Golden Gate University Law Review

Volume 51
Issue 1 *Ninth Circuit Survey*

Article 6

March 2021

Dyroff v. Ultimate Software Group, Inc.: A Reminder of the Broad Scope of § 230 Immunity

Alex S. Rifkind
Golden Gate University School of Law

NOTE

DYROFF V. ULTIMATE SOFTWARE GROUP, INC.: A REMINDER OF THE BROAD SCOPE OF § 230 IMMUNITY

*ALEX S. RIFKIND**

"Nothing vast enters into the life of mortals without a curse."[1]

INTRODUCTION

The Internet[2] is one of the most ubiquitous and accessible methods of modern communication.[3] Today, Internet users access, create, and edit online content.[4] Like newspapers, Internet content consists of a combination of information and speech. However, unlike other forms of communication, such as broadcast media,[5] the Internet receives greater speech

* J.D./LL.M Candidate, Golden Gate University School of Law, May 2021; B.S. Neuropharmacology, University of California at Santa Barbara, May 2012, M.S. Biological Sciences, Dominican University of California, May 2016. Associate Editor, 2020-21, *Golden Gate University Law Review*.

[1] Sophocles, ANTIGONE (442 B.C.E).

[2] The capitalized form *Internet* is more commonly used in U.S. publications. The *Internet* is defined as "an electronic communications network that connects computer networks and organizational computer facilities around the world." (*Internet*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/Internet (last visited Oct. 19, 2020)).

[3] Emily Elert, *How the Internet Has Spread Around the World,* POPSCI (Dec. 11, 2012) https://www.popsci.com/science/article/2012-12/widening-world-web-internet-infographic/.

[4] Blumenthal v. Drudge, 992 F. Supp. 44, 48, n.7 (1998) ("[T]he users of Internet information are also its producers").

[5] *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 868 ("[S]pecial justifications for regulation of . . . broadcast media . . . are not applicable to other speakers").

protection under the First Amendment.[6] Content regulation and speech moderation on the Internet remains controversial.[7]

Historically, Congress's regulation of the Internet proved unsuccessful. In 1996, Congress enacted the Communications Decency Act ("CDA"),[8] which banned obscene material accessible to minors over any telecommunications device, including the Internet.[9] In 1997, in *Reno v. American Civil Liberties Union,* the United States Supreme Court held many of the CDA's provisions as a vague[10] and overbroad[11] form of content-based[12] speech suppression in violation of the First Amendment.[13] Congress responded by enacting the Child Online Protection Act ("COPA"),[14] a narrower regulation that punishes indecent material displayed online with a commercial purpose.[15] Similarly, in *Ashcroft v. American Civil Liberties Union*, the Supreme Court protected speech on the Internet by affirming a preliminary injunction against COPA enforcement, finding less restrictive and potentially more efficient alternative methods of regulation.[16] Together, *Reno* and *Ashcroft* demonstrate the judiciary's reservation to impose content-based restrictions on Internet

[6] *See* U.S. Const. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."); *see generally* Reno, 521 U.S. at 885 (Because Congress has a significant "interest in fostering the growth of the Internet[,] . . . [t]he interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship").

[7] *See* David L. Hudson Jr., *Free speech or censorship? Social media litigation is a hot legal battleground,* ABA J. (Apr. 1, 2019), http://www.abajournal.com/magazine/article/social-clashes-digital-free-speech.

[8] 47 U.S.C § 223.

[9] 47 U.S.C § 223(a)(1), (d)(1).

[10] "A law is unconstitutionally vague [under the First Amendment] if it fails to provide a reasonable opportunity to know what conduct is prohibited or is so indefinite as to allow arbitrary and discriminatory enforcement." Tuscan Woman's Clinic v. Eden, 379 F.3d 531, 555 (9th Cir. 2004). However, "perfect clarity is not required even when a law regulates protected speech." Cal. Teacher's Ass'n v. Bd. of Educ., 271 F.3d 1141, 1150 (9th Cir. 2001) (citing Ward v. Rock Against Racism, 491 U.S. 781, 794 (1989)).

[11] "A law is overbroad under the First Amendment if it 'reaches a substantial number of impermissible applications' relative to the law's legitimate sweep." Shickel v. Dilger, 925 F.3d 858 (6th Cir. 2019) (quoting East Brooks Books, Inc. v. Shelby Cty., 588 F.3d 360, 366 (6th Cir. 2009)).

[12] "A content-based regulation is one that is 'based upon either the content or the subject matter of the speech." Consolidated Edison Co. of New York, Inc. v. Pub. Serv. Comm'n of New York, 447 U.S. 530, 536 (1980) (citing Ward v. Rick Against Racism, 491 U.S. 781, 791 (1989)); *see* Reed v. Town of Gilbert, Ariz., 576 U.S. 155, 163 (2015) ("A law that is content based on its face is subject to strict scrutiny regardless of the government's benign motive, content-neutral justification, or lack of 'animus toward the ideas contained' in the regulated speech") (citing Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 429 (1993)).

[13] *Reno*, 521 U.S. at 875-76.

[14] 47 U.S.C § 231.

[15] 47 U.S.C § 231(a).

[16] *See* Ashcroft v. Am. Civ. Liberties Union, 535 U.S. 564, 564 (2002) ("[F]ilters are less restrictive means than COPA . . . [as] [t]hey impose selective restrictions on speech at the receiving

speech. However, both cases concerned indecent expression, a constitutionally protected form of speech under the First Amendment.[17] Comparatively, publication of defamation or illegal content falls outside freedom of speech protection under the First Amendment.[18]

While historically within the purview of newspapers, the transition to publication of content online opened the door for an interactive computer service ("ICS")[19] to face similar intermediary liability for posting illegal or defamatory content.[20] The result of imposing intermediary liability on ICSs created a *chilling effect* on Internet speech and disincentivized ICS self-regulation of content provided by third parties.[21] Congress responded by enacting § 230 of the CDA, intending to incentivize ICSs to engage in their own process of regulation and screening.[22]

In return, § 230 provides broad intermediary liability protection to ICSs so that they may engage in content moderation without fear of exposure to liability for offensive or illegal material that slips through.[23] As a result, § 230 provides a significant safeguard to Internet innovation and development.[24] However, varied judicial interpretation of the circumstances required to invoke § 230 immunity has led to inconsistent re-

---

end, not universal restrictions at the source . . . [and] filtering software may well be more effective than COPA . . .").

[17] *See Ashcroft*, 535 U.S. at 604 (Stevens, J., dissenting) ("COPA seeks to limit protected speech").

[18] *See generally* New York Times Co. v. Sullivan, 376 U.S. 254, 262 (1964) (defamation is generally understood as a false statement of fact concerning a person that causes some form of harm to the person and his/her reputation); *see* United States v. Williams, 553 U.S. 285, 297 (2008) ("Offers to engage in illegal transactions are categorically excluded from First Amendment protection") (citing Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 388 (1973)); Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498 (1949).

[19] 47 U.S.C. § 230(f)(2) ("The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet . . . ").

[20] *See generally* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct.) (ICS held accountable for defamatory content posted on its website by anonymous third-party), *superseded by statute*, 47 U.S.C. § 230; Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (defendant ICS not liable because it did not know, or have reason to know, of defamatory content on its website); Stratton Oakmont, 1995 WL 323710 at *5-6 (defendant ICS treated as a publisher when it created an editorial staff to monitor and edit website).

[21] Zeran v. America Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

[22] *Id.* at 331.

[23] *See Id*. at 330 ("[Section] 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred").

[24] *CDA 230: The Most Important Law Protecting Internet Speech*, Electronic Frontier Found., http://www.eff.org/issues/cda230; *accord* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 Harv. L. Rev. 2296, 2313 (2014).

sults.[25] Lack of a clear standard places application of § 230 immunity on a sliding scale between the United States Court of Appeals for the Fourth Circuit's decision in *Zeran v. America Online, Inc.*[26] of unconditional immunity[27] and the United States Court of Appeals for the Seventh Circuit's decision in *Chicago Lawyers' Committee For Civil Rights Under the Law, Inc. v. Craigslist, Inc.*[28] of conditional immunity.[29] Historically, the Ninth Circuit followed the holding from *Zeran* and utilized its rationale as foundation for its own test to determine if § 230 immunity applies—the *Barnes Test*.[30]

The Ninth Circuit applied the *Barnes Test* to a § 230 immunity challenge in the recent case of *Dyroff v. Ultimate Software Group*.[31] The plaintiff, Kristanalea Dyroff, sued Ultimate Software Group ("Ultimate Software") for its alleged role in the tragic death of her son, Wesley Greer.[32] The Ninth Circuit found § 230 immunized Ultimate Software's from liability and barred Dyroff's claims.[33]

Although advocates of § 230 praised the decision in *Dyroff* for upholding ICS immunity,[34] the Ninth Circuit's interpretation of automated manipulations of third-party content as *content-neutral* tools will likely broaden the application § 230 immunity in future decisions.[35] The *Dyroff* decision comes despite concern from the media and Congress that § 230

---

[25] *See* Jerry Kang, *Communications Law & Policy*, 331, 335-38, 351-54 (4th ed. 2012) (noting a lack of unity among federal courts regarding § 230's scope of enforcement).

[26] Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).

[27] *Id*. at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service").

[28] Chi. Lawyers' Comm. For Civil Rights Under the Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008).

[29] *Id*. at 669-70.

[30] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100-01 (9th Cir. 2009) (immunity from liability existing for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider").

[31] Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, 1097 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020).

[32] *Id*. at 1094.

[33] *Id*. at 1101.

[34] *See* Eric Goldman, *A Significant Section 230 Defense Win in the Ninth Circuit-Dyroff v. Ultimate Software.* TECH. & MARKETING L. BLOG (Aug. 21, 2019), https://blog.ericgoldman.org/archives/2019/08/a-significant-section-230-defense-win-in-the-ninth-circuit-dyroff-v-ultimate-software.htm.

[35] *See* Jeffrey Neuburger, *Ninth Circuit Releases Another Important CDA Section 230 Opinion With Broad Application – Automated Content Recommendation and Notification Tools Do Not Make Social Site the Developer of User Posts.* NAT. L. REV. (Aug. 28, 2019), https://www.natlawreview.com/article/ninth-circuit-releases-another-important-cda-section-230-opinion-broad-application.

might need revision.[36] However, the focus should not necessarily concern revision and amendment, but instead reinforce the original intent of the statute and encourage greater ICS accountability in moderating illegal and unlawful content.[37]

Part I of this Note examines the factual and procedural history of *Dyroff* and discusses the Ninth Circuit's application of § 230 immunity in the case. Part II outlines the history of the CDA and examines how the federal courts have interpreted § 230 immunity leading up to its application in *Dyroff*. Part III discusses judicial interpretation of the scope of § 230 immunity. Lastly, Part IV argues that the Ninth Circuit correctly applied the law in the *Dyroff* decision, but failed to adequately define the term *content-neutral*. Further, by not defining what falls within the scope of *content-neutral*, the Ninth Circuit's holding implicitly immunizes any manipulation of third-party content facilitating communication that does not materially contribute to the content at issue. The broad shield of § 230 immunity, which was necessary for growth and development during the Internet's infancy, is antiquated and should be narrowed by Congress to foster greater accountability to prevent tragedies like *Dyroff* from recurring.

I. *DYROFF V. ULTIMATE SOFTWARE GROUP, INC.*

A. FACTUAL AND PROCEDURAL BACKGROUND

In 2007, Ultimate Software launched a social networking site called the Experience Project.[38] The website consisted of numerous and distinct online communities that were formed by members based on common interests, attributes, or experiences.[39] Users interacted anonymously with each other by posting and answering questions.[40] Experience Project did

[36] *See* Daisuke Wakabayashi, *Legal Shield for Websites Rattles Under Onslaught of Hate Speech.* THE NEW YORK TIMES. (Aug. 6, 2019), https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html; *see*, *e.g.*, Eric Goldman, *How SESTA Undermines Section 230's Good Samaritan Provisions*, TECH. & MARKETING L. BLOG (Nov. 7, 2017), http://blog.ericgoldman.org/archives/2017/11/howsesta-undermines-section-230s-good-samaritan-provisions.htm (addressing congressional efforts to amend § 230).

[37] *See*, *e.g.*, Joshua Geltzer, *President and Congress Are Thinking of Changing This Important Internet Law*, SLATE (Feb. 25, 2019), https://slate.com/technology/2019/02/cda-section-230-trump-congress.html ("Sen. Ron Wyden, a co-author of Section 230, has explained that it was intended as both a 'shield' *and* a 'sword' for tech companies, protecting them from liability for vast amounts of content for which they're not assuming responsibility but also empowering them to do what they can to eliminate the worst of that content").

[38] *Dyroff*, 934 F.3d at 1095.

[39] *Id*. at 1094-95 (group topics ranging from "I like dogs," "I have lung cancer," "I'm going to Stanford," to "I Love Heroin").

[40] *Id*. at 1094.

not limit or encourage the type of interactions members engaged in on the site.[41] Experience Project utilized advanced machine-learning algorithms to analyze user data and glean the underlying intent and emotional state of its users.[42] Ultimate Software then sold this information for commercial purposes (directed advertisements) and to steer users to particular groups through its notification and recommendation functions.[43] The recommendation functionality also included an email suite and other push notifications, which alerted users of new content posted to its groups.[44] Experience Project generated revenue through directed advertisements and the sale of tokens that users were required to purchase to post questions to other users in its groups.[45]

In August 2015, Wesley Greer, a recovering heroin addict, conducted a Google search to purchase heroin and was directed to Experience Project.[46] Greer created an account and purchased tokens that enabled him to post questions to other users.[47] He posted to a group titled "where can i score heroin in jacksonville, fl." (*sic*).[48] On August 17, 2015, Experience Project sent Greer an email notifying him that another user posted a response to the "where can i score heroin in jacksonville, fl." (*sic*) group and provided a hyperlink and URL directing his response.[49] The response came from Hugo Margenat-Castro, an Orlando-based drug dealer, who regularly used Experience Project to sell heroin.[50] Greer obtained Castro's phone number through Experience Project, and later bought heroin from Castro.[51] On August 19, 2015, Greer died from fentanyl toxicity, unaware of its presence in the heroin that he purchased from Castro.[52] Castro was later arrested and prosecuted; in March 2017, he plead guilty to selling fentanyl-laced heroin through Experience Project.[53]

In March 2016, Experience Project publicly announced it was shutting down in response to privacy concerns, which stemmed from governmental overreach and insufficient resources to respond to government

---

[41] *Id*.

[42] Dyroff v. Ultimate Software Grp., Inc., No. 17-CV-05359-LB, 2017 WL 5665670, at *2 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019).

[43] *Id*.

[44] *Id*.

[45] *Dyroff*, 934 F.3d at 1095.

[46] Dyroff v. Ultimate Software Grp., Inc., 17-CV-05359-LB, 2017 WL 5665670, at *2 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019).

[47] *Id.*

[48] *Id*.

[49] *Id*. at *3.

[50] *Id*.

[51] *Id*.

[52] *Id*.

[53] *Dyroff*, 934 F.3d at 1095.

information requests.[54] While Experience Project was active, users shared 67 million experiences, made 15 million connections, and asked 5 million questions.[55]

Kristanalea Dyroff, Greer's mother, brought suit against Ultimate Software asserting seven state claims that predicated liability on Experience Project's use of data mining and machine-learning of its users' posts to recommend and to steer Greer toward heroin-related discussion groups and the drug dealer, who ultimately sold him fentanyl-laced heroin.[56] The district court dismissed all claims, holding Ultimate Software immune under § 230(c)(1) because its recommendation algorithms constituted *content-neutral* tools that facilitated communication, but did not create or develop the content at issue.[57] The district court also found that Experience Project neither had a special relationship with Greer nor created risk through its website functionalities, and therefore owed no duty of care to Greer about another user's illegal activities.[58] Subsequently, in June 2018, Dyroff appealed to the Ninth Circuit.[59]

B. THE NINTH CIRCUIT FINDS ULTIMATE SOFTWARE NOT LIABLE UNDER § 230

On appeal, Dyroff alleged the district court erred in holding § 230 of the CDA immunized Ultimate Software, that the allegations of collusion between Ultimate Software and drug dealers using Experience Project were not plausible, and that Ultimate Software owed no duty of care.[60] However, on August 20, 2019, the Ninth Circuit affirmed the district court's ruling in a published opinion, finding that § 230 barred Dyroff's claims against Ultimate Software.[61]

Under the Ninth Circuit's *Barnes Test* "[i]mmunity from liability exists for '(1) a provider or user of an interactive computer service [("ICS")] (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another

---

[54] *Id*.

[55] *Id*.

[56] Dyroff v. Ultimate Software Grp., Inc., 17-CV-05359-LB, 2017 WL 5665670, at *1 (N.D. Cal. Nov. 26, 2017), *aff'd*, 934 F.3d 1093 (9th Cir. 2019) (Dyroff claiming (1) Negligence, (2) Wrongful Death, (3) Premises Liability, (4) Failure to Warn, (5) Civil Conspiracy, (6) Unjust Enrichment, and (7) a violation of the Drug Dealer Liability Act (Cal. Health & Safety Code §§ 11700, *et seq.*) and asserting that Ultimate Software had knowledge or should have had knowledge of illegal drug transaction occurring on its website).

[57] *Id*.

[58] *Id*.

[59] Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020).

[60] *Id*. at 1096.

[61] *Id*.

information content provider [("ICP")].'"[62] In *Dyroff*, the Ninth Circuit interpreted the term ICS expansively[63] and determined that Ultimate Software was an ICS for the following reasons: its structure was a website;[64] it did not create or publish its own content; and it did not become an ICP[65] through the use of *content-neutral* website functions. Collectively, these findings satisfied *Barnes's* first prong.[66]

The court found *Barnes's* second prong satisfied because Ultimate Software did not create or develop information or content that led to Greer's death, since the posts to the group were made by Greer and Castro.[67] Although Dyroff argued that Experience Project's recommendation algorithms and push notification system constituted creation of content, the court disagreed and reasoned that the website features were "tools meant to facilitate the communication and content of others," but were not actually content.[68]

The court held *Barnes's* third prong satisfied because Ultimate Software had not materially contributed to the content posted on Experience Project leading to Greer's death. The court drew inference from *Fair Housing Council of San Fernando Valley v. Roommates.com*,[69] and identified the following as material contributions arising to the creation of content: mandating posting criteria, suggesting posting content, or clearly making a direct contribution to unlawful and offensive user posts to the content.[70] The court found Experience Project's website functions facilitated user-to-user communication and content, but did not materially contribute to the content itself.[71]

---

[62] *Id*. at 1097 (quoting Barnes v. Yahoo! Inc., 570 F.3d 1096, 1100-1101 (9th Cir. 2009)).

[63] *See* Kimzey v. Yelp! Inc., 836 F.3d 1263, 1268 (9th Cir. 2016).

[64] *See Id.* at 1268 (acknowledging that websites are the most common interactive computer service); *see also* Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1162 (9th Cir 2008) (en banc) ("[t]oday, the most common interactive computer services are websites").

[65] An "ICP" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. §230(f)(3).

[66] *Dyroff*, 934 F.3d at 1097

[67] *Id*. at 1098-99.

[68] *Id*. at 1098; *See Kimzey*, 836 F.3d at 1098 ("[P]roliferation and dissemination of content does not equal creation or development of content").

[69] Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008) (en banc).

[70] *Id*. at 1098-99; *See also Kimzey*, 836 F.3d at 1269 (Material contribution falls into two categorially distinct actions, those traditional to publishers and those that make displayed content illegal).

[71] *Id.* at 1099 ("[T]he material contribution test makes a '"crucial distinction between, on the one hand, taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable'") (quoting *Kimzey*, 836 F.3d at 1269, n.4).

In addition, the court also considered Dyroff's attempts to circumvent § 230 immunity, which alleged Ultimate Software had actual or constructive knowledge of illegal activity occurring on its website, and owed a duty of care to Greer. Dyroff contended that Ultimate Software knew or should have known of illegal drug transactions occurring between its users, and facilitated transactions through its anonymity features.[72] The court found Dyroff's reliance upon *J.S. v. Village Voice Media Holdings, L.L.C.*[73] unpersuasive because Ultimate Software's anonymity practices, public statements of concern for internet privacy, and the burden of law enforcement information requests were not facts that plausibly suggest collusion with drug dealers.[74] Dyroff's duty of care argument was predicated on a failure to warn theory of misfeasance.[75] Misfeasance occurs when a defendant worsens a plaintiff's position and creates a duty of care where one did not originally exist.[76] The court determined that Ultimate Software did not worsen Greer's position through its recommendation algorithms and push notification features because these website functions were applied to all users.[77] Furthermore, the court held that a website could not function if facilitating communication in a *content-neutral* fashion between users created a duty of care.[78]

II. LEGISLATIVE BACKGROUND OF THE CDA AND § 230 IMMUNITY

From a modern perspective, the Internet of the '90s was an unrecognizable landscape.[79] The new dial-up Internet connected users through bulletin boards;[80] online newspapers were just emerging;[81] Google did not hold the linguistic status of a verb; and the intuitiveness

---

[72] *Id*. at 1099-100.

[73] *See generally* J.S. v. Vill. Voice Media Holdings, L.L.C., 184 Wash. 2d 95 (2015) (en banc) (holding that minors sufficiently alleged website operators of Backpage.com facilitated sexual exploitation of children and claims against website were not barred by § 230).

[74] *Dyroff*, 934 F.3d at 1100.

[75] *Id*. at 1100. ("When analyzing duty of care in the context of third-party acts, California courts distinguish between 'misfeasance' and 'nonfeasance'").

[76] Lugtu v. Cal. Highway Patrol, 26 Cal. 4th 703, 716 (2001).

[77] *Dyroff*, 934 F.3d at 1101.

[78] *Id*.; *See, e.g.*, Klayman v. Zuckerberg, 753 F.3d 1354, 1359–60 (D.C. Cir. 2014) (holding no special relationship exists between Facebook and its users).

[79] *See, e.g.*, Nicholas Carlson, *Presenting: This is What the Internet Looked Like in 1996,* BUS. INSIDER AUS. (Apr. 16, 2014), https://www.businessinsider.com.au/the-coolest-web-sites-from-1996-2014-4#-8.

[80] *See* Benj Edwards, *The Lost Civilization of Dial-Up Bulletin Board Systems,* THE ATLANTIC (Nov. 4, 2016), https://www.theatlantic.com/technology/archive/2016/11/the-lost-civilization-of-dial-up-bulletin-board-systems/506465/.

[81] *See* Peter H. Lewis, *The New York Times Introduces a Website*, N.Y. TIMES (Jan. 22, 1996) at D7.

of modern online research capabilities was nonexistent.[82] Within this burgeoning technological environment, Congress could not have foreseen how the modern Internet would develop two decades into the twenty-first century.

Congress did address one development of the Internet of the '90s: online pornography.[83] The CDA, attached to Title V of the Telecommunications Act of 1996,[84] was intended to safeguard children from exposure to indecent online material by criminalizing the knowing transmission of obscene or indecent material to minors and incentivizing telecommunication companies to participate in blocking the explicit material.[85] However, the Supreme Court in *Reno v. ACLU* struck many of the vague and controversial criminal provisions of the CDA as an overbroad form of content-based speech suppression, in violation of the First Amendment.[86] *Reno* and its progeny would later pressure Congress to revisit the CDA to ensure protection of the Internet, and ultimately provide the rationale for the addition of § 230.

A. THE RISE OF § 230 IMMUNITY

In the years preceding § 230's enactment, two Internet liability cases, *Cubby, Inc. v. CompuServe, Inc.*[87] and *Stratton Oakmont, Inc. v. Prodigy Services Co.,*[88] encouraged Congress to define the boundaries of ICS liability. The *Cubby* court held CompuServe, a predecessor to the modern ICS, was subject to the same standard of liability applied to

[82] *See* Megan Sapnar Ankerson, *How Coolness Defined the World Wide Web of the* 1990s, THE ATLANTIC (July 15, 2014), https://www.theatlantic.com/technology/archive/2014/07/how-coolness-defined-the-world-wide-web-of-the-1990s/374443/.

[83] *See* 141 CONG. REC. §1953 (daily ed. Feb. 1, 1995) (statement Sen. Exon, author of the CDA, arguing for his version of the CDA, denouncing pornography on the Internet, and expressing concern that the Internet would become a red-light district).

[84] Pub. L. No. 104-104, §§ 501-09, 551-52, 561, 110 Stat. 56, 133-37, 139-43 (1996) (codified in scattered sections of 47 U.S.C.).

[85] *See* S. REP. No. 104-23, at 59 (1995); *see* 141 CONG. REC. 15,503 (1995) (statement of Sen. Exon, author of the CDA) ("The fundamental purpose of the Communications Decency Act is to provide much needed protection for children"); *see also* Reno v. ACLU, 521 U.S. 844, 860 (1997) (the incentive to participate in blocking explicit material arising from two affirmative defenses, "[o]ne cover[ing] those who take 'good faith, reasonable, effective, and appropriate actions'" to restrict a minor's access to prohibited communications under § 223(e)(5)(A), the other covering "those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code" under § 223(e)(5)(B)).

[86] *See Reno* at 858-60, 874-76 (CDA must pass heightened First Amendment scrutiny because plaintiffs were information content providers).

[87] Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

[88] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute,* 47 U.S.C. § 230(c)(1), *as recognized in* Force v. Facebook, Inc., 934 F.3d 53 (2nd Cir. 2019).

traditional news vendors—"whether [CompuServe] knew or had reason to know of . . . allegedly defamatory [or illegal] statements."[89] Four years later, the *Stratton Oakmont* court declined to apply *Cubby's* liability standard and imposed liability on an Internet service provider who edited third party content.[90] Together *Cubby* and *Stratton Oakmont* had the effect of immunizing online service providers from liability when no action is taken to edit or screen user-generated content and creating liability when actions were taken to moderate content.[91]

The decisions in *Cubby* and *Stratton Oakmont* generated widespread publicity and lobbying by tech companies, which led Congress to consider an appropriate legislative remedy.[92] The addition of § 230 to the CDA explicitly addressed the problematic *Stratton Oakmont* decision.[93] With enactment of § 230, Congress abrogated *Stratton Oakmont's* holding and provided broad immunity to ICSs. Congress reasoned that broad immunity was a more effective means of promoting content moderation than explicitly requiring ICSs to moderate content.[94]

B. STRUCTURAL COMPONENTS OF § 230

Section 230 has two key provisions that address its primary goals—Internet innovation[95] and voluntary content moderation[96]—codified in

[89] *Cubby*, 776 F. Supp. at 140-41.

[90] *Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229 at *10.

[91] *See* Mary Jane Fine, *Mom Wants AOL to Pay in Child's Sex Ordeal, She Calls Service Liable, Despite Law*, BERGEN REC. (Apr. 19, 1998) at A01.

[92] *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008). Congressman Christopher Cox, who would later become a paid lobbyist for the tech industry, cosponsored § 230 to protect companies "who take[ ] steps to screen indecency and offensive material for their customers." 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

[93] H.R. REP. NO. 104-458, at 174 (1996) (Conf. Rep.) ("One of the specific purposes of this section is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material").

[94] 141 CONG. REC. H8471-472 (1995) ("[T]here is a tremendous disincentive for online service providers to create family friendly services by detecting and removing objectionable content. These providers face the risk of increased liability where they take reasonable steps to police their systems . . . [§ 230] removes the liability of providers . . . who make a good faith effort to edit the smut from their systems. It also encourages the online services industry to develop new technology, such as blocking software, to empower parents to monitor and control the information their kids can access").

[95] *See* 47 U.S.C. § 230(b)(1) ("[T]o promote the continued development of the Internet and other interactive computer services and other interactive media"); 47 U.S.C. § 230(b)(2) ("[T]o preserve the vibrant and competitive free market that presently exists for the Internet and other computer services, unfettered by Federal or State regulation").

[96] *See* 47 U.S.C. § 230(b)(3) ("[T]o 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"); 47 U.S.C. § 230(b)(4) ("[T]o remove disin-

§ 230(c)(1) and § 230(c)(2), respectively. Section 230(c)(1) prohibits any provider of an ICS[97] from being treated as the publisher or speaker of any content provided by an ICP.[98] Importantly, an ICS does not lose its § 230 immunity if a good faith effort is made to moderate and remove material that the provider finds objectionable.[99] This provision enables an ICS to set and enforce content standards without becoming subject to liability for the content provided by an ICP.

Section 230's broad immunity is limited by several exceptions. First, an ICS is not immunized when user content violates federal criminal law.[100] Second, there is no immunity for an ICS when its users violate copyright or other intellectual property laws.[101] Third, immunity is inapplicable to violations of federal wiretap laws or provisions of the Electronic Communications Privacy Act of 1986.[102]

III. INTERPRETING THE SCOPE OF § 230

Section 230's straightforward immunity provisions and clear exceptions left room open for judicial interpretation of how immunity should apply to an ICS when faced with a liability suit. The initial decade of § 230 enforcement was marked by sweeping application of immunity. However, the broad protection afforded at the outset would gradually erode to reveal § 230's limits.

---

centives 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"); 47 U.S.C. § 230(b)(5) ("[T]o ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer").

[97] An ICS is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).

[98] 47 U.S.C. § 230(c)(1). An "ICP" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service" as per 47 U.S.C. §230(f)(3).

[99] 47 U.S.C. § 230(c)(2) ("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, 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)").

[100] 47 U.S.C. § 230(e)(1) ("Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute").

[101] *See* 47 U.S.C. § 230(e)(2); *see also* 17 U.S.C. § 512 (2010) (providing that the Digital Millennium Copyright Act establishes a notice-and-takedown procedure requiring an ICS to remove copyright infringing material if it receives notice or face liability from the copyright holder for failure to remove the material).

[102] 47 U.S.C. § 230(e)(4).

A. § 230 AND EXPANSIVE IMMUNITY

In 1997, the United States Court of Appeals for the Fourth Circuit issued an opinion in *Zeran v. America Online*,[103] which ushered in an era of court decisions that broadly interpreted the scope of § 230 immunity. *Zeran* concerned an anonymous post on an America Online ("AOL") bulletin board alleging a user was selling offensive t-shirts.[104] The post included the user's home phone number, which resulted angry phone calls and death threats.[105] Subsequently, the user brought a liability suit against AOL for the anonymous poster's defamatory speech.[106]

The Fourth Circuit reasoned that the "plain language" of § 230(c)(1) "creates federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[107] Accordingly, any "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content—are barred."[108] The *Zeran* opinion was the first instance where a federal appellate court interpreted the scope of § 230, which resulted in courts across the nation quickly adopting its broad reading.[109]

In 2003, the Ninth Circuit applied *Zeran's* broad interpretation of § 230 immunity and extended it to a website that hosted user-generated content in *Carfarano v. Metrosplash.com*.[110] The *Carafano* decision found Matchmaker.com ("Matchmaker"), an online dating service, immune from liability arising from a user's fabricated profile that included photographs of the plaintiff.[111] After the plaintiff received sexually explicit and threatening messages in response to the false profile, plaintiff's counsel requested Matchmaker remove the false profile and the company complied.[112] The plaintiff brought suit for "invasion of privacy, misappropriation of the right of publicity, defamation, and negligence."[113]

The Ninth Circuit found Matchmaker immune under § 230 because "so long as a third party willingly provides the essential published con-

---

[103] Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997).

[104] *Id*. at 329.

[105] *Id*.

[106] *Id*. at 329-30.

[107] *Id*. at 330.

[108] *Id*.

[109] *See, e.g.*, Blumenthal v. Drudge, 992 F. Supp. 44, 46 (D.D.C. 1998) ("Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others").

[110] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

[111] *Id*. at 1121.

[112] *Id*. at 1122.

[113] *Id*.

tent, the interactive service provider [(ISP)] receives full immunity regardless of the specific editing or selection process."[114] The decision broadened the scope of § 230 immunity, so that its protections applied even when a website provided the opportunity for third parties to create illegal content.[115]

B. THE SHIELD BEGINS TO CRACK: § 230 IMMUNITY LIMITATIONS

The limitless certainty of § 230 immunity did not endure beyond its infancy. In 2008, the Ninth Circuit issued the *Roommates.com en banc* opinion[116] that marked a stark detour from its routine application of broad § 230 immunity. Roommates.com ("Roommates") connected individuals looking for housing with those who had rooms to rent. As a requirement of the rental process, subscribers created a profile using the website's automated questionnaire, which requested information concerning sexual orientation, gender, and whether children would be living in the rental.[117] Fair Housing Council of San Fernando Valley and the City of San Diego brought suit against Roommates, alleging violation of federal and state housing discrimination laws, which prohibit discrimination based on sexual orientation, gender and family status.[118]

The Ninth Circuit found § 230 did not apply to Roommates because the "CDA does not grant immunity for inducing third parties to express illegal preferences."[119] Because Roommates required subscribers to provide information that violated housing discrimination laws—sexual orientation, gender, and family status—as a condition of accessing its service and provided "a limited set of pre-populated answers, Roommates [became] much more than a passive transmitter of information provided by others; it [became] the developer, at least in part, of that information."[120] The holding affirms that transition from an ICS to an ICP proscribes application of § 230 immunity because the provision

---

[114] *Id*. at 1123-24 (Although the *Carafano* decision utilized the terms interactive service provider (ISP) and interactive computer service (ICS) interchangeably, the distinction, for purposes of § 230 immunity, presented no semantic difference. Matchmaker.com was a website, and therefore constituted both an ISP and an ICS).

[115] *See also,* Batzel v. Smith, 333 F.3d 1018, 1020-21 (9th Cir. 2003) (granting § 230 immunity for an ICS operator who took affirmative steps to edit, review, and determine whether to publish the alleged defamatory content on the ICS website and listserv).

[116] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).

[117] *Id*. at 1161.

[118] *Id*. at 1162.

[119] *Id*. at 1165.

[120] *Id*. at 1166.

"provides immunity only if the interactive computer service [(ICS)] does not 'creat[e] or develop[ ]'" the information 'in whole or in part.'"[121]

The gravamen of the Ninth Circuit's decision in *Roommates.com* concerned its definition of *development*, such that an ICS *develops* third party content "if it contributes materially to the alleged illegality of the conduct."[122] The *Roommates.com* decision received significant attention, with one legal scholar branding it "the most significant deviation from the *Zeran* line of cases"[123] and another predicting that the decision would embolden plaintiffs to capitalize on the opinion's numerous ambiguities and produce inconsistent court decisions.[124] As a result, the once clear test from *Zeran* for distinguishing between an ICS and an ICP became obscured with other courts following suit in proscribing application of § 230 immunity.[125]

In 2009, the Ninth Circuit issued another opinion in the wake of *Roommates.com* denying § 230 immunity to a website. In *Barnes v. Yahoo!, Inc.*, Barnes brought suit against Yahoo for promising to remove a defamatory posting about the plaintiff and failing to do so.[126] Barnes' former boyfriend created false profiles containing nude photographs and open solicitations to engage in sexual intercourse.[127] The former boyfriend used the fake profiles to impersonate Barnes in online chatrooms and provided Barnes' contact information and physical addresses, which resulted in Barnes receiving emails, phone calls, and personal visits with the expectation of sex.[128] Barnes contacted Yahoo requesting removal of the false profiles over the course of several months.[129] During this period, a Yahoo executive verbally confirmed that the profiles would be taken down; however, this did not occur until Barnes filed a lawsuit against Yahoo.[130]

---

[121] *Id*. at 1166 (quoting 47 U.S.C. § 230(f)(3)).

[122] *Id*. at 1167-68.

[123] Diane J. Klein & Charles Doskow, *Housingdiscrimination.com?: The Ninth Circuit (Mostly) Puts Out the Welcome Mat for Fair Housing Act Suits Against Roommate-Matching Websites*, 38 GOLDEN GATE L. REV. 329, 377 (2008).

[124] Eric Goldman, *Roommates.com Denied230 Immunity by Ninth Circuit En Banc (With My Comments)*, TECH. & MKTG. L. Blog (Apr. 3, 2008), http://blog.ericgoldman.org/archives/2008/04/roommatescom_de_1.htm.

[125] *See* Doe v. SexSearch.com, 551 F.3d 412 (6th Cir. 2008) (holding that § 230 did not immunize a dating service from civil suit by an adult plaintiff who was arrested after having sexual relations with a fourteen-year-old met on the site when the minor claimed to be eighteen); *see* FTC v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009) (holding that § 230 did not immunize defendant website where it converted legally protected records from confidential material to publicly exposed information and therefore "developed" content because it facilitated the transaction).

[126] Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).

[127] *Id*. at 1098.

[128] *Id*.

[129] *Id*. at 1099.

[130] *Id*.

The Ninth Circuit addressed the application of § 230 immunity by evaluating the statutory language of the provision.[131] By coalescing subsections 230(e)(3) and 230(c)(1), the Ninth Circuit determined that § 230 only immunizes against liability when: "(1) a provider or user of an *interactive computer service* [(ICS)] (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another *information content provider* [(ICP)]."[132] This three-pronged test would later be recognized as the *Barnes Test*.

The Ninth Circuit held that § 230 immunized Yahoo against Barnes' negligent removal claim, but not her promissory estoppel claim.[133] The negligent removal claim was found unpersuasive because "removing content is something publishers do, and to impose liability on the basis of such conduct necessarily involves treating the liable party as a publisher of content it failed to remove[,]" which is exactly what § 230 is intended to prevent.[134] In contrast, the promissory estoppel claim arose from Yahoo's unfulfilled promise, and therefore, § 230 did not apply.[135] Judge O'Scannlain reasoned that "[c]ontract liability here would come not from Yahoo!'s publishing conduct, but from Yahoo!'s manifest intention to be legally obligated to do something, which happens to be removal of material from publication."[136]

The *Barnes* decision affirmed that: (1) "neither this subsection nor any other declares general immunity from liability deriving from third-party content" because "to provid[e] immunity every time a website uses data initially obtained from third parties would eviscerate [the CDA],"[137] and (2) § 230 immunity does not apply if the claims do not relate to the publication of user-generated content.[138]

---

[131] *Id*. at 1100.

[132] *Id*.

[133] *Id*. at 1107.

[134] *Id*. at 1103.

[135] *Id*.

[136] *Id*.

[137] *Id*. at 1100 (quoting *Roommates.com*, 521 F.3d at 1100).

[138] *Id*. at 1109 (quoting *Chi. Lawyers' Comm. For Civil Rights*, 519 F.3d at 669) (internal quotation marks omitted); *see*, *e.g., Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016) (holding that § 230 did not immunize a website from a negligent failure to warn claim where plaintiff had a 'special relationship' with the website and alleged the website had actual knowledge that some of its users were engaged in a rape scheme, plaintiff was raped as result of the scheme, and the website failed to warn plaintiff and other users); HomeAway.com, Inc. v. City of Santa Monica, 918 F.3d 676 (9th Cir. 2019) (holding that § 230 did not immunize defendant website from complying with a local short term rental ordinance requiring transactions occurring on defendant's website to involve only licensed properties).

IV. *DYROFF*: THE CORRECT LEGAL OUTCOME AND A BROADENING OF § 230 IMMUNITY

A. THE NINTH CIRCUIT CORRECTLY FINDS ULTIMATE SOFTWARE NOT LIABLE

It would be easy to blame the Ninth Circuit's § 230 jurisprudence and its broad application of immunity for providing Ultimate Software a free pass to walk away from the drug-related tragedy in *Dyroff*, but this would be the incorrect analysis. The *Dyroff* decision is an efficient distillation of existing case law and application of the *Barnes Test*.[139] Much of the rationale in *Dyroff* comes from the Ninth Circuit's prior decisions in *Carafano* and *Roommates.com*. Ultimate Software neither created nor developed its own content, and even if it had, it could have retained immunity so long as it was not the specific content at issue.[140] Similar to *Carafano*, the illegal content of Greer's post did not come from Ultimate Software, but from Greer himself, and the content of the reply post came from Castro, his drug dealer.[141] And unlike in *Roommates.com*, Ultimate Software did not require Greer to create illegal content as condition of using Experience Project.[142] In addition, Ultimate Software's push notification and group recommendation algorithms did not develop or materially contribute to the illegal content in Greer's posts.[143] In contrast to *Roommates.com*, Ultimate Software's algorithmic manipulation of user generated content only facilitated communication and the content of its users. The purpose of the website functions was to accomplish a specific task or action, much like a cog in a machine, and therefore cannot constitute content created or developed by Ultimate Software.

Although Dyroff aimed at pleading around § 230, there was no legal support for her arguments that Ultimate Software colluded with drug dealers and owed Greer a duty of care. Unlike *J.S. v. Village Voice Media Holdings, LLC*, Ultimate Software did not have a specific section for illegal activity that required its own particular posting requirements.[144]

---

[139] *See Barnes*, 570 F.3d at 1100-01 ("(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider").

[140] *Carafano*, 339 F.3d at 1124.

[141] *Dyroff*, 17-CV-05359-LB, 2017 WL 5665670, at *3.

[142] *Roommates.com*, 521 F.3d at 1166.

[143] *See id*. at 1175; *see also Kimzey*, 836 F.3d at 1269 n.4 (The material contribution test makes a "crucial distinction between, on the one hand, taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable").

[144] *See* J.S. v. Village Voice Media Holdings, LLC, 184 Wash. 2d 95 (2015) (en banc) (holding that plaintiffs sufficiently alleged website operators helped develop illegal content by requiring

While the Ninth Circuit highlights Ultimate Software's anonymity polices and advocacy of Internet privacy,[145] these are not the strongest reasons to dismiss the collusion argument. Anonymity and privacy are policies equally shared by social media giants like Facebook and dark web markets like Silk Road.[146] A better reason, which the decision points out, is Ultimate Software's burden of law enforcement information requests, which does not plausibly support collusion with drug dealers.[147] Equally, Dyroff's duty of care and failure to warn theories of liability could only have found solid ground if Greer had a *special relationship* with Ultimate Software, and there was actual knowledge of illegal activity.[148] This was not the case for Greer. No special relationship existed between Ultimate Software and Greer because of the anonymity and privacy policies employed, and no facts supported that Ultimate Software had actual knowledge of illegal activity.[149] Further, the website's push notifications and recommendation algorithms did not make Greer worse off than any other user of the website because these functions were applied to all users.[150] This reasoning is consistent with *Carafano*, where § 230 immunity is not lost because the opportunity for creation of illegal and legal content are equally available.[151]

Although the Ninth Circuit correctly applied its § 230 jurisprudence in finding Ultimate Software immune from liability, it did not adequately define the scope of term *content neutral*, resulting in a holding that implicitly immunizes *any* manipulation of third-party content facilitating communication or user content that does not materially contribute to the illegality of content.

B. THE SHIELD BROADENS FOR MANIPULATION OF THIRD-PARTY CONTENT

The term *content-neutral* applies where specific website functions or tools may give rise to unlawful content but do not result in develop-

users to disclose information into its "escort" section that encouraged sexual exploitation of children and therefore were not immune from liability under § 230).

[145] *Dyroff*, 934 F.3d at 1099-100.

[146] *See generally* Aditi Kumar and Eric Rosenbach, *The Truth about the Dark Web*, 53 FIN. & DEV. 22 (2019), https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf.

[147] *Dyroff*, 934 F.3d at 1099-100.

[148] *See Doe*, 824 F.3d 846 (holding that § 230 did not immunize a website from a negligent failure to warn claim where plaintiff had a 'special relationship' with the website and alleged the website had actual knowledge that some of its users were engaged in a rape scheme, plaintiff was raped as result of the scheme, and the website failed to warn plaintiff and other users).

[149] *Dyroff*, 934 F.3d at 1100.

[150] *Dyroff*, 934 F.3d at 1101.

[151] *Carafano*, 339 F.3d at 1123-24.

ment of content for purposes of § 230 immunity, so long as there is no material contribution by an ICS to the content at issue.[152] For example, an ICS that provides the means of searching within user data, sending email notifications to users, and making grammatical revisions of user posts, retains § 230 immunity so long as those *content-neutral* tools do not materially contribute to the illegality of the content.[153] However, the *Dyroff* decision leaves open the door for varied interpretation of a *content neutral* test by failing to define its scope, particularly in the context of algorithmic manipulation of user data. Other courts have been more explicit in finding algorithmic manipulation of user data *content-neutral* if the ICS handled legal and illegal content identically.[154] Instead, the *Dyroff* decision simply lumps algorithmic manipulation of user content into the *Roommates.com* exception where no liability occurs without material contribution. While *Dyroff* is a convenient and legally tenable decision, it is not particularly helpful for future courts tasked with applying § 230 immunity to algorithmic manipulation of user content.

Additionally, the *Dyroff* decision uses the terms *content neutral tools*, *content-neutral functions*, and *content-neutral fashion* in similar capacities and without distinguishing among them.[155] Whether a *content-neutral* tool, function, and fashion are one in the same is not clear and exacerbates the uncertainty in the context of algorithmic manipulation of user content. Moreover, the court utilized the *content-neutral* language that supported the § 230 defense to rationalize its rejection of Dyroff's duty of care claim.[156] The result of conflating the duty of care claim with the undefined *content-neutral* terminology is an implicit preclusion of any duty of care workaround to § 230, so long as an ICS remains *content-neutral*.[157]

In summary, the Ninth Circuit reached a legally tenable conclusion, but employed semantically problematic terms without adequately defining their meaning or scope. As a consequence, *Dyroff* opens the door to

---

[152] *Roommates.com*, 521 F.3d at 1169.

[153] *Id.* (An ICS that provides the means of searching within user data and sending email notifications to users and that makes grammatical revisions of user posts retains § 230 immunity so long as the ICS does not materially contribute to the alleged illegality).

[154] *See* Marshall's Locksmith Service Inc. v. Google, LLC, 925 F.3d 1263, 1271 (2019).

[155] *See Dyroff*, 934 F.3d at 1096-1100 ("Ultimate Software, as the operator of Experience Project, is immune from liability under the CDA because its functions, including recommendations and notifications, were *content-neutral tools* used to facilitate communications . . . Ultimate Software owed Greer no duty of care because Experience Project's features amounted to *content-neutral functions* that did not create a risk of harm. . . No website could function if a duty of care was created when a website facilitates communication, in a *content-neutral fashion*, of its users' content") (emphasis added).

[156] *Dyroff*, 934 F.3d at 1101 ("No website could function if a duty of care was created when a website facilitates communication, in a content-neutral fashion, of its users' content").

[157] *See supra* note 147, at 66.

varied interpretations in future decisions, implicitly forecloses an avenue of recourse against ICSs where a duty of care may have existed, and collectively and perhaps unintentionally broadens § 230's immunity protections.

CONCLUSION

The *Dyroff* decision is a reminder of the broad scope of § 230 immunity. The Ninth Circuit arrived at the correct legal conclusion, but failed to provide an explanation or examples of what does and what does not constitute a *content neutral* tool. The *Dyroff* decision obscures what is *neutral* for purposes of § 230 immunity, and fosters greater opportunity for ICSs to fall under § 230's shield where any non-material algorithmic manipulation of user data enabling user-to-user communication is *content neutral*, regardless of any associated illegality.

Nevertheless, the CDA remains viable and relevant today as a safeguard for First Amendment speech on the Internet. However, current Internet development is staggeringly more sophisticated than when the CDA and § 230 were enacted in 1996. Modern Internet companies employ thousands of humans and artificial intelligence-based methods to moderate offensive and illegal content.[158] The once broad shield designed to foster growth and development of the nascent Internet has become antiquated and requires updating to reflect modern realities. Until Congress revisits the CDA and § 230, decisions like *Dyroff,* although legally correct, are likely to engender varied decisions when undefined terminology is used that unnecessarily broadens application of § 230 immunity. The Internet is no longer a child of the '90s needing congressional helicopter-parenting. It is time for the Internet to be more accountable to its users and work towards preventing tragedies like *Dyroff* by using its existing moderation tools to identify and to prevent facilitating illegal conduct.

[158] *See Social media's struggle with self-censorship*, THE ECONOMIST (Oct. 22, 2020), https://www.economist.com/briefing/2020/10/22/social-medias-struggle-with-self-censorship.