbestos importers,[252] and even Amazon's rival platform—eBay.[253] Analogical reasoning can be a powerful tool, permitting "principled consistency" across a range of factual scenarios.[254] But because no two cases are exactly alike, its utility requires that analogies be premised on meaningful similarities and irrelevant differences—what Frederick Schauer described as "rules of relevance."[255] In the Amazon's case, this means that courts ought to tread carefully when they apply pre-internet precedent and remain attentive to the ways in which the digital revolution "has caused far-reaching systemic and structural change in the economy."[256]

Amazon is no auction house. True, the two share a few superficial similarities: both provide a marketplace for third-party sellers, both allow those sellers to set their own prices, and both leave those sellers with the profits of the transaction less some predetermined fee. For many judges,

---

[250] *See* Bullard, *supra* note 210, at 207.
[251] Oberdorf v. Amazon.com, Inc., 930 F.3d 136, 148 (3rd Cir. 2019) (citing Hoffman v. Loos & Dilworth, Inc., 452 A.2d 1349 (Pa. 1982)).
[252] Garber v. Amazon.com, Inc., 380 F. Supp. 3d 766, 776 (N.D. Ill. 2019) (citing Hammond v. N. Am. Asbestos Corp., 454 N.E.2d 210 (Ill. 1983)).
[253] Stiner v. Amazon.com, Inc., 120 N.E.3d 885, 891 (Ohio Ct. App. 2019), *aff'd* No. No. 2019-0488, 2020 WL 5822477 (Ohio Oct. 1, 2020) (citing Inman v. Technicolor USA, Inc., No. 11-666, 2011 WL 5829024, at *5 (W.D. Pa. Nov. 18, 2011)).
[254] Cass R. Sunstein, Commentary, *On Analogical Reasoning*, 106 HARV. L. REV. 741, 746 (1993).
[255] Frederick Schauer, *Precedent*, 39 STAN. L. REV. 571, 577–79 (1987). Schauer illustrated this principle by noting that "[a] judgment finding tort liability based on the ownership of a black dog is precedent for a judgment regarding the owner of a brown dog, but not for a judgment regarding the owner of a black car." *Id.* at 577.
[256] Direct Marketing Ass'n v. Brohl, 575 U.S. 1, 18 (2015) (Kennedy, J., concurring).

these have been the relevant similarities, making their states' decades-old case law controlling.[257] Yet there are also significant differences between them, especially when a seller takes part in the Fulfilled by Amazon program; as Judge Motz's concurrence in *Erie Insurance* points out, "[n]early the only thing Amazon [does] not do" in these transactions is hold title.[258] "Amazon even assume[s] the risk of credit card fraud, receive[s] payment, and remit[s] a portion of that payment to the manufacturer."[259] And even when a third-party seller handles their own logistics, many of Amazon's other practices—in particular, its extensive data collection from both third-party sellers and consumers and its application of endorsements like "Amazon's Choice"[260]—make it distinct from any other member of a pre-internet distribution chain.

Even setting all of those differences aside and assuming that Amazon's third-party sales are nothing more than twentieth-century online auctions, its cyber nature constitutes a relevant difference that justifies departing from prior case law. The internet is a fundamentally different medium than its preceding analogues, a point that the Supreme Court has repeatedly made in a range of otherwise diverse contexts. For example, the Court recently permitted states to assess sales taxes against retailers who lack a physical presence in the consumer's state—in the process reversing more than a quarter-century of case law.[261] It justified its departure from the principle of *stare decisis* by highlighting the ways in which "[t]he Internet's prevalence and power have changed the dynamics of the national economy."[262] Likewise, the Court has repeatedly declined to expand its criminal procedure jurisprudence wholesale into the digital

---

[257] *E.g.*, Oberdorf v. Amazon.com, Inc., 930 F.3d 136, 157–58 (3rd Cir. 2019) (Scirica, J., concurring in part and dissenting in part); Erie Ins. Co. v. Amazon.com, 925 F.3d 135, 143 (4th Cir. 2019).
[258] *Erie*, 925 F.3d at 145 (Motz, J., concurring).
[259] *Id.*; *see also* Edelman & Stemler, *supra* note 10, at 188 ("These mechanisms of standardization and control may suggest that the putative online marketplace is not an intermediary between sellers and buyers at all, but the true seller.").
[260] Nicole Nguyen, *"Amazon's Choice" Does Not Necessarily Mean a Product is Good*, BUZZFEED NEWS (June 14, 2019, 2:54 PM), https://www.buzzfeednews.com/article/nicolenguyen/amazons-choice-bad-products.
[261] South Dakota v. Wayfair, Inc., 138 S. Ct. 2080, 2097 (2018), *rev'g* Quill Corp. v. North Dakota, 504 U.S. 298 (1992).
[262] *Id.*

world, rejecting analogies to older case law that minimize the constitutional novelty of technological progress.[263]

Amazon is a trillion dollar enterprise, capturing almost half of all online spending while employing over half a million workers.[264] Its platform has revolutionized commerce, connecting buyers and sellers in ways that would not have been possible in the pre-internet world. All the while, it has become a pioneer in mining its user base for what Shoshana Zuboff has termed "behavior surplus": data scraped from its customers' searches and transactions that can be repackaged into valuable prediction products.[265] Whatever the privacy and antitrust implications of these practices, their novelty belies the claim that Amazon's business practices can be neatly analogized to preceding models.[266]

Rules of relevance "are contingent upon both time and culture," and even factors once thought dispositive must be viewed in the context of a changing world.[267] Whatever the precedential value of the twentieth-century decisions, they can neither fully resolve Amazon's place within modern product liability doctrine, nor should they be mechanically applied to cases involving third-party merchants. The alternative—treating Amazon a flea market or an auction house—is an example of analogical reasoning gone awry, "an inadequate inquiry into the matter of relevant differences and governing principles."[268]

---

[263] *E.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (declining to extend the third-party doctrine to cell-site location information); Riley v. California, 573 U.S. 373, 403 (2014) (declining to extend the doctrine permitting warrantless searches incident to lawful arrest to include a suspect's cell phone). *See also* Orin Kerr, *Forward: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403 (2013) ("Maintaining the function of old rules can require changing those rules to adapt to the new environment.").

[264] David Streitfeld, *Amazon Hits $1,000,000,000,000 in Value, Following Apple*, NY TIMES (Sept. 4, 2018), https://www.nytimes.com/2018/09/04/technology/amazon-stock-price-1-trillion-value.html.

[265] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 74–82 (2019); *see also id.* at 269 ("Amazon is on the hunt for behavioral surplus.").

[266] Genevieve Lakier has made a similar point when discussing the First Amendment's application to search engines. *See* Genevieve Lakier, *The Problem Isn't the Use of Analogies but the Analogies Courts Use*, KNIGHT FIRST AMEND. INST. (Feb. 26, 2018), https://knightcolumbia.org/content/problem-isnt-use-analogies-analogies-courts-use.

[267] Schauer, *supra* note 255, at 578.

[268] Sunstein, *supra* note 254, at 746.

C. Certified Liability

If the policy rationale for extending liability to Amazon is so strong and most states' product liability statutes permit this interpretation, why have plaintiffs failed in nearly every attempt? One important reason appears to be Amazon's practice of removing product liability suits to federal court,[269] a forum that gives the company an important structural advantage as it litigates these questions.

Since *Erie*, federal courts have lacked the ability to create general common law and must instead resolve diversity suits by applying the laws of the forum state.[270] Sometimes that law is clear and well-settled, making the federal court's job a straightforward exercise in applying precedent to facts. But in other cases, where that law is unsettled or where the suit presents a question of first impression, a task is much harder. The Supreme Court has held that even in these cases, state law provides an answer; and so the task of a court sitting in diversity is to "ascertain from all the available data what the state law is and apply it."[271] This exercise, sometimes called an "*Erie* guess," is intended to produce vertical uniformity between federal and state courts, removing the incentive for the kind of forum-shopping that was endemic in pre-*Erie* litigation.[272] "[F]or the same transaction," the Court has written, "the accident of a suit by a non-resident litigant in a federal court instead of in a State court a block away, should not lead to a substantially different result."[273]

In practice, however, these guesses about unsettled state law can and often do turn out to be inconsistent.[274] There is some debate as to why this is the case. It could be, as one federal judge noted, that the federal judiciary is just less attuned to "the nuances of that state's history, policies, and local issues" than are their state court counterparts.[275] Alterna-

---

[269] *See supra* notes 136–39 and accompanying text.
[270] Erie R.R. Co. v. Thompkins, 304 U.S. 64, 78 (1938).
[271] West v. Am. Tel. & Tel. Co., 311 U.S. 223, 237 (1940).
[272] 19 CHARLES ALAN WRIGHT ET AL., FEDERAL PRAC. & PROC. § 4507 (3d ed. 1998).
[273] Guaranty Trust Co. v. York, 326 U.S. 99, 109 (1945).
[274] *See* John L. Watkins, Erie *Denied: How the Federal Courts Decide Insurance Coverage Cases Differently and What to Do About It*, 21 CONN. INS. L.J. 455, 459 (2015) ("A number of distinguished jurists have recognized that incorrect *Erie* guesses have plagued the federal judiciary for years in many different substantive areas of the law."); Dolores K. Sloviter, *A Federal Judge Views Diversity Jurisdiction Through the Lens of Federalism*, 78 VA. L. REV. 1671, 1679 (1992) ("Despite our best efforts to predict the future thinking of the state supreme courts," those courts "have found fault with a not insignificant number of past '*Erie* guesses' . . . .").
[275] Sloviter, *supra* note 274, at 1682.

tively, some scholars have more cynically suggested that *Erie* guesses are more a reflection of what federal judges think state law *should* be, rather than what state law actually *is*.[276] Finally, it might just be that some cases present such difficult legal questions that any court—state or federal—would struggle to arrive at consistent answers. As Judge Friendly once quipped, "Our principal task, in this diversity of citizenship case, is to determine what the New York courts would think the California courts would think on an issue about which neither has thought."[277]

But regardless of the reason, one thing that is clear is that an area where federal courts tend to be especially conservative in their *Erie* guesses is when they are asked to expand the scope of state law.[278] That, they almost invariably hold, is the task of state tribunals, not federal diversity courts. And even where recent state court decisions might permit a reasonable guess as to the direction of state law, federal judges are still reticent to alter the status quo.[279] As one court recently put it, "we should perhaps—being out of the mainstream of [our state's] jurisprudential development—be more chary" of blazing a new trail "than should an inferior state tribunal," even where recent decisions allow the "predict[ion] with assurance where that law would be had it been declared."[280]

Whatever the merits of this judicial modesty, one of its consequences has been the rise of a new type of forum shopping.[281] Where state law is unclear but liability depends on its extension to new and untested circumstances, defendants have a strong incentive to ensure cases are heard in a forum in which judges are institutionally hesitant to take precisely this step. Federal courts' skepticism towards accepting novel claims disrupts the horizontal uniformity that *Erie* guesses were intended to create.[282] The result is a playing field tilted strongly towards maintain-

---

[276] Laura E. Little, *Erie's Unintended Consequence: Federal Courts Creating State Law*, 52 AKRON L. REV. 275, 283–84 (2015).
[277] Nolan v. Transocean Air Lines, 276 F.2d 280, 281 (2d Cir. 1960), *judgement set aside*, 365 U.S. 293 (1961).
[278] *See* 17A JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRAC. – CIVIL ¶ 124.22(6), n.17 (3d ed. 1997) (collecting cases).
[279] *Id.*
[280] Meador v. Apple, Inc., 911 F.3d 260, 264 (5th Cir. 2018); *see also id.* ("If guidance from state cases is lacking, 'it is not for us to adopt innovative theories of recovery under state law.'") (quoting Mayo v. Hyatt Corp, 898 F.2d 47, 49 (5th Cir. 1990)).
[281] Watkins, *supra* note 274, at 474–75.
[282] *See* Bradford R. Clark, *Ascertaining the Laws of the Several States: Positivism and Judicial Federalism After* Erie, 145 U. PA. L. REV. 1459, 1542 (1997) (noting that federal court rigidity leads to a situation where "parties benefited by the status quo will

ing the status quo, and as a result, the party favored by this status quo "will almost invariably seek federal jurisdiction . . . in order to prevent the state's highest court from reaching the issue."[283]

This is exactly the problem facing plaintiffs when Amazon removes their product liability lawsuits to federal courts. By design, Amazon has disrupted the twentieth-century retail model, literally transforming the way in which many Americans shop.[284] It should come as no surprise, then, that its role doesn't fit neatly within the confines of existing product liability doctrine and that state law needs to evolve for the policy concerns outlined above to be effectuated. But this is just the sort of common lawmaking that federal courts are most hesitant to undertake. It may also explain why federal courts have instead largely just tried to apply definitions drawn from U.C.C. provisions and state court decisions involving auctioneers, flea markets, and other distinctly un-Amazon entities.[285] The result has been a continuation of a status quo—a world in which Amazon almost never faces legal repercussions when third-party merchants peddle dangerous goods through its website.[286]

Yet even as a lack of state court precedent relating to Amazon's liability creates this situation, it also signals the path forward. Removal does not and should not signal the end of state court involvement, and the Supreme Court has long indicated a strong preference for state law questions to be answered in "courts equipped to rule authoritatively on them."[287] For suits against Amazon, this probably doesn't mean a remand; with a few rare exceptions, federal judges cannot send properly removed cases back to a state court, even if a state court is the more appropriate

---

inevitably seek to litigate their cases in federal, rather than state, court," as federal courts will only adopt novel claim or defense if "the party can establish that it has been adopted by an appropriate organ of the state").

[283] McCarthy v. Olin Corp., 119 F.3d 148, 158 (2d Cir. 1997) (Calabresi, J., dissenting).

[284] *See* Nick Statt, *How Amazon's Retail Revolution is Changing the Way We Shop*, VERGE (Oct. 23, 2018), https://www.theverge.com/2018/10/23/17970466/amazon-prime-shopping-behavior-streaming-alexa-minimum-wage ("Amazon has already changed how we shop and, by extension, how we live our lives.").

[285] *See supra* Part III.B.2.

[286] *Id.* Indeed, Amazon has argued that federal courts not only *should* avoid expanding the scope of strict liability, but also that they *must* avoid doing so. Supplemental En Banc Brief for Appellee Amazon.com, Inc. at 14, Oberdorf v. Amazon.com, Inc., 930 F.3d 136 (3rd Cir. 2019) (No. 18-1041), 2019 WL 5304320.

[287] Arizonans for Official Eng. v. Ariz., 520 U.S. 43, 76 (1997).

forum.[288] Nor does it require abstention, which under the Court's present doctrine is only appropriate in cases where a state's "sovereign prerogative" hangs in the balance.[289] Instead, federal courts should turn to the procedure designed for precisely the situation they face with Amazon—certification.

With the sole exception of North Carolina, every state and territory now permits federal courts sitting in diversity to submit questions of law to the forum's high court for authoritative resolution.[290] Originally developed as a more efficient alternative to a *Pullman* abstention, certification is now a widely available tool for federal courts, providing them with a valuable means of avoiding the difficult policy choices inherent in *Erie* guesses.[291] The Supreme Court has enthusiastically endorsed the practice, noting that "in the long run [it] save[s] time, energy, and resources and helps build a cooperative judicial federalism."[292] Its use has widespread support throughout all levels of the judiciary.[293] And academic commentators have been similarly effusive, describing certification as a way to promote comity, reduce the judicial guesswork that necessarily accompanies *Erie* guesses, and eliminate incentives for forum shopping by ensuring a uniform state law.[294]

---

[288] *See generally* 14C WRIGHT ET AL., *supra* note 272, § 3739; *see also* Lehmen Bros. v. Schein, 416 U.S. 386, 390 (1974) ("[T]he mere difficulty in ascertaining local law is no excuse for remitting the parties to a state tribunal for the start of another lawsuit.").

[289] Louisiana Power & Light Co. v. City of Thibodaux, 360 U.S. 25, 28 (1959).

[290] Gregory L. Acquaviva, *The Certification of Unsettled Questions of State Law to State High Courts: The Third Circuit's Experience*, 115 PA. ST. L. REV. 377, 384–85 (2010); *see also id*. at 385, n.59 (listing the relevant statutes).

[291] Clark, supra note 282, at 1548–49; *see also* Jonathan Remy Nash, *Examining the Power of Federal Courts to Certify Questions of State Law*, 88 CORNELL L. REV. 1672, 1681 (2003) ("Today, certification is the primary method by which federal courts faced with undecided questions of state law are able to enlist the aid of state courts to resolve those questions.").

[292] *Lehmen Bros.*, 416 U.S. at 391; *see also Arizonans for English*, 520 U.S. at 79 ("Taking advantage of certification made available by a State may 'greatly simplify[y]' an ultimate adjudication in federal court.") (quoting Bellotti v. Baird, 428 U.S. 132, 151 (1976)).

[293] *See* Acquaviva, *supra* note 290, at 387 ("[V]oluminous empirical studies demonstrat[e] widespread approval of certification procedures among both state and federal judges.").

[294] *See* William G. Bassler & Michael Potenza, *Certification Granted: The Practical and Jurisprudential Reasons Why New Jersey Should Adopt a Certification Procedure*, 29 SETON HALL L. REV. 491, 498 (1998) ("Certification promotes comity and cooperative federalism by allowing the highest court of each state to develop governing principles of state substantive law."); *id.* at 499 ("Certification furthers the underlying principle of

Despite this favorable consensus, certifications remain quite rare, with "*Erie*-guesses . . . remain[ing] federal courts' preferred method of ascertaining the meaning of unclear state law."[295] The reasons for this are complex and likely, at least in part, procedural; some states do not allow district judges to certify questions,[296] while others are so slow in responding that any efficiencies from the practice are lost.[297] There is also a strong belief within some corners of the federal judiciary that resolving these state law cases is a key part of the federal judge's job and a rejection of arguments that certification produces an answer that is in any way "better."[298] This predisposition against certification has been on full display in product liability suits against Amazon. Out of all the federal court opinions examined in this review, just three even mentioned certification as an option, one of which only did so to state that it would be inappropriate absent a request by either party.[299]

This cannot be correct. Certification has never required a request from the litigants, nor is their objection to it fatal. The only necessary condition for a federal court to certify is the presence of "[n]ovel, unsettled questions of state law."[300] Other factors are certainly relevant,[301] and clearly not every unsettled question can or should be certified. But "principles of federalism and comity favor giving a State's high court the op-

---

Erie—elimination of forum shopping—through the development of a single definitive statement of state substantive law."); Haley N. Schaffer & David F. Herr, *Why Guess? Certification and the Eighth Circuit*, 36 WM. MITCHELL L. REV. 1625, 1627 ("Certification allows [federal courts] to avoid *Erie* guesses and thus avoid errors while at the same time providing litigants with a correct and more efficient determination of their legal rights than abstention."). *But see* Justin R. Long, *Against Certification*, 78 GEO. WASH. L. REV. 114 (2009) (offering the rare dissenting view from this consensus).

[295] Frank Chang, Note, *You Have Not Because You Ask Not: Why Federal Courts Do Not Certify Questions of State Law to State Courts*, 85 GEO. WASH. L. REV. 251, 256 (2017).

[296] *E.g.*, PA. CODE § 29.451 (only permitting certification from "The United States Supreme Court; or [a]ny United States Court of Appeals").

[297] *See* JONA GOLDSCHMIDT, CERTIFICATION OF QUESTIONS OF LAW: FEDERALISM IN PRACTICE 54 (1995).

[298] *See* Chang, *supra* note 295, at 256; *see also* Bruce M. Selya, *Certified Madness: Ask a Silly Question . . .*, 29 SUFFOLK U. L. REV. 677, 687 (1995) ("I believe that it engenders more understanding, and a healthier respect for state courts and what they do, when federal courts tackle the complexities of state law head on.").

[299] Erie Ins. Co. v. Amazon.com, 925 F.3d 135, 145 (4th Cir. 2019) (Motz J., concurring).

[300] Arizonans for English v. Arizona, 520 U.S. 43, 79 (1997).

[301] *See* MOORE ET AL., *supra* note 278, ¶ 124.22(7)(c)(ii) (surveying cases and identifying seven factors that various courts have considered when deciding whether to certify).

portunity to answer important questions of state law," particularly where answering those questions "require[s] the weighing of policy considerations."[302] This means that when a circuit court goes *en banc* to determine the meaning of state tort law,[303] it is probably failing to give state courts their due. The better solution would be to let the state's high court answer the question that has so divided this group of federal jurists.

Federal courts do a disservice to the development of state law when they permit litigants to forum shop their way to a desired outcome. This was true pre-*Erie*, when federal courts explicitly made their own common law, and it is true post-*Erie,* when federal courts provide a forum for litigants who wish to maintain the status quo. Whatever Amazon's reasons for seeking removal,[304] the result of its litigation strategy has been a preservation of a status quo in which the world's largest online store often bears no liability for its customers' injuries. And it is only now—more than 20 years since zShops first launched—that the first state high court finally has the chance to weigh in.[305]

"When federal courts, in effect, prevent state courts from deciding unsettled issues of state law, they violate fundamental principles of federalism and comity."[306] The federal judiciary ought to recognize this result as a consequence of Amazon's litigation strategy and use the tools at their disposal to respond in kind. Recently the Fifth Circuit did just that. In December 2020, the court certified the question of Amazon's liability in *McMillan* to Texas's Supreme Court, which agreed to hear the case several weeks later.[307] Whatever decision Texas's nine justices ultimately reach, it will be an authoritative pronouncement on the Lone Star

---

[302] Town of Castle Rock, Colorado v. Gonzales, 545 U.S. 748, 777 (2005) (Stevens, J., dissenting).

[303] *Cf.* Oberdorf v. Amazon.com, Inc., 936 F.3d 182 (3rd Cir. 2019) (mem.) (granting petition for rehearing *en banc*).

[304] And to reiterate: Amazon's preference for a federal forum might well be motivated by considerations beyond perceived differences in outcome. *See supra* notes 140–43 and accompanying text.

[305] *Cf.* Stiner v. Amazon.com, Inc., 129 N.E.3d 461 (Ohio 2019).

[306] McCarthy v. Olin Corp., 119 F.3d 148, 158 (1997) (Calabresi, J., dissenting).

[307] *See* Orders on Cases Granted, Amazon.com, Inc. v. McMillan, No. 20-0979 (Tex. Jan. 8, 2021).

The Fifth Circuit is actually the second court to have certified the question of Amazon's liability to a state's high court. In June 2020—almost four months after *en banc* oral arguments—the Third Circuit certified the question in *Oberdorf* to the Pennsylvania's Supreme Court. *See* Order requesting Certification of Question of State Law to Pennsylvania Supreme Court pursuant to Third Circuit LAR Misc. 110, Oberdorf v. Amazon.com Inc., No. 18-01041, Dkt. 114 (3d Cir. June 2, 2020). Shortly thereafter the

State's law, not just a guess. It will also be a decision by a court able to directly grapple with the competing policy concerns central to this case. For a question with such sweeping implications that some scholars have warned it could mark the "end of online marketplaces,"[308] that seems indisputably the better outcome.

Conclusion

After a 2019 investigation by the *Wall Street Journal* identified thousands of unsafe, mislabeled, and recalled products for sale on Amazon's Marketplace,[309] a group of senators wrote to Jeff Bezos to express their "grave concerns."[310] "Unquestionably," the lawmakers wrote, "Amazon is falling short of its commitment to keeping safe those consumers who use its massive platform," warning the company that reacting to negative publicity did not show a real commitment to consumer protection.[311] In response, Amazon promised reforms, describing an "industry-leading safety and compliance program" while touting a $400 million investment in machine learning tools for identifying suspicious products.[312] Yet over a year later, little seems to have changed. In March 2020—as the nation was entering into its first coronavirus lockdown—a follow-up investigation by the *Journal* found hundreds of mislabeled, counterfeit, and potentially ineffective masks and respirators for sale through its Marketplace, many sold by sellers who were also engaged in illegal price gouging.[313]

---

parties settled, and the case was dismissed as moot. *See* Order dismissing case pursuant to Fed. R. App. P. 42(b), No. 18-01041, Dkt. 119 (3d Cir. Sept. 23, 2020).

[308] Eric Goldman, *Amazon May Be Liable for Marketplace Items–Oberdorf v. Amazon*, TECH. & MKTG. L. BLOG. (July 8, 2019), https://blog.ericgoldman.org/archives/2019/07/amazon-may-be-liable-for-marketplace-items-oberdorf-v-amazon.htm.

[309] *See* Berzon, Shifflett, and Scheck, *supra* note 224.

[310] Letter from Richard Blumenthal, Robert Menendez, and Edward Markey, United States Senators, to Jeff Bezos, CEO and Chairman, Amazon.com, Inc. (Aug. 29, 2019), available at https://www.blumenthal.senate.gov/imo/media/doc/2019.08.29%20Letter%20to%20Amazon%20re%20Defective%20Products%20FINAL%20pdf.pdf?mod=article_inline.

[311] *Id.*

[312] *Product Safety and Compliance in Our Store*, DAY ONE: THE AMAZON BLOG (Aug. 23, 2019), https://blog.aboutamazon.com/company-news/product-safety-and-compliance-in-our-store?mod=article_inline.

[313] Alexandra Berzon and Daniela Hernandez, *Amazon Battles Counterfeit Masks, $400 Hand Sanitizer Amid Virus Panic*, WALL ST. J. (Mar. 11, 2020), https://www.wsj.com/articles/amazon-battles-counterfeit-masks-400-hand-sanitizer-amid-virus-panic-11583880384.

Even product liability's critics have conceded that "market forces usually will be less effective for products that are not widely sold and the companies that sell these products will tend to have weaker incentives to increase their safety."[314] For many of Amazon's third-party sellers, the effect of those market forces appears to be nil. The platform's vast scale and its sellers' relative anonymity mean that many listings on its Marketplace are effectively credence goods, and even ex post investigations are frequently unable to identify the actual manufacturer.[315] Thus, courts should permit plaintiffs to sue Amazon for defective products sold through its Marketplace, evolving the scope of product liability doctrine to match the realities of a twenty-first century world. And when this litigation takes place in federal fora, courts should follow the lead of the Fifth Circuit, using the tools at their disposal to ensure that state judges shape the future of state law.

* * *

[314] Polinsky & Shavell, *supra* note 84, at 1449; *see also id.* at 1476 ("This observation strengthens the case for product liability for products that are not widely sold . . . .").
[315] Alexandra Berzon, *How Amazon Dodges Responsibility for Unsafe Products: The Case of the Hoverboard*, WALL ST. J. (Dec. 5, 2019), https://www.wsj.com/articles/how-amazon-dodges-responsibility-for-unsafe-products-the-case-of-the-hoverboard-11575563270.

Appendix

Product liability lawsuits filed against Amazon from January 1, 2015, through December 31, 2020, involving goods sold by third-party merchants. Cases marked with a "+" symbol indicate those successfully removed to federal court. Cases marked with a ++ symbol indicate those removed to federal court but ultimately remanded back to state court.

Litigated Through a Case Dispositive Motion

- *State Farm Fire & Cas. Co. v. Amazom.com Servs., Inc.*, No. 008550/2019, 2020 WL 7234265 (N.Y. Sup. Ct. Dec. 8, 2020)
- *Indiana Farm Bureau Ins. v. Amazon.com, Inc.*, No. 1:19-cv-01568, 2020 WL 6400808 (S.D. Ind. Oct. 3, 2020)
- *Wright v. Amazon.com, Inc.*, No. 2:19-cv-00086, 2020 WL 6204401 (D. Utah Oct. 22, 2020)+
- *Wallace v. Tri-State Assembly, LLC*, No. 155741/2017, 2020 WL 3104357 (N.Y. Sup. Ct. June 11, 2020)
- *McMillan v. Amazon.com, Inc.*, 433 F. Supp. 3d 1034 (S.D. Tex. 2020), *question certified*, 983 F.3d 194 (5th Cir. 2020)+ *Philadelphia Indemnity Ins. Co. v. Amazon.com, Inc.*, 425 F. Supp. 3d 158 (E.D.N.Y. 2019)+
- *State Farm Fire & Casualty Co. v. Amazon.com, Inc.*, 414 F. Supp. 3d 870 (N.D. Miss. 2019)
- *State Farm Fire & Casualty Co. v. Amazon*, 407 F. Supp. 3d 848 (D. Ariz. 2019), *aff'd* 2020 WL 6746745 (9th Cir. 2020)+
- *Papataros v. Amazon*, 2019 WL 4011502 (D.N.J. Aug. 26, 2019), *order stayed* 2019 WL 4740669 (D.N.J. Sept. 3, 2019)+
- *State Farm Fire & Casualty Co. v. Amazon*, 390 F. Supp. 3d 964 (W.D. Wis. 2019)
- *Garber v. Amazon.com, Inc.*, 380 F. Supp. 3d 766 (N.D. Ill. 2019)+
- *Loomis v. Forrinx Tech. (USA), Inc.*, No. BC632830, 2019 WL 2031426 (Cal. Super. Ct. Apr. 2, 2019), *appeal filed* No. B297995 (Cal. Ct. App. May 6, 2019)
- *Carpenter v. Amazon*, 2019 WL 1259158 (N.D. Cal. March 19, 2019), *appeal filed*, No. 19-15695 (9th Cir. 2019)
- *Bolger v. Herocell, Inc.,* No. 37-2017-00003009-CU-PL-CTL (Cal. Super. Ct. Mar. 6, 2019), *rev'd sub nom., Bolger v. Amazon.com, LLC*, 267 Cal. Rptr. 3d 601 (Cal. Ct. App. 2019)
- *Love v. WEECCO(TM)*, 2018 WL 5044639 (N.D. Ga. Oct. 17, 2018), *rev'd and remanded*, 774 F. App'x 519 (11th Cir. 2019)

- *Eberhart v. Amazon.com, Inc.*, 325 F. Supp. 3d 393 (S.D.N.Y. 2018)
- *Allstate New Jersey v. Amazon.com, Inc.*, 2018 WL 3546197 (D.N.J. July 24, 2018)+
- *Fox v. Amazon.com, Inc.*, 2018 WL 2431628 (M.D. Tenn. May 30, 2018), *aff'd in part, rev'd in part*, 930 F.3d 415 (6th Cir. 2019)+
- *Erie Insurance Co. v. Amazon.com, Inc.*, 2018 WL 3046243 (D. Md. Jan. 22, 2018), *aff'd in part, rev'd in part,* 925 F.3d 135 (4th Cir. 2019)+
- *Stiner v. Amazon.com, Inc.*, 2017 WL 9751163 (Ohio Com. Pl. Sept. 20, 2017), *aff'd* 120 N.E.3d 885 (Ohio Ct. App. 2019), *aff'd* No. 2019-0488, 2020 WL 5822477 (Ohio Oct. 1, 2020)
- *Oberdorf v. Amazon.com, Inc.*, 295 F. Supp. 3d 496 (M.D. Pa 2017), *aff'd in part, vacated in part*, 930 F.3d 136 (3d Cir. 2019), *reh'g en banc granted*, 936 F.3d 182 (3d Cir. 2019), *question certified*, 237 A.3d 394 (Pa. 2020), *dismissed* (3d Cir. Sept. 23, 2020)*McDonald v. LG Electronics USA, Inc.*, 219 F. Supp. 3d 533 (D. Md. 2016)+

Pending

- *Lorentson v. Amazon.com, Inc.*, No. 2:20-cv-01832 (W.D. Wash. filed Dec. 21, 2020)
- *Scott v. Global Vision, Inc.*, No. 3:20-cv-01287 (S.D. Ill. filed Dec. 1, 2020)
- *Carrilo v. Amazon.com, Inc.*, No. 3:20-cv-02347 (S.D. Cal. filed Dec. 1, 2020)
- *Phy v. Instant Brands Inc.*, No. 6:20-cv-01325 (D. Kan. filed Nov. 20, 2020)
- *Kimmel v. Samsung SDI Co. Ltd.*, No. 2:20-cv-01998 (D. Ariz. filed Oct. 15, 2020)
- *Burnett v. Amazon.com, Inc.*, No. 1:20-cv-03959 (N.D. Ga. filed Sept. 24, 2020)
- *Walker v. Honest Industries, Inc.* No. 4:20-cv-02289 (S.D. Tex. filed June 29, 2020)
- *Garza v. Altaire Pharmaceuticals Inc.*, No. 3:20-cv-01524 (N.D. Tex. filed June 10, 2020)+
- *Hubacki v. Classic Brands, LLC*, No. 20STCV15094 (Cal. Super. Ct. filed Apr. 20, 2020)++
- *Harrison-Wood v. Amazon.com, Inc.*, No. 20-2-05905-1 (Wash. Super. Ct. filed Apr. 16, 2020)
- *Sgherza v. Kozyar*, No. 3:30-cv-03649 (D.N.J. filed Apr. 3, 2020)

- *Hanafy v. Bodum Holdings AG*, No. 4:20-cv-01110 (S.D. Tex. filed Apr. 1, 2020)
- *Great Northern Insurance Co. v. Amazon.com, Inc.*, No. 1:19-cv-00684 (N.D. Ill. filed Feb. 1, 2020)+
- *Williams ex rel. K.W.B. v. Amazon.com, Inc.*, No. 2:20-cv-00408 (E.D. Pa. filed Jan. 24, 2020)
- *Vasile v. Amazon.com, Inc.*, No. 2:19-cv-20477 (D.N.J. filed Nov. 19, 2019)+
- *Warnshuis v. Amazon.com, Inc.*, No. 1:19-cv-01454 (E.D. Cal. filed Oct. 15, 2019)+
- *Huber v. Sunbeam Products, Inc.*, No. 2:19-cv-01776 (E.D. Cal. filed Sept. 06, 2019)+
- *USAA Gen. Indemnity Co. v. Amazon.com, Inc.*, No. 18-2-08310-4 (Wash. Super. Ct. filed May 24, 2018).
- *N.J. Mfrs. Ins. Grp. v. Dauhatsu Industria e Comercio de Moveis e Aparelhos Electricos LTDA*, No. 2:18-cv-09038-KM-CLW (D.N.J. filed May 10, 2018)
- *Buonavolanto v. LG Electronics U.S.A., Inc.*, No. 1:18-CV-02802 (N.D. Ill. filed Apr. 19, 2018)+
- *Jarrett v. Amazon.com, Inc.*, No. 1:17-cv-06357 (D.N.J. filed Aug. 23, 2017)
- *Bradley v. EasyACC.com, Inc.*, No. 2:17-CV-01587 (E.D. Pa. filed Apr. 7, 2017)+

Settled or Otherwise Voluntarily Dismissed

- *Farm Bureau Prop. & Cas. Ins. Co. v. Amazon.com, Inc.*, No. 0:20-cv-00756 (D. Minn. dismissed Oct. 22, 2020)
- *Cooper v. Instant Brands Inc.*, No. 1:18-cv-02611 (D. Colo. dismissed Aug. 28, 2020)+
- *State Farm Gen. Ins. Co. v. Anker Innovations Ltd.*, No. 2:20-cv-00606 (E.D. Cal. dismissed Aug. 27, 2020)+
- *Rosario v. Joovy Holding Co.*, No. 1:19-cv-24356 (S.D. Fla. dismissed Aug. 20, 2020)+
- *Hacala v. Amazon.com, Inc.*, No. 5:19-cv-05131 (W.D. Ark. dismissed July 22, 2020)+
- *Allsop v. Amazon Svcs. Inc.*, No. HHD-CV19-6117350-S (Conn. Super. dismissed May 14, 2020)++
- *Nelson v. Amazon Fulfillment Services, Inc.*, No. 2:19-cv-02518 (E.D.N.Y. dismissed Apr. 30, 2020)+

- *Cannon v. Amazon.com, Inc*, No. 3:20-cv-00216 (N.D. Tex. dismissed Feb. 18, 2020)
- *Maisel v. Hoverboard LLC*, No. 0708441/2017 (N.Y. Sup. Ct., dismissed Mar. 12, 2020)
- *Fulkerson v. ASDM Beverly Hills, Inc.*, No. 1:19-cv-04095 (S.D. Ind. dismissed Feb. 27, 2020)+
- *Tanner v. Elive Limited*, No. 2:19-cv-00336 (D. Nev. dismissed Oct. 4, 2019)+
- *CSAA Insurance Exchange v. Siker Power Inc.*, No. 3:19-cv-01652 (N.D. Cal. dismissed Aug. 6, 2019)+
- *Kenny v. LC Holdings, LLC*, No. 1:18-cv-00472 (S.D. Ohio dismissed July 22, 2019)+
- *Hughes v. Medical Depot Inc.*, No. 2:18-cv-02187 (D.S.C. dismissed July 3, 2019)
- *General Ins. Co. of Am. v. Amazon.Com Services, Inc.*, No. 5:18-cv-02072 (N.D. Cal. dismissed May 28, 2019)+
- *Schaffner-Wilson v. Amazon.com Inc.*, No. 2:19-cv-00034 (N.D. Ind. dismissed Apr. 17, 2019)
- *Arellano v. Allwin Powersports Corp.*, No 2:19-cv-00462 (C.D. Cal. dismissed Apr. 8, 2019)+
- *Sarvis v. Expo International Inc.*, No. 4:18-cv-01270 (D.S.C. dismissed Feb. 15, 2019)
- *Kijewski v. Amazon.com LLC*, No. 3:18-cv-00440 (E.D. Va. dismissed Jan. 3, 2019)+
- *Georgiou v. Louisville Ladder, Inc.*, No. 4:17-cv-06588 (N.D. Cal. dismissed Dec. 10, 2018)+
- *Silin v. Instant Brands, Inc.*, No. 5:18-cv-00781 (N.D. Cal. dismissed Nov. 16, 2018)
- *Triolo v. Amazon.com, Inc.*, No. 2:17-cv-06661 (E.D.N.Y. dismissed Oct. 17, 2018)
- *Stokes v. Amazon.com, LLC*, No. 6:17-cv-03269 (W.D. Mo. dismissed Aug. 29, 2018)+
- *Taylor v. Amazon.com, Inc.*, No. 2:17-cv-08046 (C.D. Cal. dismissed June 26, 2018)+
- *Riley v. Amazon.com, Inc.*, No. 7:17-cv-00223 (S.D. Tex. dismissed Apr. 18, 2018)+
- *Apeldoorn v. Amazon.com, Inc.*, No. 4:17-cv-01954 (N.D. Ala. dismissed Mar. 2, 2018)
- *Ballinger v. Amazon.com, Inc.*, No. 17-CI-00450 (Ky. Cir. Ct. dismissed Jan. 1, 2018)++

- *Sweatt v. Amazon.com, Inc.*, No. 2:16-cv-00179-RWS (N.D. Ga. dismissed Dec. 14, 2017)+
- *Lambert v. SIYA Inc.*, No. 5:16-cv-01605 (S.D. W.Va. dismissed June 15, 2017)+
- *Kross v. Leray Group LTD*, No. BC606676 (Cal. Super. Ct. dismissed May 22, 2017)
- *Tomcik v. Amazon.com LLC*, No. 3:16-cv-01704 (N.D. Cal. dismissed May 11, 2017)
- *State Farm Fire v. Horizon Hobby, LLC*, No. 6:16-cv-00691 (D. Or. dismissed Jan. 22, 2017)+
- *Brown v. VSHZ Inc.*, No. 4:15-cv-04684 (D.S.C. dismissed Dec. 13, 2016)
- *Merrill v. Amazon.com, Inc.*, No. 2:16-cv-00063 (D. Wyo. dismissed Dec. 13, 2016)
- *Cox v. Brand 44, LLC*, No. 1:15-cv-11903 (D. Mass. dismissed Oct. 7, 2016)

The Moral Case for Adopting a U.S. Right to be Forgotten

Lindsay Holcomb*

Introduction

In 1940, British poet W.H. Auden wrote of an "Unknown Citizen" who was identified only by fragments of the data collected about him over the course of his life.[1] Hospitals, psychologists, schools, journalists, employers, and government organizations told of his good health, military service, education level, and the propriety of his opinions.[2] The poem's last two lines, however, underscore the shallowness and inadequacy of such information in forming a nuanced picture of the man's life. "Was he free? Was he happy?" Auden writes. "The question is absurd: Had anything been wrong, we should certainly have heard."[3]

Today, far more so than in the time of Auden, individuals are both unknown and all too knowable—the details of their lives available with just a few strokes of a keyboard, but largely devoid of context or character. Brief moments of a person's life can become defining features of his public self by virtue of the internet's infinite memory and an increasing feeling that with the right data, a person can be "known" without ever having met him. Around 80 percent of employers,[4] 30 percent of universities,[5] and 40 percent of law schools search applicants online.[6] "Slut shaming" and "revenge porn" sites dedicated to humiliating women by showing them in sexually vulnerable positions are visited each day,

---

* J.D. Candidate, University of Pennsylvania Law School, Class of 2021.

[1] W.H. Auden, *The Unknown Citizen, in* Another Time (1940).

[2] *Id.*

[3] *Id.*

[4] Cross-Tab, Online Reputation in a Connected World 6–8 (2010).

[5] Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, N.Y. Times (Nov. 9, 2013), http://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html?_r=0.

[6] Paulina Firozi, *Law School Admissions Use Facebook, Google to Screen Applicants, Study Finds,* Daily NW. (Oct. 30, 2011), https://dailynorthwestern.com/2011/10/30/campus/campusarchived/law-school-admissions-use-facebook-google-to-screen-applicants-study-finds/.

some garnering over 350,000 unique visitors.[7] Local newspapers, and sites like mugshotsonline.com, that compile booking photos from law enforcement agencies and display them to a broader public, profit off of the humiliation of others and leave a discoverable record of a person's brushes with the law.[8] As Internet Law scholar Viktor Mayer-Schönberger has written, the digital disclosure of the personal details of our lives, "will forever tether us to all our past actions, making it impossible, in practice, to escape them."[9]

The implications of a knowing society, fueled by a digital cultural memory, are complex and far-reaching. People lose their jobs because of social media posts;[10] they are denied degrees because of embarrassing information posted about them online;[11] they are prevented from coaching their kids' sports teams because of articles describing decades-old misdemeanors;[12] and they are haunted by cyberbullying and revenge porn when intimate or embarrassing images and facts make their way to the broader public. In essence, they are shamed, vilified, and othered, both online and in person, because the digital amalgam of their lives makes them appear wholly knowable and therefore, condemnable. Such information is, to quote Judge Barbara Lenk of the Massachusetts Supreme Court, a "virtual sword of Damocles," available instantaneously, around the clock, and anywhere in the world.[13]

---

[7] *See* Alex Morris, *Hunter Moore: The Most Hated Man on the Internet*, ROLLING STONE (Oct. 11, 2012, 9:10PM), http://www.rollingstone.com/culture/news/the-most-hated-man-on-the-Internet-20121113. (Most examples of victims used in the article were of women whose compromised photos were uploaded in the revenge-porn website).

[8] Ingrid Rojas & Natasha Del Toro, *Should Newspapers Make Money Off of Mugshot Galleries?,* FUSION (Mar. 9, 2016, 3:32 PM), https://fusion.tv/story/278341/naked-truth-newspapers-mugshot-galleries.

[9] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 125 (2009).

[10] *See* Sam Hananel, *Woman Fired Over Facebook Rant; Suit Follows*, NBCNEWS.COM (Nov 9, 2010, 5:08 PM), http://www.nbcnews.com/id/40097443/ns/business-careers/t/woman-fired-over-facebook-rant-suit-follows/#.XgAs9hdKh0s (exploring an instance of firing due to social media).

[11] MAYER-SCHÖNBERGER, *supra* note 9, at 1.

[12] Tom Jackman, *Successful Basketball Coach with 15-Year-Old Drug Conviction Challenges NCAA's 'No Felons' Rule*, WASH. POST (Jan. 23, 2017, 2:50 AM), https://www.washingtonpost.com/news/true-crime/wp/2017/01/23/successful-basketball-coach-with-15-year-old-drug-conviction-challenges-ncaas-no-felons-rule.

[13] *Doe v. Sex Offender Registry Bd.*, 41 N.E.3d 1058, 1067 (2015).

In the European Union, as of May 2014, this threat of digital memory has been countered with a new right to be forgotten, enabling individuals to request that search engines delist links to sensitive information about them.[14] The right is premised on the potential for rehabilitation—the idea that privacy allows us to fully evolve as individuals because it prevents others from digging up the digital memory of our past transgressions. As Mayer-Schönberger writes, "[w]e forgive through forgetting, but the digital tools that surround us no longer let us do that—and instead brutally remind us again and again, long into our future of the mistakes we've made in our past."[15] Years after a person has erred or offended in some way, details of an unfortunate incident can continue to haunt him as he endeavors to rebuild his life, stultifying his personal growth.

In the U.S., the right to be forgotten has generated ample criticism.[16] Many proclaim that the new right is a violation of free speech that in essence allows individuals to rewrite the past, undermining the work of journalists who understand themselves as writing the first drafts of history.[17] In the immediate aftermath of the European Court of Justice's ruling on the right to be forgotten, The New York Times Editorial Board argued that "lawmakers should not create a right so powerful that it could limit press freedoms or allow individuals to demand that lawful information in a news archive be hidden."[18] The Washington Post Editorial Board stated that the right was "not looking too wise."[19] An editor for the Chi-

---

[14] Case C-131/12, *Google, Inc. v. Mario Costeja*, ECLI:EU:C:2014:317, ¶ 2 (May 13, 2014).

[15] MAYER-SCHÖNBERGER, *supra* note 9, at 202.

[16] *See e.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000); Jens-Henrik Jeppesen & Emma Llansó, *EU 'Right to be Forgotten' Sets Bad Precedent for Free Expression Worldwide,* CTR. FOR DEMOCRACY & TECH. (Feb. 11, 2016) https://cdt.org/insights/eus-right-to-be-forgotten-policy-sets-bad-precedent-for-free-expression-worldwide; Victor Luckerson, *Americans Will Never Have the Right to Be Forgotten*, TIME (May 14, 2014, 8:46 AM), https://time.com/98554/right-to-be-forgotten.

[17] *See e.g.*, Volokh *supra* note 16, at 1122-23; Jeppesen *supra* note 16; Luckerson *supra* note 16.

[18] THE EDITORIAL BOARD, *Ordering Google to Forget*, N.Y. TIMES (May 13, 2014) https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html.

[19] Editorial, *UnGoogled: The Disastrous Results of the 'Right to be Forgotten' Ruling*, WASH. POST (Jul. 12, 2014), https://www.washingtonpost.com/opinions/ungoogled-the-disastrous-results-of-the-right-to-be-forgotten-ruling/2014/07/12/91663268-07a8-11e4-bbf1-cc51275e7f8f_story.html.

cago Tribune wrote of the right, "Once you turn censors loose, they seldom know where to stop,"[20] and an article in the Philadelphia Inquirer explained that it was highly unlikely that a right to be forgotten would ever cross the Atlantic.[21]

But is it so unlikely that such a right could ever be adopted in the U.S.? Is the right as harmful to the press as its critics insist? This article challenges the notion that the right to be forgotten is in direct opposition to the American values of free expression and the public's right to know by arguing that such a right has roots in American moral culture as well as jurisprudence in the right to rehabilitation, and ultimately, suggests adopting a form of the right to privacy in the U.S. Part I reviews the origins of the European right to be forgotten, focusing on the *Google Spain* decision and relevant articles of the General Data Protection Regulation (GDPR). Part II argues that the U.S. has long supported a rehabilitative notion of privacy, which provides sturdy ground on which the right to be forgotten could stand in the U.S. Part III addresses First Amendment criticisms of the right. Part IV assesses how the right to be forgotten might be operationalized in the U.S. This article concludes with a discussion of the moral benefits of a right to be forgotten, particularly in how a more forgiving society can in fact increase speech and democratic participation.

I. European Right to be Forgotten

This section will provide a historical overview of the right to be forgotten from the European Court of Justice's (ECJ) decision that established the right to the implementation of the right on Google, and finally, to the codification of the right in the GDPR. The purpose of outlining this four-year period in European privacy jurisprudence is not only to better understand the right to be forgotten and what sorts of content removal and delisting it permits, but also to recognize the strong through line of a commitment to second chances, fresh starts, and individual rehabilitation that undoubtedly motivates the right.

---

[20] Clarence Page, Opinion, *Google and the 'Right to be Forgotten,'* CHI. TRIB. (May 21, 2014), https://www.chicagotribune.com/opinion/ct-xpm-2014-05-21-ct-google-forgotten-right-europe-clarence-page-ope-20140521-story.html.

[21] John Timpane, *Can the Internet Learn to Forget?*, PHILA. INQUIRER (Jun 28, 2014, 3:01 AM), https://www.inquirer.com/philly/news/nation_world/20140628_Can_the_Internet_learn_to_forget_.html.

A. Birth of the Right to be Forgotten

The right to be forgotten was first formally established in 2014 when Mario Costeja Gonzalez, a Spaniard, lodged a complaint with the Agencia Española de Protección de Datos (AEPD)—the Spanish Data Protection Agency—against Spain's *La Vanguardia* newspaper, Google Spain, and Google Inc.[22] In 1998, *La Vanguardia* had published two articles announcing real estate auctions connected with the recovery of Costeja's social security debts, and years later, when people googled Costeja, links to the articles appeared on the first page of results.[23] By 2014, the attachment proceedings described in the articles had been resolved years before, and they were no longer relevant to his life. Thus, Costeja wanted the articles removed, either by the newspaper deleting the content or by Google delisting links to the content, so that the information about him would no longer be discoverable by others.[24]

While the AEPD determined that *La Vanguardia* did not have to comply with Costeja's request because its editors were mandated by the Spanish government to publish sales arising from social security debts, the AEPD ordered Google Spain and Google Inc. to delist the articles from their search results.[25] As the Agency argued, because search engines are data processors, they can be compelled to preclude access to information published on the internet in order to safeguard individuals' fundamental rights.[26] Google appealed the case to Spain's highest court, which in turn, referred the matter to the ECJ.[27] At this point, Costeja's claim had distilled into the weighty question of whether on the basis of the fundamental rights envisioned by European Data Protection Directive of 1995, operators of Internet search engines are obliged to remove or erase personal information published by third party websites, even when the information is true and the initial publishing of such information was lawful.[28]

Article 12(b) of the 1995 Directive provided that every data subject has the right to obtain from a data controller "the rectification, erasure, or blocking of data processing . . . in particular because of the incomplete or inaccurate nature of the data," while Article 14(a) granted the data subject the right to "object at any time . . . to the processing of

---

[22] Case C-131/12, *Google, Inc.*, ¶ 2.
[23] *Id.* ¶ 14.
[24] *Id.* ¶ 15.
[25] *Id.* ¶ 17.
[26] *Id.*
[27] *Id.* ¶¶ 18, 20.
[28] *Id.* ¶¶ 19–20.

data relating to him."[29] The court considered these positions in tandem with the data privacy protections laid out in Article 8 of the EU Charter of Fundamental Rights,[30] ultimately determining that search engines are subject to "affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name."[31] That is, by facilitating the investigation and disclosure of a subject's sensitive data, on the basis of a search of his name, Google affected individual privacy rights.[32]

From this conclusion, the court ruled that individuals whose personal data is accessible through search engine results may request that their information no longer be made available to the general public via inclusion in a list of results.[33] If, in a balancing test between the individual's privacy and the public's right to know, privacy is deemed a weightier concern, the individual may "invoke[e] his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion."[34] Individuals' rights of privacy override "not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name."[35] In sum, the ECJ established what has come to be known as "the right to be forgotten"—a legal privilege based on the idea that the fundamental right to privacy includes a right to request that certain data, particularly data that is no longer necessary to fulfill the purposes for which it was collected, be removed from the internet. Where data is not "adequate, relevant, and not excessive," as provided in the directive, and it is no longer in the public interest, it should be deleted.[36]

Implicit in this ruling is an understanding of the individual as a product of the data made available about him. Submerged under a mountain of publicly accessible data, an individual might find it difficult to differentiate himself or break free from what is already known about him.

---

[29] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 38, 31 (EC).
[30] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 10, https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[31] Case C-131/12, *Google, Inc.*, ¶ 80.
[32] *Id.*
[33] *Id.* ¶ 82.
[34] *Id.* at 3.
[35] *Id.* at 97.
[36] *Id.*

A person who went bankrupt decades ago might feel that he can never be seen as anything but a debtor because news of his financial troubles form the bulk of the publicly available information about him. As Mayer-Schönberger has written, comprehensive digital memory represents a "pernicious version of the digital panopticon," which shapes individual behavior and causes people to see themselves as they are seen by those watching them.[37] The ability for individuals to rid themselves of this digital record of their lives, and to be seen by others as different from whatever information a search engine might show about them, allows for the development of more free and self-actualized citizens. As Costeja told The Guardian newspaper the day after the ruling, "I was fighting for the elimination of data that adversely affects people's honour, dignity and exposes their private lives. Everything that undermines human beings, that's not freedom of expression."[38] The ECJ's decision ultimately reflected an acknowledgement that the representation of an individual's persona online produces tangible effects in his real life as well, undermining his ability to escape his past, even when he desperately wants to.

B. Implementing the *Google Spain* Decision

After the Google Spain decision, the independent European advisory body on data protection and privacy, also named the Article 29 Data Protection Working Party, published guidelines outlining how member states and search engines alike should implement the "right to be forgotten" pursuant to the ECJ decision.[39] The Working Party established a list of common criteria for delisting requests to assist agencies in their assessment of the complaints.[40] The criteria include whether: the data subject plays a role in public life, the subject is a minor, the data is accurate, the data is relevant and not excessive, the information is sensitive, the data is being made available for longer than necessary for the purposes of

---

[37] MAYER-SCHÖNBERGER, *supra* note 9, at 6.
[38] Ashifa Kassam, *Spain's Everyday Internet Warrior Who Cut Free from Google's Tentacles,* GUARDIAN (May 13, 2014), https://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez.
[39] Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/121, Article 29 Data Protection Working Party, WP225 (Nov. 26, 2014).
[40] *Id.* at 13–20.

processing, the processing is causing prejudice to the subject, and the search result links to information that puts the subject at risk.[41]

The most contentious of these criteria were, and remain, the subject's role in public life and the data's relevance, as both matters concern somewhat subjective evaluations. To that end, the Working Party posited that those who have a role in public life might include politicians, senior public officials, and business-people; and recommended that if the applicant has a role in public life and the information in question does not constitute genuinely private information, DPAs and search engines should be more hesitant to permit delisting results.[42]

Relevance, the Working Party explained, was in large part a factor of temporal pertinence.[43] If the information was published decades ago, it is almost certainly less relevant than data published within the last few years. Similarly, information that relates to the personal life of the applicant will be considered less relevant than information that relates to the professional life of the applicant, taking into account the individual's line of work and the public's interest in having information related to the individual's professional life based on his name.[44] One can imagine, for example, an article about a medical malpractice suit against a doctor, or bar sanctions levied against a lawyer, being of particularly high public interest in cases where a potential patient or client is searching for those professionals by name.

A strong motivation for the Working Party's efforts at better explaining the right was to provide intermediaries with the tools necessary to make their delisting decisions.[45] Google, for one, has explicitly stated that it evaluates requests in accordance with "carefully developed criteria in alignment with the Article 29 Working Party's guidelines."[46] As of November 2019, Google has received delisting requests for nearly 3.5 million URLs in the EU, 45 percent of which have been successful. Most controversial among critics of the right are the roughly 350,000 URL delisting requests that pertain to news articles covering crime, professional wrongdoing, or political involvement.[47] Examples of the content

---

[41] *Id.*
[42] *Id.* at 13–14.
[43] *Id.* at 15–16.
[44] *Id.* at 16.
[45] *Id.* at 5.
[46] Requests to delist content under European privacy law, GOOGLE: TRANSPARENCY REPORT, https://transparencyreport.google.com/eu-privacy/overview (last visited Dec. 31, 2020) [hereinafter TRANSPARENCY REPORT].
[47] *Id.*

successfully delisted ranged from a Bulgarian news article containing accusations about an individual sexually abusing his child, to a Spanish news article describing a businessman's involvement in an offshore tax avoidance scheme, to a British news article reporting that a person had been sentenced to 30 weeks in prison for causing grievous bodily harm to that individual's partner.[48]

From the little that Google discloses about the rationale behind its decisions, it seems clear that Google's reviewers make an effort to focus on the criterion of the data's relevance, respecting the data subject's efforts to rebuild his life after hardship. Often, in the limited decisions that Google makes publicly available, the reviewer justified her delisting choice in a successful deletion claim by explaining that the person had been acquitted of a criminal charge or had served his sentence. Thus, even in the nascent stages of the right to be forgotten in Europe, intermediaries were wary of the stultifying effects of reputationally damaging information online as the subjects of delisting requests attempted to rebuild their lives.[49]

C. Right to be Forgotten and the GDPR

In 2012, EU Justice Commissioner Viviane Reding delivered a speech titled "Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" to a conference in Munich.[50] In the speech, she argued that one of the most important ways "to give people control over their data" was to establish the right to be forgotten, and that Europeans would certainly have that right in the coming years.[51] "I want to explicitly clarify that people shall have the right—and not only the 'possibility'—to withdraw their consent to the processing of the personal data they have given out themselves," Reding told the audience.[52] "The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years

---

[48] *Id.*
[49] *Id.*
[50] Viviane Reding, Vice President of the European Comm'n and European Comm'r for Justice, Fundamental Rights and Citizenship, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 22, 2012) (transcript available at https://ec.europa.eu/com mission/press-corner/detail/en/SPEECH_12_26).
[51] *Id.*
[52] *Id.*

after they were shared or made public."[53] Reding's comments were largely well-received in Europe insofar as they seemed to establish what was already a widely-held ideological commitment on the continent—that people should have control over the representation of their online personas.[54] To that end, the proposal was merely illuminating laws and customs in existence at the time.

Still, when the right to be forgotten was solidified firmly into European law with the implementation of the GDPR in May 2018, it certainly went beyond the ECJ's conception of the right in both reach and strength.[55] This expansion recognized the increasing need for an instrument allowing individuals to retain more than a modicum of personal control over their data. In that sense, the right to be forgotten expanded on the existing right to erasure[56] in order to accommodate a changing digital environment in which personal data is generated, made public, and shared on a massive scale.

Article 17 of the GDPR, which provides the official codification of the right to be forgotten, states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay" if certain circumstances apply.[57] These circumstances, which are provided for in Article 17(1)(a-f) include that the personal data is no longer necessary for the purpose an organization originally collected or processed it; that an organization is relying on an individual's consent as the lawful basis for processing the data and the

---

[53] *Id.*

[54] *See* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 166 (2016) (quoting "Any company operating in the E.U. market or any online product that is targeted at E.U. consumers must comply with E.U. rules").

[55] *See* Adam Satariano, *'Right to Be Forgotten' Privacy Rule Is Limited by Europe's Top Court*, N.Y. TIMES, Sept. 24, 2019, https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html (stating "Europe's highest court limited the reach of the landmark online privacy law known as 'right to be forgotten' on Tuesday, restricting people's ability to control what information is available about them on the internet").

[56] *Communication from the Commission to the European Parliament and the Council: Stronger Protection, New Opportunities - Commission Guidance on the Direct Application of the General Data Protection Regulation*, at 2-3, COM (2018) 043 final (May 25, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0043&from=en.

[57] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation), (GDPR) art. 17, 2016 O.J. (L 119) 1, 43.

individual withdraws his consent; or that there is no overriding legitimate interest for the organization to continue with the processing.[58] To this last point, Article 17(1)(c) allows for the right to erasure following any successful invocation of the right to object in Article 21 of the GDPR.[59] That is, in any case in which a subject objects to processing under Article 21, and the controller cannot demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject," the subject is eligible not only for a cessation of processing by the particular processor in question, but also for all of the rights and privileges established in Article 17.[60]

As this last point demonstrates, Article 17 flips the burden of proof such that the data controller, rather than the data subject, must show why its interest in processing the data supersedes the data subject's interest in preventing further processing. "Compelling legitimate grounds for processing" are to be determined by the processor based on Article 6 of the GDPR, which provides the circumstances in which processing is necessary to accomplish some pertinent interest or obligation.[61] If the controller fails to establish the existence of such compelling circumstances, the controller must erase the data in question. Importantly, Article 17 can be invoked against any controller who processes personal data provided that one of the above circumstances applies.[62]

Article 17(3) constrains the right to be forgotten, providing that an organization's right to process an individual's data might trump an individual's right to be forgotten if, for example, the data is being used to exercise the right of freedom of expression, or the data represents important information that serves the public interest.[63] The scope of this exception depends on member state law pursuant to Article 85 of the GDPR, which requires member states to reconcile the protection of personal data with freedom of expression and information.[64] Though freedom of expression is a fundamental right in European Law, the decision of the drafters of the GDPR to defer to member states in considering the balance between privacy and free expression indicates an understanding that

---

[58] *Id.* at 43–44.
[59] *Id.* at 44.
[60] *Id.* at 45.
[61] *Id.* at 36.
[62] *Id.* at 43–44.
[63] *Id.* at 44.
[64] *Id.* at 83–84.

there are vastly different approaches to journalism among member states within the EU.

D. Varying Interpretations of the Balancing Test

In their duty under Article 85 to provide for exemptions to reconcile the protection of personal data with the freedom of expression, the various member states have taken significantly individualized approaches as it pertains to Article 17. A 2019 ruling in Germany, for example, enabled a man convicted of murder in 1982 to have links to news articles reporting on his crime delisted from Google's search results.[65] The court did not allow for the deletion of any of the material from the news organization's archive, however. The man argued that links to the newspaper's internet archive constituted a violation of his privacy rights and his "ability to develop his personality." Germany's Constitutional Court agreed, explaining that delisting the results was wholly in line with its duty to protect the constitutional rights of German citizens. As the man's attorney explained to a German newspaper after the successful ruling, "Even with spectacular cases and serious crimes like murder, perpetrators have a right to be forgotten and a new chance in society . . . . It's only by making it possible for past records to recede that individuals have a chance to start anew in freedom."[66] The ruling was heralded by press freedom and privacy advocates alike because it explicitly refused to fundamentally sacrifice press freedom in favor of personal rights, while protecting a German individual's ability to obtain a fresh start.

In Italy meanwhile, courts have on several occasions ordered the complete deletion of news stories from their host sites. One particularly notable example involved the publication of a story in 2008 about two brothers who got into a fight at a restaurant in Positano, which culminated in one stabbing the other.[67] One of the brothers sued the publication citing the right to be forgotten and arguing that his privacy had been violated by the reporting. Any Google search of his name led to the

---

[65] 1 BvR 16/13 (Recht auf Vergessen I) Federal Constitutional Court (Nov. 6, 2019) (available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106_1bvr001613.html).

[66] Ben Knight, *Germany's Top Court Upholds Murderer's Right to be Forgotten*, DW, (Nov. 27, 2019), https://www.dw.com/en/germanys-top-court-upholds-murderers-right-to-be-forgotten/a-51436980.

[67] Adam Satariano and Emma Bubola, *One Brother Stabbed the Other. The Journalist Who Wrote About it Paid a Price*, N.Y. TIMES (Sep. 23, 2019), https://www.nytimes.com/2019/09/23/technology/right-to-be-forgotten-law-europe.html.

article, which reported the details of a humiliating family argument, which the man desperately wanted to forget. In 2018, the Italian Supreme Court ruled that the publication had to delete the story of the stabbing, explaining that it was dated and no longer of public interest.[68] Many journalists on the continent were surprised by the court's suggestion that news stories should have an expiration date "just like milk, yoghurt or a pint of ice-cream" after a period of two years and publishers who kept stories around longer should be fined.[69] This ruling is also a significant departure from the application of the right found in *Google Spain* in that the court chose to blame the source of the information rather than the intermediary providing that information.[70]

The difference between these recent decisions in Germany and Italy underscores the significant differences among various member states in interpreting Article 17. As both cases show, however, when claims of reputational damage and privacy infringement are advanced under the auspices of the right to be forgotten, courts will be sympathetic to an individual's desire to rebuild his life free from easily available, stigmatizing information about his past. Where the existence of dated information strongly hinders an individual's attempts to reinvent himself in the wake of a shameful event, courts are motivated to rule in favor of the data subject as a means of affirming the widely held conception that every person is deserving of a second chance. As will be discussed below, this sentiment is one that is echoed quite strongly in the American legal tradition as well.

II. America's Rehabilitative Notion of Privacy

This section presents a cultural and legal overview of the profoundly American notion of second chances, fresh starts, and the ability to overcome the mistakes of one's past. It moves from a discussion of the cultural history of forgetting to a discussion of the legal history of protecting individuals' efforts at rehabilitation. Finally, it addresses some of the criticisms of the right to be forgotten from

---

[68] La Corte Suprema Di Cassazione [Cass.][Supreme Court of Cassation], Nov. 4, 2015, n. 13161.

[69] Athalie Matthews, *How Italian Courts Used the Right to be Forgotten to Put an Expiry Date on the News*, GUARDIAN (Sep. 20, 2016, 4:12 AM), https://www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news.

[70] *Id.*

American scholars. The goal of this section is to demonstrate that like the European right to be forgotten, which is premised on the idea that individuals should have control over their identity online, American jurisprudence is laced with discrete commitments to the sanctity of individuals' zones of privacy, which provide reason to restrict speech in certain circumstances.

A. Conceptual Grounding of the Right in the U.S.

Deeply embedded in American culture is the notion that on U.S. soil, individuals are entitled to a second chance. The country's immigrant history, pioneer spirit, and commitment to reform support the widespread idea that everyone is able to start anew regardless of what might have occurred in their past. As Alan Westin and Michael Baker noted in the 1970s, "[m]any citizens assume, out of a variety of religious, humanistic, and psychiatric orientations, that it is socially beneficial to encourage individuals to reform their lives, a process that is impeded when individuals know (or feel) that they will automatically be barred by their past 'mistakes' at each of the later 'gate-keeping' points of social and economic life."[71]

This conception of each individual's capacity for improvement has been facilitated by the fact that for much of modern history, the vast majority of individual actions were not recorded, and if they were recorded, the reach of such reports was curbed by the geographic limits of circulation as well as the attention span of gossips and the difficulty of accessing a newspaper's archives by the general public.[72] The fallibility of human memory allowed individuals to err and subsequently recover their reputations without significant effort. Free from the creeping omnipresence of their past, individuals were able to craft an ever-evolving self, change their beliefs, and pursue whatever goals they desired without being constrained by the views they once held, or the decisions they once made. Support of this principle did not come at the cost of accountability, it simply understood that long after a person had offended his community in some way, he should be allowed the opportunity to rebuild his life without fear of shame or derision from those who wished to dwell on his past. Because the past could be forgotten, it could be final.

Forgetfulness in that sense is a powerful social good in that it allows individuals to experiment and take risks without fear that every

---

[71] A.F. WESTIN & M.A. BAKER, DATABANKS IN A FREE SOCIETY 267 (1972).
[72] MAYER-SCHÖNBERGER, *supra* note 9, at 125.

act has permanence and will come back to haunt them years later. In environments where people believe they are constantly under surveillance, people begin to act more conservatively and spend more energy on conforming to social norms than they would otherwise.[73] Privacy provides an antidote to this problem of persistent and insurmountable data collection because it encourages forgetfulness. If data is not constantly available for access, it is harder to remember and assess years later. As Westin and Baker write, societies that choose "forgive and forget" over "preserve and evaluate" tend to be more democratic and more free, namely because the nature of the self that develops in a surveillance society is different.[74] Beginning one's life again as a means of escaping a difficult past is perfectly in line with the notions of autonomy advanced by much of American political and cultural lore.

B. Case Law Supporting an American Right to be Forgotten

Common law principles, premised on the conviction that each individual can improve himself, have long been the means through which Americans have established themselves as autonomous individuals, curtailed the longevity of public embarrassment, and shrouded their pasts from an unwanted audience.[75] In spite of the constitutional protections for the publication of truthful information, elements of a right to be forgotten have existed in U.S. case law for centuries. Several early holdings support that individuals have a right to privacy in embarrassing past information and that those who publish such information should be held accountable.[76] The right-to-be-forgotten-like language used by these courts suggests a long-standing compatibility between intentional forgetting and freedom of expression, particularly where a private individual's psychological well-being and ability to rehabilitate herself are in jeopardy. Surveying a number of these cases provides valuable insight into the ways in which the First Amendment and the right to be forgotten might be able to peacefully coexist online in the U.S. today.

To that end, in 1845, the U.S. Supreme Court decided a case involving a published letter to the editor in which a reader expressed criti-

---

[73] Jean-François Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 INFO. SOC'Y 33, 36 (2002).
[74] WESTIN & BAKER, *supra* note 70, at 268.
[75] *See infra* note 93–94.
[76] White v. Nicholls, 44 U.S. 266, 285 (1845); Morton v. State, 3 Tex. App. 510, 515 (1878); State v. Bienvenu, 36 La. Ann. 378, 383 (La. 1884); Melvin v. Reid, 297 P. 91, 91 (Cal. Dist. Ct. App. 1931).

cism of a retired public servant's past work.[77] The publisher of such a piece, the court wrote, would properly face liability because the article had impaired personal happiness and social order.[78] "[P]ublications that harm a man's 'sympathetic and social' nature could rightly be the subjects of litigation," the court held.[79] Anyone might "have had a cause of action against the publisher of truthful information as long as that information was 'calculated to make [an individual] infamous, odious, or ridiculous.'"[80] Tied up in the court's assessment was a pronounced appreciation for individual honor and legacy. If the subject of the piece was no longer serving in any official capacity, he should not be forced to endure the reputational damage the publication of such a letter would cause, even if the criticisms were warranted and the facts were true.[81] Ultimately, matters of the private domain should not be broadcast offensively for the world to see.

Thirty years later, a Texas court reiterated these ideas in the context of a local newspaper's publication of a letter to the editor explaining that a former alderman in the city of Galveston was dishonest while he was in office.[82] The court upheld the conviction of the publisher,[83] indicating that the former alderman was now a private individual, and his personal advancement should not be hindered by whatever wrongs he was alleged to have committed in his past. "A man may be allowed to keep poisons in his closet, but not publicly vend them about as cordials," the court explained.[84] Interfering with the man's privacy and continuing to harp on his wrongs long after they occurred offends the dignity of all concerned.[85]

In 1884, the Louisiana Supreme Court upheld the conviction of a publisher for distributing a pamphlet, which suggested that a priest had had numerous affairs with nuns, students, and others over the course of more than two decades.[86] "[T]hat would be a barbarous doctrine which would grant to the evil-disposed the liberty of ransacking the lives of

---

[77] White v. Nicholls, 44 U.S. 266, 285 (1845).
[78] Amy Gajda, *Privacy, Press, and the Right to Be Forgotten in the United States*, 93 WASH. L. REV. 201, 209 (2018) (referencing *White*, 44 U.S. 266).
[79] *Id.* at 209–10 (referencing *White*, 44 U.S. 266).
[80] *White*, 44 U.S. at 285.
[81] *Id.* at 290.
[82] Morton v. State, 3 Tex. App. 510, 515 (1878).
[83] *Id.* at 519.
[84] *Id.* at 516.
[85] *Id.*
[86] State v. Bienvenu, 36 La. Ann. 378, 383 (La. 1884).

others to drag forth and expose follies, faults or crimes long since forgotten and perhaps expiated by years of remorse and sincere reform," the court wrote.[87] "[T]ruth of the libel does not serve to rebut the presumption of malice flowing from its publication." Underlying the court's holding was a clear conclusion that the damage caused by dredging up unsavory facts about others' lives was not worth the public's interest in the information unearthed, even if that information was scandalous and entirely true. The publication of facts of private life long after they were relevant threatened the social order by undoing years of good citizenship after a brief dalliance with impropriety.

The culmination of this century of jurisprudence, teasing out the areas in which privacy interests might supersede freedom of expression, was a 1931 case, *Melvin v. Reid*, involving a documentary film about a woman who had been a prostitute decades earlier.[88] The film was shown in several states, causing many of Melvin's friends to learn of her past and scorn and abandon her, so Melvin sued to prevent further spread of the film and to collect damages for grievous mental and physical suffering.[89] The California Court of Appeals held that because the filmmaker had exposed her past transgressions long after she had changed her life to be "exemplary, virtuous, honorable, and righteous," he had invaded her privacy.[90] "She should have been permitted to continue [her life] without her reputation and social standing destroyed by the publication of the story of her former depravity with no other excuse than the expectation of private gain by the publishers," the court held.[91] Revealing her past "transgressions" was inappropriate in light of the years she had spent "rehabilitating" herself.

The *Melvin* court provided a definition of privacy with clear bearings on the right to be forgotten, providing, "[t]he right of privacy may be defined as the right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity. In short, it is the right to be let alone."[92] The court was particularly concerned with the way that facts about Melvin's past life might come back to haunt her and impact her ability to "pursue and obtain happiness."[93] In a progressive stance,

---

[87] *Id.* at 382.
[88] Melvin v. Reid, 297 P. 91, 91 (Cal. Dist. Ct. App. 1931).
[89] *Id.*
[90] *Id.* at 91, 93.
[91] *Id.* at 93.
[92] *Id.* at 92 (quoting 21 R.C.L. 1197, 1198).
[93] *Id.* at 93.

echoing their European counterparts, the California court explained, "whether we call this a right of privacy or give it any other name is immaterial, because it is a right guaranteed by our Constitution that must not be ruthlessly and needlessly invaded by others."[94]

This last line emphasizes the conceptual framework from which a right to be forgotten might be organized in the U.S. A right to privacy, or a right to avoid "ruthless and needless invasion by others," seems to reflect our moral intuitions. Where an individual has experienced hardship or committed some offense, these instances are not definitive of his entire life absent the continuous harping of publications critical of his past. "One of the major objectives of society as it is now constituted . . . is the rehabilitation of the fallen and the reformation of the criminal," the *Melvin* court wrote.[95] Journalistic pieces that retrieve the unsavory details of a person's life to make them publicly known prevent such rehabilitation and reformation by serving as false talismans for an individual's entire body of lived experience.

A 1971 case of a similar ilk, *Briscoe v. Reader's Digest Ass'n, Inc.*, involved an article describing the 1956 armed hijacking of a truck by a man, Briscoe, who had since "abandoned his life of shame and became entirely rehabilitated," thereafter living "an exemplary, virtuous and honorable life."[96] As a result of the publication, Briscoe's 11-year-old daughter, as well as his friends, learned of his criminal past for the first time and afterwards rejected him.[97] As the court explained, the plaintiff's claim "is not so much one of total secrecy as it is of the right to define one's circle of intimacy—to choose who shall see beneath the quotidian mask."[98] Without the ability to control his reputation and determine the audience for his transgressions, Briscoe likely felt alienated and without agency. As the court wrote, "Loss of control over which 'face' one puts on may result in literal loss of self-identity, and is humiliating beneath the gaze of those whose curiosity treats a human being as an object."[99]

The court determined that while Reader's Digest undoubtedly had the right to report the facts of the past crime, the identification of the

---

[94] *Id.* at 93–94.
[95] *Id.* at 93.
[96] Briscoe v. Reader's Digest Ass'n, Inc., 483 P.2d 34, 36 (Cal. 1971), *overruled by* Gates v. Discovery Commc'ns, Inc., 101 P.3d 552 (2004).
[97] *Id.*
[98] *Id.* at 37.
[99] *Id.* (internal citations omitted).

plaintiff served "little independent public purpose" other than curiosity.[100] Newsworthiness, the court explained, was to be determined by assessing the social value of the facts published, the extent to which the party voluntarily acceded to a position of public notoriety, and the depth of the article's intrusion into private affairs, such that the more intimate the facts the less the public should know.[101] Disclosing such private matters was counter to the rehabilitative interests of the state, namely that "the rehabilitated offender can rejoin that great bulk of the community from which he has been ostracized for his anti-social acts. In return for becoming a 'new man,' he is allowed to melt into the shadows of obscurity."[102]

In *Briscoe*, the emphasis on the plaintiff's having distanced himself from the original offense indicates a clear acknowledgement of the idea that individual character is fundamentally mutable and revisable. It also correctly assumes that people treat those with criminal records differently, particularly those charged with violent felonies. The shaming and stigmatizing mechanisms of the criminal justice system undoubtedly play into our relations with others, even after people have shown themselves to be rehabilitated for several years. Ultimately, where most people do not know the information that the plaintiff seeks to hide, and where the plaintiff has developed an expectation of privacy, the dissemination of long-hidden information by would-be truth-tellers causes shame and unwanted attention for which publications can be held liable.

Importantly, these cases represent something different from the tort of disclosure. The tort of disclosure has three elements: first, the disclosure must be public; second, the facts involved must be of a private, confidential nature; and third, the subject matter of the disclosure must be one that a reasonable person of ordinary sensibilities would find offensive and objectionable.[103] Disclosure, conceptualized as such, harkens back to the 1890 law review article by Samuel Warren and Louis Brandeis titled, "The Right to Privacy."[104] Here, the two men sounded the alarm about the damage caused when "what is whispered in the closet [is] proclaimed from the house-tops,"[105] after a Boston gossip rag published a series of exposés, which broadcast secrets disclosed at one of

---

[100] *Id.* at 40.
[101] *Id.* at 43.
[102] *Id.* at 41.
[103] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).
[104] *Id.* at 193.
[105] *Id.* at 195.

Warren's gilded dinner parties.[106] "To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle," Warren and Brandeis wrote.[107] Disclosure, conceptualized as such, is premised on the protection of private, confidential information from being spread to the public.

Melvin and *Briscoe* are of an entirely different character in that they are concerned with publications revisiting facts that have long been public but have also long been forgotten. The documentarian making the film on Melvin's life drew inspiration from a series of articles that had been written about Melvin after she was accused of murder and ultimately acquitted, twenty years earlier.[108] Since then, she had changed her name, moved, and accepted a new job, such that no one in her immediate circle knew of her earlier life. The same is true of Briscoe, whose violent hijacking the press covered when it occurred but were not discussed at all in the decades that followed between the incident and the decision by Reader's Digest to publish a new story on Briscoe's crime.[109] For the publications in both cases, their offensive action was re-attracting attention to the sordid affairs of individuals who had since been rehabilitated, *not* exposing individuals' previously-concealed or publicly-unknown secrets. As a result this unique privacy tort could likely form the conceptual basis of an American right to be forgotten.

C. Statutes Approximating the Right

The same privacy ideals underlying the European right to be forgotten are present in myriad legislative materials throughout the U.S. The most protective of such acts tend to concern minors who have been involved in the criminal justice system. Several states possess statutes that order the sealing or allow for the expungement of juvenile criminal records when the individual turns eighteen.[110] Meanwhile, Minnesota[111] and North Dakota[112] mandate the destruction of photos and fingerprints

---

[106] LETA JONES, *supra* note 47, at 62; *see* Danielle Keats Citron, *The Roots of Sexual Privacy: Warren and Brandeis & the Privacy of Intimate Life*, 42 COLUM. J.L. & ARTS 383, 385 (2019).
[107] Warren & Brandeis, *supra* note 102, at 196.
[108] Melvin v. Reid, 297 P. 91, 91 (Cal. Dist. Ct. App. 1931).
[109] *Briscoe v. Reader's Digest Ass'n*, Inc., 483 P.2d 34, 35 (Cal. 1971) *overruled by* Gates v. Discovery Commc'ns, Inc., 101 P.3d 552 (2004).
[110] *See, e.g.* MONT. CODE ANN. § 41-5-216(1) (2019); N.C. GEN. STAT. § 7B-2901 (2020); TENN. CODE. ANN. § 10-7-504 (2020).
[111] MINN. STAT. § 626.556 Subd. 11c (2019).
[112] N.D. CENT. CODE § 27-20-53(4)(2019).

associated with juvenile criminal records. The language of this latter statute provides, "Upon the final destruction of a file or record, the proceeding must be treated as if it never occurred . . . . Upon inquiry in any matter the child, the court, and representatives of agencies . . . shall properly reply that no record exists with respect to the child."[113] A legislatively-mandated process of forgetting enables young people to obtain a second chance, legitimizing widely-held intuitions that a person's entire life should not be marred by a youthful mistake.

Similarly, in January 2015, California implemented its "Eraser Law," which provides California minors with a narrowly-defined approximation of the right to be forgotten.[114] The Eraser Law allows these young people to remove or request and obtain removal of content or information they posted on an operator's website, application, or online service, provided that the minor is a registered user of the resource.[115] The statute was motivated by concern that digital natives would be uniquely harmed as they endeavor to pursue higher education or employment opportunities because of the sheer volume of content available about them on the internet. State Senator Darrell Steinberg, who introduced the bill argued, "Children should be allowed to erase that which they post because mistakes can follow a young person for a long time and impact their chances of getting into college and landing a job . . . . This bill would ensure the continued ability to delete information that a minor realizes could be harmful to his or her future endeavors."[116] Of course, the Eraser Law does not provide the same protections afforded by the European right to be forgotten, in that the deletion requests only pertain to content the subject posted himself; however, it still extends beyond any other U.S. digital-privacy law to formally acknowledge that an individual's personal development might be hindered by the resurgence of embarrassing online materials years after they were posted.

Finally, in 2017, New York State Assemblyman David Weprin introduced a bill that essentially mimicked the right to be forgotten, requiring "search engines, indexers, publishers and any other persons or entities which make available, on or through the internet or other widely used computer-based network, program or service, information about an

---

[113] *Id.* § 27-20-54(2).
[114] S.B. 568, 2013 Leg., 2013–14 Sess. (Cal. 2013), available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.
[115] *Id.* § 22581.
[116] *Remarks on SB 568 Privacy: Internet: Minors, Hearing Before the Sen. Judiciary Comm.*, 113th Cong. 7 (Apr. 23, 2013) (statement of Senator Darrell Steinberg).

individual to remove such information, upon the request of the individual, within thirty days of such request."[117] Assemblyman Weprin was inspired by one of his constituents who had sued Google, Yahoo, and Bing to no avail, requesting that the sites "remove [the plaintiff's] full name from their search engines" after the plaintiff's ex-boyfriend had posted a series of sexually explicit videos of her on various pornography sites.[118] The uniqueness of the woman's four-word, West-African name made it virtually impossible for any potential searcher to avoid encountering the videos when searching her name.[119] According to the complaint, the woman could not obtain employment as a result of the video and sought relief as such.[120] Weprin, who was moved by the woman's experience, introduced a somewhat-hasty approximation of delisting rights, which, as of this writing, has yet to be voted on in the state senate.

On the federal level, the U.S. government has instituted myriad legislation attempting to protect records of personal financial difficulties from resurgence later in a person's life. The stated aim of the 1971 Fair Credit Reporting Act, for example, was to protect individuals from the potentially-damaging effects of the modernizing data collection and aggregation policies of credit bureaus.[121] The act prohibited the reporting of "any other adverse item of information" that occurred more than seven years before the publication of the report,[122] substantially limiting the memories of credit bureaus and intentionally obscuring information such bureaus would undoubtedly like to possess. In effect, a credit agency might be forced to forget about the historical fact of a bankruptcy to the benefit of an individual who has turned around his formerly financially-troubled life. The FCRA, as well as statutes involving juvenile crime records and the limited ability to request data erasure, speak to a larger philosophy of individual rehabilitation that allows people to unburden

---

[117] Assemb. B. A05323, 202nd N.Y. Assemb., Reg. Sess. (N.Y. 2017).
[118] Julia Marsh, *Revenge Porn Victim to Google: Make Me Disappear*, N.Y. POST (Jan. 3, 2017, 6:48 PM), https://nypost.com/2017/01/03/revenge-porn-victim-wants-her-name-deleted-from-google/.
[119] Julia Marsh, *Revenge Porn Victim Wants US to Adopt "Right to be Forgotten" Law*, N.Y. POST (Jan. 4, 2017, 7:34 PM), https://nypost.com/2017/01/04/revenge-porn-victim-wants-us-to-adopt-right-to-be-forgotten-law/.
[120] Verified Complaint for Declaratory Judgment and Injunction Relief, Angele Brilihon Bolou Abodo v. Google, Yahoo, & Bing, (N.Y. Jan. 2, 2017), Index No. 150005/2017 (available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2376&context=historical).
[121] 15 U.S.C. § 1681 (1970).
[122] *Id.* § 605(a)(5).

themselves from their pasts and start their lives anew. Such legislation constitutes a government-mandated program of social forgetfulness that mirrors the conceptual justifications of the right to be forgotten in Europe.

D. Responding to First Amendment Criticisms

Criticism of the right to be forgotten in the U.S. has been based largely on the idea that the right is fundamentally in conflict with the First Amendment. Those against the adoption of the right on American soil tend to posit a somewhat draconian understanding of First Amendment jurisprudence, wherein privacy is categorically sacrificed at the altar of free expression. One example is a 2011 blog post written by Google's Chief Privacy Counsel, Peter Fleischer, which suggests that the right to be forgotten might be a clever form of censorship. "More and more, privacy is being used to justify censorship," Fleischer writes.[123] "And in a world where ever more content is coming online, and where ever more content is findable and shareable, it's also natural that the privacy counter-movement is gathering strength. Privacy is the new black in censorship fashions."[124] Ultimately, Fleischer argued that no law can or should provide a right to remove all references to an individual from the internet.

Responding to Fleischer's post, Professor Jefferey Rosen wrote that the right represents "the biggest threat to free speech on the Internet in the coming decade" because removal of someone else's content is outright unconstitutional.[125] Professor Dawinder Sidhu responded similarly stating, "In American society . . . we allow the relative significance of a piece of information to be debated in the marketplace of ideas, not removed from public consideration altogether. . .."[126] Professor Eugene Volokh, probably the harshest critic of the right to be forgotten, added that free speech considerations always outweigh privacy considerations in the U.S. because "a good deal of speech that reveals information about people, including speech that some describe as being of merely 'private

---

[123] Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY. . .?, (Mar. 9, 2011), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

[124] *Id.*

[125] Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. 3, 88 (2012).

[126] Dawinder Sidhu, *We Don't Need a "Right to be Forgotten." We Need a Right to Evolve,* NEW REPUBLIC (Nov. 7, 2014), https://newrepublic.com/article/120181/america-shouldnt-even-need-right-be-forgotten.

concern,' is actually of eminently legitimate interest . . . . to people deciding how to behave in their daily lives, whether daily business or daily personal lives."[127] The underlying theme of these arguments is that when privacy comes into conflict with the First Amendment, privacy loses, thereby pre-empting the adoption of any sort privacy-based speech limitation.

Critics of the right to be forgotten typically cite two cases—*Cox Broadcasting v. Cohn* and *Florida Star v. B.J.F.*—as vanquishing any possibility of the right to be forgotten in the U.S. because they allegedly stand for the proposition that under the First Amendment, states cannot pass laws restricting the media from disseminating truthful but embarrassing information. Neither of these cases, however, explicitly prevent a right to be forgotten.

In *Cox Broadcasting,* where a television station reported the name of a rape victim who had been murdered, despite a Georgia statute at the time that made the identification of a rape victim a misdemeanor, the court held that "the First and Fourteenth Amendments will not allow exposing the press to liability for truthfully publishing information released to the public in official court records."[128] In that sense, the *Cox Broadcasting* holding is actually quite narrow, limited by whether the information was (1) recently released to the public and (2) released through official public records.[129] Thus, the case would not apply where these two features of information dissemination were not present.

Cox Broadcasting also seems to support strong protections for privacy given the court's articulation of a "zone of privacy surrounding every individual, a zone within which the state may protect him from intrusion by the press, with all its attendant publicity."[130] Surely, then, for particularly sensitive areas of private life that might fall into this zone of privacy, a state might be able to enforce a right to be forgotten that passes First Amendment muster. Finally, the justices explicitly reject Volokh's contention that free speech concerns always trump privacy concerns, stating, "In this sphere of collision between claims of privacy and those of the free press, the interests on both sides are plainly rooted in the

---

[127] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1115 (2000).
[128] Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496 (1975).
[129] *Id.* at 471.
[130] *Id.* at 487.

traditions and concerns of our society."[131] *Cox Broadcasting* clearly recognizes that media liability can be appropriate in those circumstances when the press discloses certain private facts.

In *Florida Star*, decided a decade later, a rape victim sued a newspaper after the newspaper published her name, and again the court refused to hold the media liable because the government itself had already released the victim's name to the media.[132] Again, the court deliberately limited its holding with privacy considerations in mind, explaining, "We do not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the state may protect the individual from intrusion by the press, or even that a state may never punish publication of the name of a victim of a sexual offense."[133] The *Florida Star* holding seems to leave room for liability for the press in similar instances, including where the publication of certain information might otherwise be constitutional. As Professor Daniel Solove has written, "*Florida Star* can be construed to suggest that a law adopting a less categorical approach—by addressing the use of identifying data more contextually—might not be subject to strict scrutiny under the First Amendment."[134] That is, instead of looking at the content of the information in question, the court could examine whether the information touches upon a protected zone of privacy such that any information revealed about this particular area would be protected.

As these archetypally pro-media rulings show, there is significant flexibility within the justices' opinions such that a right to be forgotten might still be freely advanced. In both cases, the court specifically refused to grant the publication's request for protections for *all* truthful information and declined to expressly suggest that publishers *always* have the right to reveal true information about a person's past. In fact, in *Cox Broadcasting*, the court referenced a statement by the *Briscoe* court that "the rights guaranteed by the First Amendment do not require total abrogation of the right to privacy."[135]

Because both cases narrow their holdings to protect only publicly available information, it is entirely conceivable that a right to be forgotten might exist for older non-public records. For example, if a newspaper

---

[131] *Id.* at 491.
[132] Fla. Star v. B. J. F., 491 U.S. 524, 528, (1989).
[133] *Id.* at 541.
[134] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure,* 53 DUKE. L. J. 967, 1022–23 (2003).
[135] *Cox Broad.*, 420 U.S. at 475.

published an article that contained information about an adult's juvenile criminal record, and that record had since been expunged, the individual might have a right-to-be-forgotten-like privacy right regarding that information since it was no longer publicly available. Similarly, since neither case discusses whether a person might have such a right to protect information that has never appeared in any government record at all, a right to be forgotten might also exist in sensitive information about a person's past unearthed to the press via any non-official means. Ultimately, Supreme Court jurisprudence does not serve as a hard ban on any sort of right like the right to be forgotten, but rather limits the liability of publications in cases where information about the matter in question was already publicly available.

III. Operationalizing a Right to be Forgotten in the U.S.

This section outlines the means through which a right to be forgotten might be institutionalized in the U.S. It argues that journalistic entities, broadly defined, should be compelled to utilize expiration and anonymization in order to respond to compelling requests for the removal of articles. It provides examples of news organizations that are already participating in these activities, and it concludes with a discussion of how government-mandated anonymization and expiration might be able to survive a First Amendment challenge if there were a compelling governmental interest in each individual's right to self-actualization, rehabilitation, and ability to have a second chance.

A. Anonymization and Expiration

As is established in the myriad cases and statutes cited above, a right-to-be-forgotten-like privacy right carries enormous social benefits. This is especially true in the information age as digital memory seems poised to alter social memory in significant ways. Because more of our activities are taking place online—from shopping to communicating to mapping directions—individuals are more easily reduced to a vast quantity of data points than ever before. Once these data are collected, it is easily aggregated and correlated with other kinds of data, which can be utilized to provide a clearer understanding of each individual user than any individual data point can alone. Such data has an alarming degree of predictive power in that when it is combined in the right way, it leads to the possibility of discovering new information about the data subject in question. More than ever before, a legislatively-enforced program of so-

cial forgetfulness is needed to combat the creeping ability to be wholly knowable based off of a few fragments of online information.

Were such a program to be introduced it would likely hinge on two strategies of obscuring information—expiration and anonymization—both of which should be carried out by news organizations themselves. Arguably the foremost means of instituting a policy of widespread forgetting is establishing expiration dates for links to articles. As Mayer-Schönberger has suggested, "meta-information tags" might allow webpage authors to define how long search engines keep the link to a particular web page in their index.[136] This, of course, speaks to the relevance of the information in question—a quality that is important both for news sites as well as for the subjects of news articles. As the newsworthiness of the information declines over time, media organizations will have progressively less interest in protecting the information. For example, it is highly unlikely that a decades-old piece on a local crime would be visited by many users, and the ad revenue from the piece would likely be negligible. At the same time, the longer the piece is online, the more likely it is that the subject of the piece would want it removed, particularly if he is applying to college, trying to get a job, using a dating app, or undertaking any of the other myriad activities that might inspire others to google his name. Surely there must be a point at the intersection of the declining profitability and journalistic value of the article for the news organization, and the increasing nuisance of the article for the data subject in question, at which the expiration of the link to the article could be agreed upon. The French Data Protection Authority, the CNIL, for example, has specified the maximum duration for which data may be kept, taking into account the purposes of the collection and the public interest served by its retention.[137] It seems conceivable that a similar legislative move could be made in the U.S.

Several local newspapers' editorial boards already participate in their own versions of forced expiry. The Tampa Bay Times, for example, formed a committee of four editors in 2016 to adjudicate requests for the

---

[136] MAYER-SCHÖNBERGER, *supra* note 9, at 179–180.

[137] *Sheet n°14: Define a Data Retention Period*, COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (June 11, 2020), https://www.cnil.fr/en/sheet-ndeg14-define-data-retention-period#:~:text=the%20data%20relating%20to%20payroll,be%20kept%20for%205%20years.

removal or alteration of stories in their archive.[138] While the paper's editors admitted they never would have entertained such a request in a pre-internet era, they knew that in an age where an obscure story from decades ago might appear on the first page of results after a search of someone's name, retention is not always the best policy. In one of the committee's first meetings, the editors granted a request to delete a story from years earlier in which a woman had been identified as having worked with a "naked maids" cleaning service when she was 19 years old.[139] The woman was now older, farther removed from the story, and felt the story was embarrassing and unfairly defined her life. In deleting the post, the newspaper likely weighed the balance between the journalistic and financial value of the piece and the individual shame and hardship caused by its mentioning that particular individual and voted that the latter was far more serious.[140] Though journalists no doubt stand by the importance of their craft, they recognize when the hardships faced by certain subjects outweigh the value of their work and they have no qualms limiting access to their work online. As the Society for Professional Journalists Code of Ethics provides, "Balance the public's need for information against potential harm or discomfort. Pursuit of the news is not a license for arrogance . . . ."[141] These harm-minimization principles seem to indicate quite clearly that it is only when the balance weighs in favor of publication over individual privacy that journalism ethics would support the story.

The second strategy of obscuring information that might support a right to be forgotten is the anonymization of news stories. Here, editors of online publications might be compelled to anonymize the subject of dated news stories if the subject is a private individual, the incident in question is not particularly grave, and the subject's identification contributes nothing journalistically to the piece. If public and institutional memory is skewed towards preservation and evaluation, as opposed to deletion and forgetting, altering online data beyond immediate recogniz-

---

[138] Terry Carter, *Erasing the News: Should Some Stories Be Forgotten?* A.B.A. J. (Jan. 1, 2017, 12:10 AM), http://www.abajournal.com/magazine/article/right_to_be_forgotten_US_law.

[139] *Id.*

[140] *See id.* (stating "the paper's managing editor, Jennifer Orsi, thought it wasn't fair for that instance in her life to define her now").

[141] *Code of Ethics*, SOC'Y PROF. JOURNALISTS (Sep. 6, 2014), https://www.spj.org/pdf/spj-code-of-ethics.pdf [https://web.archive.org/web/20201010022256/https://www.spj.org/pdf/spj-code-of-ethics.pdf].

ability may prove more feasible than outright removal. Newspapers could perhaps issue a note, in the form of current corrections notices, explaining that the article had been altered as a result of a right to be forgotten request, thereby maintaining full transparency for readers. Anonymizing articles allows for a replication of the unidentified, innominate world of the pre-internet era in which private individuals were able to make mistakes and subsequently rebuild their lives free from scrutiny. In this earlier time, Americans had far less control over what they knew of others and far more control over how they allowed themselves to be known because they were sheltered by their compatriots' inability to use technology to peer into their private life whenever they wanted.[142] The crux of anonymization in this sense is simply the de-identification of shameful or embarrassing acts or speech from the individuals who produced them such that the story remains the same, but the actor is unrecognizable by others.

Several papers in the U.S. already utilize anonymization policies to accommodate the privacy demands of subjects of their reporting. Cleveland.com, the paper of record for northeast Ohio, instituted such a policy in 2019, enabling those whose names have been mentioned in past articles to request that their names be removed from old stories.[143] As the editor of cleveland.com, Chris Quinn wrote when he announced the policy, "Not a week goes by anymore, it seems, that several of us in the newsroom don't hear from people who are blocked from improving their lives by the prominence of cleveland.com stories about their mistakes in Google searches of their names. They don't get jobs, or their children find the content, or new friends see it and make judgments."[144] Cleveland.com does not alter articles about elected officials, celebrities, or other persons, nor does it obscure information related to violent or sex crimes, but it does allow individuals who have committed misdemeanors to disassociate themselves with the transgressions of their past. As the newspaper recognized, the news value of local crime stories is rarely in the name of the perpetrator involved, but rather, the details of the incident itself.[145] For example, removing the name of a drunken teenager who drove into a storefront from a story about underaged drinking being on

---

[142] SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 33 (2018)
[143] Chris Quinn, *Right to be Forgotten*, CLEVELAND.COM (Jun. 12, 2019), https://www.cleveland.com/opinion/2018/07/right_to_be_forgotten_clevelan.html.
[144] *Id.*
[145] *Id.*

the rise makes no difference in accomplishing the goals of journalism, namely seeking truth and reporting it. But if the teenager's name is included, it may cause enormous personal embarrassment and hardship for him for decades to come. Such a use of personal information seems wholly counteractive to the Society of Professional Journalists' mandate to minimize harm and "avoid pandering to lurid curiosity."[146]

Both expiration and anonymization would require a significant balancing test to evaluate the newsworthiness of the piece versus the privacy rights of the person implicated. The criteria used should follow from the recommendations of Working Party 29 as well as the best practices of the newspapers mentioned above, which are already involved in their own form of balancing test to remove certain dated articles. Factors that should be considered in this balancing test include the length of time between the offense and the request for removal, the public notoriety of the subject, the sensitivity of the material in question, the age of the subject at the time of the article's publication, and the extent to which the identification of the subject contributes to the newsworthiness of the piece. Underlying all of these inquiries should be the question posed by the cleveland.com editor in his initial defense of the paper's right-to-be-forgotten-esque program: how long should someone have to pay for a mistake?[147] Do we want to face a future that is forever unforgiving because we are unable to forget our past?

These are complex questions, but there is every indication that news organizations are able to think carefully and thoughtfully about them. More so than a search engine, whose conception of newsworthiness is based on the number of page visits and search algorithm rather than journalistic standards,[148] or an independent body charged with handling requests from individuals for all publications, news organizations are best equipped to evaluate when an article is no longer of service to their own particular aims—journalistic, financial, or otherwise.[149] This is

---

[146] SOC'Y PROF. JOURNALISTS, *supra* note 140.
[147] Quinn, *supra* note 142.
[148] Danny Sullivan, *Under the Hood: Google News & Ranking Stories,* SEARCH ENGINE LAND (Nov. 24, 2009, 9:00 AM), https://searchengineland.com/google-news-ranking-stories-30424 [https://web.archive.org/web/20201010044347/https://searchengineland.com/google-news-ranking-stories-30424].
[149] *What is Newsworthy?* (Dec. 22, 2019) https://www.pbs.org/newshour/extra/app/uploads/2013/11/What-is-Newsworthy-Worksheet.pdf [https://web.archive.org/web/20200115183518/https://www.pbs.org/newshour/extra/app/uploads/2013/11/What-is-Newsworthy-Worksheet.pdf].

because editors and publishers know their standards of reporting, understand their audience, and use data analytics platforms, which provide them with detailed information about user engagement on a particular article.[150] As the producers of the content in question, they should be afforded the ultimate say on whether an article stays or goes. The right would thus be conceptualized as a means for journalists to take moral agency over their work and alter it when the information they have written and reported becomes inappropriately harmful.

To some extent, news organizations might take their cues from the justice system just as Cleveland.com has committed to doing.[151] In judicial bodies across the nation, officials make daily assessments as to whether individuals with troubled or embarrassing pasts have changed from who they once were. Parole boards, for example, determine whether an individual should be released from prison by looking at the length of time that has passed since the crime, evaluating the offender's accomplishments while incarcerated, and reviewing his prior criminal record.[152] Family court judges assess whether biological parents who have lost custody of their children have changed their ways enough to regain custody once again.[153] Judges in criminal cases can be inclined to mitigate a defendant's sentence if they are persuaded that the defendant is remorseful.[154] The Department of Justice often offers amnesty to corporations that voluntarily disclose their past wrongdoings and commit to bolstering their compliance department and changing company policies.[155]

---

[150] Elizabeth Hansen & Emily Goligoski, *Guide to Audience Revenue and Engagement* COLUM. JOURNALISM REV. (Feb. 8, 2018) (available at https://www.cjr.org/tow_center_reports/guide-to-audience-revenue-and-engagement.php).

[151] *See* Chris Quinn, *We Want to Expand Our Right to be Forgotten and This Time Its About Fairness and Equity* CLEVELAND.COM (Oct. 3, 2020) https://www.cleveland.com/news/2020/10/we-want-to-expand-our-right-to-be-forgotten-and-this-time-its-about-fairness-and-equity-letter-from-the-editor.html (explaining the newspaper's intention to work with the courts to determine cases where people have successfully had their criminal records sealed).

[152] U.S. Parole Comm'n, *What Happens at a Parole Hearing,* U.S. DEPT. OF JUSTICE (Dec. 23, 2019). (available at https://www.justice.gov/uspc/frequently-asked-questions#q2).

[153] Robert H. Mnookin, *Child Custody Adjudication: Judicial Functions in the Face of Indeterminacy,* 39 L. & CONTEMP. PROBLEMS 226, 280 (Summer 1975).

[154] Rocksheng Zhong, *So You're Sorry? The Role of Remorse in Criminal Law,* YALE MED. THESIS DIGITAL LIB. 1 (Jan. 2013) (available at https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=1852&context=ymtdl).

[155] DOJ Manual 9-28.900 – Voluntary Disclosures.

Ultimately, the legal system is already well-disposed to determine whether an individual has changed his ways enough such that the current version of himself is meaningfully different than the person he was before. Surely news organizations could adopt some of these standards as they devise guidelines determining whether information published about a person's past was irrelevant or excessive. Formally acknowledging that people have changed is, as Leta Jones writes, demonstrative of "a larger cultural willingness to allow individuals to move beyond their personal pasts, a societal capacity to offer forgiveness, provide second chances, and recognize the value of reinvention."[156] The value of such forgiveness is enormous in a world in which individuals can no longer rely on the fallibility of memory to support their efforts at self-reflection and reinvention.

B. Overcoming First Amendment Challenges

Both expiration and anonymization would likely be in tension with the First Amendment insofar as they constitute a government-imposed restriction on speech;[157] however, such tension might be mitigated if it is determined that there is a compelling government interest in allowing individuals the freedom to evolve and to have second chances.[158] As shown through credit reporting regulations and juvenile crime record laws, both state and federal legislatures seem genuinely invested in the idea that in some circumstances, an individual's past follies should not burden his future goals. If juvenile criminal records can be hidden from employers' background checks, and bankruptcy filings can be hidden from credit reporting agencies, why should reports of such events be allowed to remain in online news archives? The retention of such a record only serves to undermine the goal of these statutes explicitly aimed at ensuring public and institutional forgetfulness. If society has decided to give an individual a second chance, the internet should do the same by "forgetting" information that is no longer relevant to who that person is today.

---

[156] LETA JONES, *supra* note 53, at 11.

[157] *See generally* Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny,* 144 U. PA. L. REV. 2417 (1996) (discussing when First Amendment values are transcended by other governmental interests).

[158] *See supra* Part II (explaining that there is a long history of case law and legislation in the U.S. endorsing an apparent government interest in allowing individuals the freedom to have a second chance).

Most restrictions on speech are reviewed starting with an assessment of whether the restriction in question is content-based or content-neutral.[159] The difference between content-based and content-neutral speech restrictions has been defined by the Court as the difference between restrictions which discriminate based on viewpoint and restrictions which discriminate based on factors external to semantic content such as the time, place, and manner of speech.[160] While content-based restrictions on speech receive strict scrutiny—a more rigorous and speech-protective test of constitutionality—content-neutral restrictions do not.[161] Thus, a speech regulation such as the right to be forgotten has a much greater chance of passing constitutional muster if it is deemed to be content-neutral.[162]

---

[159] *See* Volokh *supra* note 151 at 2419.

[160] *See*, *e.g.,* Police Dept. of Chi. V. Mosley 408 U.S. 92, 101 (1972) (A Chicago ordinance prohibiting picketing within 150 feet of a school, except for labor picketing, was deemed unconstitutional. Writing for the Court, Justice Thurgood Marshall explained that the ordinance "describes impermissible picketing not in terms of time, place, and manner, but in terms of subject matter. The regulation thus slips from the neutrality of time, place, and circumstance into a concern about content. This is never permitted."); Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989) (A New York City ordinance mandating the use of city-provided sound systems for concerts in Central Park was upheld, giving broad deference to the City's interest in "maintaining order." As long as "the means chosen are not substantially broader than necessary to achieve the government's interest," a regulation will not be invalidated because a court concludes that the government's interest "could be adequately served by some less-speech-restrictive alternative."). R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) ("Content-based regulations are presumptively invalid."); Carey v. Brown, 447 U.S. 455, 462 n.6 (1980) ("It is, of course, no answer to assert that the Illinois statute does not discriminate on the basis of the speaker's viewpoint, but only on the basis of the subject matter of his message. The First Amendment's hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic.").

[161] *See* Volokh *supra* note 151 at 2421 n.29; David L. Hudson Jr., *Content Neutral*, FIRST AMEND. ENCYC., https://www.mtsu.edu/first-amendment/article/937/content-neutral (last visited Jan. 10, 2021); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642 (1994) ("Regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny."); United States v. Alvarez, 132 S. Ct. 2537, 2548 (2012) (referring to the scrutiny applied to content-based speech regulations as "the most exacting scrutiny"). *See*, *e.g.*, Brown v. Entm't Merchs. Ass'n., 131 S. Ct. 2729, 2738 (2011); United States v. Playboy Entm't Grp., 529 U.S. 803, 813 (2000); Sable Commc'ns of Cal., Inc. v. FCC 492 U.S. 115, 126 (1989).

[162] Leslie Gielow Jacobs, *Clarifying the Content-Based / Content Neutral and Content / Viewpoint Determinations* 34 MCGEORGE L. REV. 595, 596 (2003) ("A content-based government speech restriction receives the most rigorous scrutiny, which is almost al-

i. Restriction Is Content Neutral

While the right to be forgotten may appear to be a solely content-based restriction, insofar as it would be invoked only where specific speech content was objected to by a particular requester; in fact, from the perspective of the government, the restriction would be content-neutral. In establishing a right to be forgotten, Congress would not be aiming to curtail the expression of a particular idea, but rather setting guideposts on the forms which internet speech may take and the lifespan for which it may exist. In that sense, telling search engine providers to delist dated URLs is closer to telling concert promotors they cannot exceed a particular volume in their shows, or telling protesters they may not assemble after 8pm on weeknights, than it is to criminalizing indecent phone messages or imposing financial burdens on literary works by former felon mentioning past crimes.[163] That is, it is not the semantic content of the speech that is subject to restriction, but rather the time, place, or manner of the expression—namely its existence in cyberspace and its ease of availability to the public in perpetuity.[164]

There are a number of tests which can be used to establish whether a restriction is content-neutral, but the thrust of the focus in any of these formulations involves "whether the government has adopted a regulation of speech because of disagreement with the message it conveys."[165] In the case of the right to be forgotten, the government is not disagreeing with *what* the message conveys, but rather, disagreeing with *how* it is conveyed. For example, if an individual wanted to enforce her right to be forgotten to delist a photo posted by another person on Facebook, the restriction on the poster's speech would not be responding to the content of the photo, but rather the photo's being publicly available on the internet. Two variations on this example help to clarify the con-

---

ways fatal. By contrast a content neutral speech restriction receives much more lenient intermediate review.").

[163] Sable Communications of Cal. v. F.C.C., 492 U.S. 115 (1989); Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Board, 502 U.S. 105 (1991).

[164] *See* Wilson Huhn, *Assessing the Constitutionality of Laws That Are Both Content-Based and Content-Neutral: The Emerging Constitutional Calculus* 79 IND. L. J. 801, 806 (explaining "it is not always possible to classify a law as purely content-based or purely content-neutral. Many laws regulating expression—perhaps most such laws—are *both* content-based *and* content neutral").

[165] *Ward*, 491 U.S. at 791; *see also* Renton v. Playtime Theatres, Inc. 475 U.S. 41, 48 (1986) (holding that content-neutral "speech regulations are those that are justified without reference to the content of the regulated speech").

tent-neutral nature of the right. First, if the photo existed only in print form and was kept in the photographer's home, the subject of the photo would not be able to exercise the right because the speech would not have the spatial or temporal properties of an internet URL and thus would not warrant delisting. Second, regardless of the content of the photo—whether it depicted its subject drinking underage, attending a protest, or reading studiously—so long as it was posted publicly online, and the subject was not a public figure, the subject of the photo could try to invoke the right. In either event, the restriction would treat the content of the speech the individual seeks to have delisted impartially and instead focus solely on the nature of its publication.

There are many similarities between restrictions on the listing of URLs and other speech restrictions the Court has deemed to be content-neutral. Consider, for example, the case of *Ward v. Rock Against Racism*, in which New York City mandated the use of city-provided sound systems for public concerts in Central Park in order to reduce the maximum amount of noise produced by such an event.[166] The ordinance was enacted in response to several complaints from individuals living near the concert venue who were disturbed by the noise level, but the sponsors of a rock concert complained that the ordinance interfered with their First Amendment rights.[167] The Court upheld the ordinance, explaining that it was narrowly tailored to the content-neutral "desire to control noise levels at bandshell events, in order to retain the character of the [park] and its more sedate activities, and to avoid undue intrusion into residential areas and other areas of the park."[168] The city's aim—namely preserving public space so that all could enjoy it and so that no other activities such as "reclining, walking, and reading"[169] were dissuaded—was endorsed by the Court as a compelling interest.[170]

There are many parallels between the City's ordinance and a right to be forgotten in that both are concerned primarily with regulating a certain manner of speech rather than the content of the speech. Both endeavor to protect public space for the enjoyment of the many rather the few, and both recognize that allowing the volume of certain speech to be too high can have a chilling effect on other activities that people enjoy in public space. Just as a New Yorker might choose not to read or nap in

---

[166] *Id.* at 784.
[167] *Id.*
[168] *Id.* at 792.
[169] *Id.* at 784.
[170] *Id.* at 796.

Central Park when rock music is blasting at 120 decibels, a person might be dissuaded from posting a selfie to social media or write a blog post if she believes that those artifacts of her digital existence will be broadcast to the public for eternity. Neither advocate for removing a particular type of speech from the public forum entirely, just limiting its reach. Just as the concert can still be heard by those close to the stage, an article containing a particular nugget of unseemly private information can still be accessed by those who look for it directly through the host site rather than via a search engine listing. Thus, while a city can adopt an ordinance, limiting the allowable level of noise created by public concerts in light of a spate of complaints, Congress seems capable of adopting an ordinance limiting the widespread accessibility of blog posts reporting on the intimate details of a private person's life after she requests them to be removed.[171] In the first case it is the excessive quantity of sound that is objected to, and in the second it is the excessive quantity of digital space that the speech takes up. In both cases, however, it is clear that the government's interest is on restricting the volume of speech, rather than in restricting its content.

ii. Compelling Government Interest

Having determined that a right to be forgotten is a content-neutral restriction, its constitutionality may be determined according to whether or not the restriction serves a compelling government interest.[172] Many government interests could be deduced from the right to be forgotten, but foremost among these would be an interest in tranquility, acknowledging the deeply human desire to be left alone by bothersome, loud speech. Such a government interest is nearly identical to that identified by the Court in numerous other content-neutral speech restrictions, which emphasize the "tranquility interests" of private individuals.[173] In *Frisby v. Schultz*, for example, the Court held that a town ordinance preventing picketing on quiet, residential streets was not a First Amendment violation because the ordinance served the compelling government interest of protecting residential privacy.[174] In *Kovacs v. Cooper*, the Court held that a city ordinance banning sound trucks was constitutional because the city

---

[171] *Id.* at 799.
[172] *Id.*; McCullen v. Coakley, 134 S. Ct. 2518, 2529 (2014); *Clark*, 468 U.S. 288, 293 *supra* note 159.
[173] *See Ward* v. 491 U.S. 781, 791-792 *supra* note 154; Frisby v. Schultz, 487 U.S. 474, 477 (1988); Kovacs v. Cooper, 336 U.S. 77, 97-97 (1949) (Frankfurter, J. concurring).
[174] *Frisby*, 487 U.S. 474, 484.

had a compelling government interest in preventing "inroads upon the public peace" and "safeguarding the steadily narrowing opportunities for serenity and reflection."[175]

The Supreme Court has also identified a right to tranquility in one's thoughts and private life, in a personal, emotional sense.[176] In *National Archives v. Favish*, for example, the Court refused a request from a reporter for death scene records of the complainant family's relative, drawing a zone of privacy around intimate memories and the emotional well-being of decedents.[177] The justices worried that widespread publication could extend the lifespan of invasive and troubling information long past its relevance, such that the "peace of mind and tranquility" of family members would be threatened far into the future by "a sensation-seeking culture."[178] The Court recognized that in areas of particular sensitivity, long-held privacy customs—even those with little judicial precedent such as grieving—are a valid basis for justifying the shaping and reshaping of a protected zone of privacy.[179] Freedom to pursue peace of mind, tranquility, memory, and happiness can be conceptualized as fundamental rights protected within zones of privacy from intrusions by public speech.

The same case could surely be made in the context of the right to be forgotten. Given the significant support afforded to individual growth reflected in 19th and early 20th century caselaw, as well as the Court's clear recognition of a compelling government interest in protecting tranquility and public peace, it seems possible that a restriction on speech intending to shield private persons from perpetual reminders of their past might be upheld. After all, the Court has deemed restrictions on loudspeakers, sound trucks, protests, and the publication of death scene photos to be constitutional insofar as they protect against unwanted intrusions into interior life. In many of these cases, what is complained of is the effect of technology—be it a sound system, bull horn, news site, or

---

[175] *Kovacs*, 336 U.S. 77, 97.
[176] *See* Palko v. Connecticut, 58 S. Ct. 149, 152 (1937) (noting the existence of zones of privacy in many places in which "fundamental rights" which are "implicit in the concept of ordered liberty" are threatened by outside intrusion). The phrase "implicit in the concept of ordered liberty" used here refers to those unenumerated rights people may experience subliminally and feel a deep connection to such as the right to be left alone.
[177] Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 157 (2004) ("It is the right of privacy of the living which it is sought to enforce here . . . to protect their feelings, and to prevent a violation of their own rights in the character and memory of the deceased.").
[178] *Id.* at 158.
[179] *Id.*

search engine—capable of broadcasting speech in a certain undesirable way, impinging on a certain government interest. In that sense, it is the technology or the manner of speech that threatens the government interest rather than the fact of speaking itself. As Justice Frankfurter explained in *Kovacs*, "Only a disregard of vital differences between natural speech, even of the loudest spellbinders, and the noise of sound trucks would give sound trucks the constitutional rights accorded to the unaided human voice."[180] Thus, if the Court were to find that the government has a significant interest in protecting the privacy and tranquility of private individuals, in "safeguarding the steadily narrowing opportunities for serenity and reflection,"[181] and thereby allowing for freedom for personal growth, the right to be forgotten might overcome First Amendment challenges.

Conclusion—The Moral Value of the Right to be Forgotten

Ultimately, the right to be forgotten is an issue of extraordinary urgency and significance. As an ever-growing amount of information is available about each person online, the importance of the ability to revise one's past increases dramatically. While the human mind is naturally predisposed to forgiving by forgetting, digital memory does not allow us the same convenience. Instead, it reminds us again and again of our past transgressions, forming an easily discoverable log of our lives and leaving us exposed to prying eyes far into the future. The harmful effect of the internet's inability to forget is the erasure of a line between the person someone once was and the person he is now as a result of reforming himself. As Daniel Solove writes, "We may find it increasingly difficult to have a fresh start, a second chance, or a clean slate. We might find it harder to engage in self-exploration if every false step and foolish act is chronicled forever in a permanent record. This record will affect our ability to define our identities, to obtain jobs, to participate in public life, and more. Ironically, the unconstrained flow of information on the internet might impede our freedom."[182]

Instead of trapping people in the mistakes of their past and forcing them into stagnancy, the right to be forgotten allows individuals to adjust their opinions, rejoin society after criminal involvement, evade the

---

[180] *Kovacs*, 336 U.S. 77, 97.
[181] *Id.*
[182] DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 17 (2007).

scrutiny of personal and professional connections, and freely change their identities. To draw on some examples from Europe, the right to be forgotten can allow an individual who sued her former employer for discrimination to obscure articles about the lawsuit when she is applying for a new job.[183] It can allow someone with schizophrenia to obscure an article discussing his escape from a mental hospital, and it can allow someone charged with fraud to obscure an article connecting him with the alleged crimes once he is acquitted.[184] The right to be forgotten can also hide an article describing an individual's struggles with addiction, a blog post containing an individual's address and phone number, and an actress profile on a pornography site.[185] The right acknowledges the messiness of life by mitigating the internet's ceaseless storage of readily accessible personal information, and making it harder, but not impossible, for others to access this sensitive data. In doing so, the right effectively re-creates the limitations on information gathering that existed in the pre-internet era.

---

[183] *See* TRANSPARENCY REPORT *supra* note 45 (stating "[Google] received a request by a former high-ranking employee of a large business to delist one URL from Google search, a news article reporting about the individual suing their former employer for unfair dismissal" that was subsequently delisted).

[184] TRANSPARENCY REPORT *supra* note 45.

[185] *See Id.* (stating "[Google] received a request from the Italian Data Protection Authority to delist 19 URLs recounting phone conversations in which an individual participated, related to the bankruptcy of one of Italy's largest banks. The phone conversations had been illegally wiretapped. We deleted all 19 URLs in question, considering the unlawful source of the information and the lack of very strong public interest in relation to the individual's name otherwise"); *see also* Woodrow Hartzog & Evan Selinger, *Google Action on Revenge Porn Opens the Door on Right to be Forgotten in the US* GUARDIAN (Jun. 25, 2015) https://www.theguardian.com/technology/2015/jun/25/googles-revenge-porn-opens-right-forgotten-us (explaining that a "category-based approach" to the right to be forgotten has numerous advantages; "different solutions, ranging from expunging a minor's criminal record to deleting stale credit history, can be worked out independently of one another"); *see also* Chris Quinn, *We're Expanding Our Right-to-be-Forgotten Experiment* CLEVELAND.COM (Sept. 12, 2018) https://www.cleveland.com/metro/2018/09/were_expanding_our_right-to-be.html (explaining that one of the posts removed by Cleveland.com involved "someone who had been in the health field and stole some drugs from her employer"); *see also Do We Always Have to Delete Personal Data if a Person Asks?* EURO. COMM. (last accessed Jan. 19, 2021) https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en#examples (explaining that a company that runs a social media organization is obliged to delete photos of a minor if he decides that said photos are harming his career prospects).

A general recognition that individuals have the right to avoid lifelong stigmatization and ostracism as a result of their mistakes in the past has many positive consequences. It encourages individuals to present themselves authentically to their peers now, without fear of reprisal in the future should unsavory aspects of their character be unearthed decades later. This revisability leads to uninhibited, robust forms of communication and action. Freed from the specter of future judgment, people can experiment and take risks. They can engage in passionate debate and advocate unconventional positions without worry that if they change their mind down the road, their earlier views will be held against them; they can attend protests free from fear that a college admissions officer might negatively view their political involvement in the decision-making process; and they can receive gender-confirming surgery without concern that old articles misgendering them or using their dead name might be easily accessible.

The ability to hide indicia that one has at one time held an opinion with which he now disagrees or has been a person with whom he no longer identifies allows one to expand the expressive choices available to him and lessens the time and energy costs involved in making a decision. Freedom and privacy are inextricably interdependent, and if individuals do not have the ability to keep some parts of their lives private, and forget some of the troubling moments of their past, they will lose the liberty to develop as multifaceted, self-actualized beings. Ultimately, implementing the right to be forgotten can mitigate the demise of second chances in American life.