THE CASE FOR A CDA SECTION 230 NOTICE-AND-TAKEDOWN DUTY

Michael L. Rustad* & Thomas H. Koenig**

TABLE OF CONTENTS

* Michael L. Rustad, Ph.D., J.D., L.L.M. is the Thomas F. Lambert Jr. Professor of Law at Suffolk University & Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School. He is the author of more than sixty law review articles in publications such as the Northwestern University Law Review, Iowa Law Review, Indiana Law Journal, North Carolina Law Review, and the Wisconsin Law Review. His most recent books are GLOBAL INFORMATION TECHNOLOGIES: ETHICS AND THE LAW (2nd edition; 2023) (with Koenig), GLOBAL INTERNET LAW IN A NUTSHELL (5th ed., 2022), and THE GLOBAL INTERNET HORNBOOK (4th ed. 2022). He is the editor of COMPUTER CONTRACTS: NEGOTIATING, DRAFTING (2023 edition). He has been cited 4,100 times on Google Scholar and almost 2000 times on Lexis/Nexis.

** Thomas H. Koenig is a professor emeritus at Northeastern University in Boston. He was a fellow at Harvard University Law School, a Fulbright Fellow at the University of Belgrade (Serbia) Law School, and has served as a visiting faculty member at Tufts University, Brown University, SUNY at Buffalo, and in Hungary's program on Post-Soviet Change Management.

We thank the staff of Volume 22 of the Nevada Law Journal for their careful edits of this Article.

INTRODUCTION

Section 230 of the Communications Decency Act of 1996 (CDA Section 230) "is regularly cited as the most important law supporting the Internet, e-commerce and the online economy."[1] CDA Section 230, part of Title V of the Telecommunications Act of 1996, confers a wide-ranging shield against defamation liability that immunizes any "interactive computer service" that publishes, hosts, or distributes information provided by third-party users.[2] Congress enacted CDA Section 230 to protect the 1990s' fledgling Internet access providers, such as America Online, CompuServe, and Prodigy, from having to defend against a predicted flood of defamation lawsuits launched by those injured by third-party postings on their services. "[I]f a new Internet startup needed to be prepared to defend against countless lawsuits on account of its users' speech, startups would never get the investment necessary to grow and compete with large tech companies."[3] Congress declared, "It is the policy of the United States . . . to promote the continued development of the Internet and other interactive computer services and other interactive media."[4] CDA Section 230 states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[5]

In the quarter century since Congress enacted CDA Section 230, this liability defense has played a crucial role in developing the contemporary World Wide Web.[6] Courts have expanded CDA Section 230's liability shield to en-

---

[1] Jeffrey D. Neuburger, *United States: Commerce Dept. Petitions FCC to Issue Rules Clarifying CDA Section 230*, MONDAQ (Aug. 7, 2020), https://www.mondaq.com/unitedstates/social-media/971694/commerce-dept-petitions-fcc-to-issue-rules-clarifying-cda-section-230 [https://perma.cc/JQ85-2FYE].

[2] 47 U.S.C. § 230(a)(1). The two immunity provisions of Section 230 are:

> [1] 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. . . . [and] [2] No provider or user of an interactive computer service shall be held liable on account of . . . 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.

Id. § 230(c)(1)–(2).

[3] Elliot Harmon, *It's Not Section 230 President Trump Hates, It's the First Amendment*, ELEC. FRONTIER FOUND. (Dec. 9, 2020), https://www.eff.org/deeplinks/2020/12/its-not-section-230-president-trump-hates-its-first-amendment [https://perma.cc/EQ84-GS9B].

[4] 47 U.S.C. § 230(b)(1).

[5] 47 U.S.C. § 230(c)(1).

[6] U.S. DEP'T OF JUST., SECTION 230—NURTURING INNOVATION OR FOSTERING UNACCOUNTABILITY? KEY TAKEAWAYS AND RECOMMENDATIONS 1 (2020), https://www.justice.gov/file/1286331/download [https://perma.cc/DWQ4-BH5X].

compass all online intermediaries, not just Internet Service Providers (ISPs). In 2023, powerful Internet gatekeepers, such as Google, YouTube, Facebook, and Twitter, no longer require such a broad immunity and should have a duty to takedown illegal content, which is the law in the European Union. The United States Justice Department has called for downsizing CDA Section 230 because the "combination of significant technological changes since 1996 and the expansive interpretation that courts have given Section 230 . . . has left online platforms both immune for a wide array of illicit activity on their services and free to moderate content with little transparency or accountability."[7]

The National Association of Attorneys General calls on Congress to scale back CDA Section 230 because it enables online criminal activity such as "online black market opioid sales, ID theft, deep fakes," and election meddling.[8] In May of 2020, former President Trump issued an Executive Order limiting CDA Section 230's scope, contending that many websites should lose their legal immunity because of their pattern of disfavoring conservative viewpoints and deleting accounts without warning.[9]

In our 2002 book, *In Defense of Tort Law*, we predicted that new Internet torts would evolve to protect consumers in cyberspace. We were mistaken. Today, the field of cybertorts is largely limited to intentional torts against a primary wrongdoer. Negligence and strict liability torts against Internet intermediaries have not evolved because CDA Section 230 blocks them.[10] The courts have consistently construed CDA Section 230 to eliminate all tort liability against websites, search engines, and other online intermediaries arising out of third-party postings on their services. The result is that large gatekeepers such as Facebook, Google, Twitter, and YouTube have no duty to respond to takedown notices, even if the deplorable content is a continuing tort or crime.

In 2018, Congress created the first exception to CDA Section 230's broad liability shield "in the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, commonly known as FOSTA. Post-FOSTA, Section 230 immunity will not apply to bar claims alleging violations of certain sex trafficking laws."[11] We propose that Congress recognize the duty of platforms to remove or disable content constituting ongoing torts or crimes hosted by giant "gate-

---

[7] *Id*.

[8] John Lucas, *AG Moody Joins with Other Attorneys General to Urge Congress to Stop Protecting Illegal Activity on the Net*, CAPITOLIST (May 23, 2019), https://thecapitolist.com/ag-moody-joins-with-other-attorneys-general-to-urge-congress-to-stop-protecting-illegal-activity-on-the-net [https://perma.cc/27BE-26PU].

[9] Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (May 28, 2020).

[10] Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertorts for the Internet of Things*, HARV. L. REC. (Nov. 17, 2016), http://hlrecord.org/rebooting-cybertorts-for-the-internet-of-things [https://perma.cc/L6SS-3B8W].

[11] VALERIE C. BRANNON, CONG. RSCH. SERV., LSB10306, LIABILITY FOR CONTENT HOSTS: AN OVERVIEW OF THE COMMUNICATION DECENCY ACT'S SECTION 230 (2019), https://fas.org/sgp/crs/misc/LSB10306.pdf [https://perma.cc/NXV8-RSKV].

keeper" entities, such as Facebook, YouTube, Twitter, and Google. "The legal protections provided by CDA 230 are unique to U.S. law; European nations, Canada, Japan, and the vast majority of other countries do not have similar statutes on the books."[12]

In this Article, we will argue that CDA Section 230 should not be burned down, but rather updated to address platforms hosting ongoing torts and crimes with no redeeming First Amendment interest, such as revenge porn, terrorist incitement and instructions, or the promotion of fraudulent COVID-19 cures. Our CDA reform creates a notice-and-takedown (NTD) regime for illegal content that has no purpose other than harming victims who currently have no means to get it disabled. Our reform would give content creators and other posters a legal right to dispute takedown and require putback of content erroneously deleted or arguably protected by the First Amendment.

The European Commission (EC) contends that enormous gatekeepers pose the greatest dangers "in the dissemination of illegal content and societal harms."[13] The EC has proposed that platforms reaching more than ten percent of the 45 million consumers in Europe be subject to the gatekeeper's rules mandating notice-and-takedown.[14]

Our CDA online intermediary proposal for content constituting ongoing torts, crimes, or other illegal content synthesizes some provisions of the Digital Millennium Copyright Act (DMCA) and the European Union's (EU) Digital Services Act (DSA). Harmonizing important U.S. and EU takedown standards would be a major step toward developing a global standard for the liability of Internet intermediaries.

The first two parts of this Article will demonstrate the need to require online intermediaries to remove content constituting ongoing cybertorts and other illegal content. Part I will provide a brief history of CDA Section 230 and how courts have expanded the statute from a modest liability shield, only applicable to defamation, to an all-encompassing defense that protects all online intermediaries against all third party cybertorts.

Part II will make the case for CDA Section 230 modernization to address the problem of Internet platforms having no duty to remove unlawful third party content. Since 1996, Google, Facebook, YouTube, and other powerful online

---

[12] *Section 230 of the Communications Decency Act: 47 U.S.C. § 230, a Provision of the Communication Decency Act*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/QYG9-MBA7].

[13] European Commission, *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*, EUR. COMM'N, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment [https://perma.cc/5L99-2YAT].

[14] European Commission, *Digital Markets Act: Ensuring Fair and Open Digital Markets*, EUR. COMM'N (Dec. 15, 2020), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets [https://perma.cc/3Q4Y-28AT].

intermediaries have created a multi-billion dollar, cross-border electronic marketplace. Cybercriminals increasingly deploy these networks as vehicles for disseminating illegal content, selling dangerously defective goods, and spreading fraudulent health information. "ISPs are generally in the best position to mitigate damages from online fraudulent schemes, website defamation, and other information-based torts by taking down objectionable content."[15] Section 230's liability shield results in many unjust outcomes.

Part III will present our ambitious reform of CDA Section 230 by establishing a limited NTD obligation to remove tortious or other illegal content that endangers the public. Our CDA Section 230 NTD proposal adapts provisions of Section 512 of the DMCA that requires ISPs to takedown content that infringes a third party's copyright.[16] As with the DMCA, service providers will have a duty to remove ongoing tortious content provided they have written or digital notice. As with Europe's DSA, our CDA Section 230 reform enables content creators whose material has been removed to appeal adverse decisions by websites and other platforms in federal court.

The European Union's Digital Services Act went into effect on November 16, 2022, updating the European Union's (EU) e-Commerce Directive's Internet intermediary rules.[17] Currently, the EU's e-Commerce Directive provides a general guideline for online intermediaries. In contrast, the recently enacted DSA establishes a comprehensive legal framework, adapting online intermediary law for social media, search engines, online marketplaces, and other online services that operate in the EU. Paralleling the EU's Digital Services Act,[18] our reform provides that U.S. online intermediaries are only liable for failing to delete content constituting ongoing torts or crimes on their services if they have "actual knowledge" and fail to expeditiously disable access to the posted illegal content. Harmonizing U.S. law with the EU's DSA will be an important step toward developing global Internet intermediary rules for illegal content. Modeling the specifics of notice-and-takedown of ongoing U.S. cybertorts on the

---

[15] Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 339 (2005).

[16] 17 U.S.C. §512(i)(1)(A).

[17] The Digital Services Act together with the Digital Markets Act are intended as a comprehensive package of measures for the provision of digital services in the European Union and seek to address the challenges posed by online platforms. In the Digital Services Act, which is underpinned by this impact assessment report, the intervention focuses on deepening the single market for digital services and establishing clear responsibilities for online platforms as well as other intermediary services to protect their users from the risks they pose, such as illegal activities online and risk to their fundamental rights. The Digital Markets Act complements these provisions and focuses on the gatekeeper role and unfair practices by a prominent category of online platforms.

European Commission Staff Working Document Impact Assessment, at 5, COM (2020) 825 final (Dec. 15, 2020); *see also* European Commission, *The Digital Services Act Package*, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[18] European Commission, *supra* note 14.

EU's comprehensive rules for large gatekeepers will result in a workable global Internet intermediary standard for dealing with illegal content, while protecting the right of free expression.

I. CDA SECTION 230 ENABLED INTERNET DEVELOPMENT

A. Why Congress Enacted CDA Section 230

Prior to Congress enacting CDA Section 230 in 1996, U.S. courts were sharply divided as to whether Internet service providers were liable for the defamatory postings of third-party users.[19] In *Cubby, Inc. v. CompuServe, Inc.*,[20] a New York federal court ruled that CompuServe, an online service provider, was not liable for statements published by third parties on its service as it did not have an affirmative, active role in creating the posting.[21]

The *Cubby* court stated, "CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so."[22] CompuServe was entitled to First Amendment protection as a "distributor," subject to liability only if it knew or had reason to know of the allegedly defamatory statements.[23] The court concluded that CompuServe had no editorial control over the publication at issue and it would not have been practical for it to assess every publication it carried to determine whether there was defamatory content.[24]

CompuServe could not be held liable for harm resulting from third-party content absent a threshold showing that it "knew or had reason to know" of the content and its harmful nature.[25] The *Cubby* court reasoned that the ISP could only be liable for torts if the plaintiff proved that it had actual or constructive knowledge of defamatory materials.[26] Under this decision, distributors were classified as mere conduits, akin to telegraph and telephone companies, because

---

[19] Stratton Oakmont, Inc. v. Prodigy Servs Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *7, *10 (N.Y. Sup. Ct. May 24, 1995) (finding ISP liable for defamatory statements because it exercised some editorial control and did not promptly take down statement made on Internet forum labeling company's stock option as fraudulent and its actions as criminal). Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140–41, 143 (S.D.N.Y. 1991) (finding that ISP was not liable for statements made in electronic bulletin board since it did not exercise editorial control).

[20] *Cubby, Inc.*, 776 F. Supp. at 135.

[21] *Id.* at 141.

[22] *Id.* at 140.

[23] *Id.* at 141.

[24] *Id.* at 140.

[25] *Id.* at 140–41.

[26] *Id.* at 141.

they have no liability for content created by others unless the ISP has specific knowledge of the defamatory messages.

In 1995, a New York court classified a social media platform as a publisher rather than distributor, thus creating conflicting Internet intermediary liability standards.[27] In *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[28] a New York trial court held that online service providers were potentially liable for the speech of third-party users who posted defamatory statements on their service. Prodigy's computer network had "at least two million subscribers who communicate[d] with each other and with the general subscriber population on PRODIGY's bulletin boards."[29] "Money Talk" was then "the leading and most widely read financial computer bulletin board in the United States, where members [could] post statements regarding stocks, investments and other financial matters."[30] Prodigy portrayed itself as a "family oriented computer network" that "exercised editorial control over the content of messages posted on its computer bulletin boards."[31]

The New York trial court decided a case where an anonymous poster on Prodigy's Money Talk bulletin wrote that Stratton Oakmont, a New York securities investment banking firm (and its officer), had committed criminal and fraudulent acts in connection with the initial public offering of a stock.[32] The court ruled that Prodigy was a publisher that had made a "conscious choice, to gain the benefits of editorial control," thus opening itself up to "greater liability than CompuServe and other computer networks that make no such choice."[33] The court found there was "no doubt that at least for the limited purpose of monitoring and editing the 'Money Talk' computer bulletin Board, PRODIGY directed and controlled Epstein's actions" and was therefore liable for the posted defamatory statements.[34]

---

[27] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *1 (N.Y. Sup. Ct. May 24, 1995).

[28] *Id.* at *1.

[29] *Id.* at *3.

[30] *Id.*

[31] *Id.* at *2.

[32] *Id.* at *1–2.

> At issue in this case are statements about Plaintiffs made by an unidentified bulletin board user or "poster" on PRODIGY's "Money Talk" computer bulletin board on October 23rd and 25th of 1994. These statements included the following:
>
> (a) STRATTON OAKMONT, INC. ("STRATTON"), a securities investment banking firm, and DANIEL PORUSH, STRATTON's president, committed criminal and fraudulent acts in connection with the initial public offering of stock of Solomon-Page Ltd.;
>
> (b) the Solomon-Page offering was a "major criminal fraud" and "100% criminal fraud";
>
> (c) PORUSH was "soon to be proven criminal"; and,
>
> (d) STRATTON was a "cult of brokers who either lie for a living or get fired.

[33] *Id.* at *5.

[34] *Id.* at *7.

The Congressional Conference Report on CDA Section 230, which was adopted as Title V of the Telecommunications Act of 1996, specifically states:

> [T]his section provides "Good Samaritan" protections from civil liability for providers or users of an interactive computer service for actions to restrict or enable restriction of access to objectionable online material. . . . [O]ne of the specific purposes of [section 230] is to overrule *Stratton–Oakmont* [*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.[35]

Section 230(c)(1) of the CDA, entitled "Protection for private blocking and screening of offensive material," states that "[n]o provider or user of an interactive computer service[36] shall be treated as the publisher or speaker of any information provided by another information content provider."[37] "Section 230 of the Act, also known as the Cox–Wyden Amendment ('the Amendment'), protects certain internet-based actors from certain kinds of lawsuits."[38] "The statute's 'policy' includes the promotion of interactive computer services and the 'vibrant and competitive free market' for such services, as well as the encouragement of 'blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.' "[39] "Congress sought to encourage websites to make efforts to screen content without fear of liability," and "to permit the continued development of the internet with minimal regulatory interference."[40]

The CDA's "'Good Samaritan' provisions were intended to ensure that even if online service providers did exercise some limited editorial control over the content posted on their sites, they would not thereby be subject to publisher liability."[41] Congress recognized that the Internet offers "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[42]

Representatives Chris Cox and Ron Wyden added Section 230 as an amendment to the CDA "to encourage the unfettered and unregulated develop-

---

[35] Doe v. America Online, Inc., 783 So. 2d 1010, 1014 (Fla. 2001).

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

[37] *Id*. § 230(c)(1).

[38] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099 (9th Cir. 2009).

[39] *Id*. (quoting 47 U.S.C. § 230(b)(1)–(2), (4)–(5)).

[40] Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 19 (1st Cir. 2016).

[41] VALERIE C. BRANNON, CONG. RSCH. SERV., LSB10306, LIABILITY FOR CONTENT HOSTS: AN OVERVIEW OF THE COMMUNICATION DECENCY ACT'S SECTION 230 (2019), https://sgp.fas.org/crs/misc/LSB10306.pdf [https://perma.cc/MNP8-WYJ7].

[42] 47 U.S.C. § 230(a)(3).

ment of free speech on the Internet, and to promote the development of e-commerce."[43] Chris Cox explained CDA Section 230's purpose:

> Without Section 230, social media platforms would be exposed to lawsuits for users' reviews of products, restaurants, books, and movies. Airbnb and HomeAway would be exposed to lawsuits for users' negative comments about a rented home. Any service that connects buyers and sellers, workers and employers, content creators and website visitors, or victims and victims' rights groups—or provides any other interactive engagement opportunity one can imagine—could not continue to function on the Internet displaying user-generated content.[44]

An Arizona federal court stated that Congress enacted CDA Section 230 "[t]o avoid unduly burdening the continued development of the Internet . . . . 'Whether wisely or not,' Congress 'made the legislative judgment to effectively immunize providers of computer services from civil liability in tort with respect to materials disseminated by them but created by others.' "[45]

By its express terms, CDA Section 230(c)(1) "protects websites from liability [under state or local law] for material posted on the[ir] website[s] by someone else."[46] This immunity for third-party information (or content) disappears if the website operator is responsible, in whole or in part, for the creation or development of the information.[47] The CDA makes website operators immune from liability for third-party information (or content) unless the website operator "is responsible, in whole or in part, for the creation or development of [the] information."[48] Websites are not liable for user-generated content that they did not create. The CDA states, "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."[49]

The Ninth Circuit developed a three-pronged test for Section 230 immunity, which exists if "(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."[50] Website operators are immune from liability for third-party information

---

[43] Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003).

[44] Brief of Chris Cox, Former Member of Congress and Co-Author of CDA Section 230, and Netchoice as *Amici Curiae* in Support of Plaintiffs and Reversal at 7, Homeaway.com, Inc. v. City of Santa Monica, 918 F.3d 676 (9th Cir. Mar. 13, 2019) (No. 18-55367).

[45] United States v. Lacey, No. CR-18-00422-PHX-SMB, 2020 U.S. Dist. LEXIS 2645, at *9–10 (D. Ariz. Jan. 7, 2020).

[46] Doe v. Internet Brands, Inc., 824 F.3d 846, 850 (9th Cir. 2016); *see also* 47 U.S.C. § 230(e)(3).

[47] Communications Decency Act, 47 U.S.C. § 230(c)(1).

[48] *Id*. § 230(f)(3).

[49] *Id*. § 230(c)(1).

[50] Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, 1097 (9th Cir. 2019) (quoting Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100–01 (9th Cir. 2009)).

unless the website operator "is responsible, in whole or in part, for the creation or development of [the] information."[51] "Section 230(c) ensures that as a 'Good Samaritan,' an interactive computer service provider may remove some objectionable third-party content from its website without fear of subjecting itself to liability for objectionable content it does not remove."[52] Online intermediaries do, however, have liability for their own direct torts, such as personal property torts, the invasion of privacy, negligently enabling the spread of viruses, or failing to prevent cybercrimes.[53]

B. How Courts Overextended CDA Section 230

The original purpose of the CDA was to shield websites from publishers' liability for defamation. In the past two decades, federal courts have stretched Section 230's immunity beyond publisher defamatory liability to cover every conceivable tort, thus violating a basic principle that a responsible website is an answerable one.[54] The liability shield currently creates a broad immunity for websites, search engines, chatroom, blogs, and countless other Internet institutions from liability for any third-party tortious postings. As a result, cybertort victims have no meaningful remedy against website hosts that enable continuing Internet-related torts and crimes because websites and Internet platforms have no liability for third party postings.

In *Blumenthal v. Drudge*,[55] commentator Matt Drudge issued a false report on AOL that Sidney Blumenthal, an aide to President Clinton, had a history of

---

[51] 47 U.S.C. §§ 230(c)(1), (f)(3).

[52] Daniel v. Armslist, LLC, 926 N.W.2d 710, 718 (Wisc. 2019) (quoting Chi. Laws.' Comm. for Civ. Rts. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666, 669–70 (7th Cir. 2008)).

[53] Rustad & Koenig, *supra* note 15, at 344.

When a consumer experiences financial loss, identity theft, or the malicious meltdown of their personal computer, the online cybercriminal almost always defaults or is not locatable. The primary wrongdoer is generally beyond the reach of jurisdiction, particularly because the ISP has no duty to aid in locating the origin of the illegal posting. Many consumer frauds, for example, originate in the new Russian Republics, which have become "a popular venue for innovative cyberscams involving credit card numbers stolen from websites." While repeat players enjoy a favorable legal environment, consumers have no recourse against web hosts, websites, or service providers that benefit from selling advertising or providing other services for cybercriminals. Consumers are left defenseless in cyberspace because immunized service providers are the only identifiable deep pocket. ISPs currently have no duty to police the Internet or to develop technologies to track down off-shore posters of objectionable materials.

Id. at 350–51.

[54] *Id.* at 371.

An activist judiciary, however, has radically expanded § 230 by conferring immunity on distributors. Section 230(c)(1) has been interpreted to preclude all tort lawsuits against ISPs, websites, and search engines. Courts have . . . haphazardly lump[ed] together web hosts, websites, search engines, and content creators into this amorphous category.

Id.

[55] Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

spousal abuse.[56] The court noted that AOL "affirmatively promoted Drudge as a new source of unverified instant gossip."[57] AOL had the authority under its agreement with Drudge to edit and remove Drudge's submissions, and yet it sought to take no responsibility for any damage Drudge might cause.[58] AOL paid royalties to Drudge for publishing the Drudge Report on its service.[59] Drudge later retracted the story, and AOL published the retraction on its service.

Blumenthal contended AOL should be liable for the defamatory communication even though he conceded that AOL was an interactive computer service. Blumenthal argued that Drudge was "not just an anonymous person who sent a message over the Internet" because of his license agreement with AOL.[60] Nevertheless, the court held that AOL was immune under CDA Section 230.[61] The plaintiff contended AOL's editorial role made it a content provider, divesting it of its Section 230 immunity because the ISP not only sponsored the site but also paid Drudge $3,000 monthly in royalties for publishing on the website.[62]

The *Blumenthal* court found that AOL was nevertheless entitled to CDA Section 230 immunity—even though it had the right to edit, update, manage, or even remove objectionable content in its agreement to publish the Drudge Report.[63] The court stated, "Congress has conferred immunity from tort liability as

---

[56] *Id*. at 46. ("The DRUDGE REPORT has learned that top GOP operatives who feel there is a double-standard of only reporting republican shame believe they are holding an ace card: New White House recruit Sidney Blumenthal has a spousal abuse past that has been effectively covered up.").

[57] *Id*. at 51.

[58] *Id*.

[59] *Id*. at 47. ("The agreement made the Drudge Report available to all members of AOL's service for a period of one year. In exchange, defendant Drudge received a flat monthly 'royalty payment' of $3,000 from AOL.").

[60] *Id*. at 51.

[61] *Id*. at 52–53.

[62] *Id*. at 51. ("Plaintiffs make the additional argument, however, that Section 230 of the Communications Decency Act does not provide immunity to AOL in this case because Drudge was not just an anonymous person who sent a message over the Internet through AOL. He is a person with whom AOL contracted, whom AOL paid $3,000 a month—$36,000 a year, Drudge's sole, consistent source of income—and whom AOL promoted to its subscribers and potential subscribers as a reason to subscribe to AOL.").

[63] *Id*. at 47–52. ("AOL has certain editorial rights with respect to the content provided by Drudge and disseminated by AOL, including the right to require changes in content and to remove it; and it has affirmatively promoted Drudge as a new source of unverified instant gossip on AOL. Yet it takes no responsibility for any damage he may cause. AOL is not a passive conduit like the telephone company, a common carrier with no control and therefore no responsibility for what is said over the telephone wires. Because it has the right to exercise editorial control over those with whom it contracts and whose words it disseminates, it would seem only fair to hold AOL to the liability standards applied to a publisher or, at least, like a book store owner or library, to the liability standards applied to a distributor. But Congress has made a different policy choice by providing immunity even where the interactive

an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even when the self-policing is unsuccessful or not even attempted."[64] The court's expansive interpretation of Section 230 protected AOL, even though in this case it closely resembled a content creator. Similarly, in *Ben Ezra, Weinstein, & Co. v. America Online Inc.*,[65] the Tenth Circuit concluded that "Congress clearly enacted § 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions."[66]

C. CDA Section 230 Shields All Internet Intermediaries from Cybertort Liability

In the next Section, we present compelling case studies showing how the CDA Section 230 liability shield enables illegal content to harm consumers, divesting them of any remedy against Internet intermediaries even if the primary wrongdoer is also beyond the reach of the law. "Torts in cyberspace arose out of e-mail, web site, or software distribution, rather than traditional categories of injury such as automobile accidents, slip and fall mishaps, premises liability, operating room malpractice, and injuries due to dangerously defective products."[67] Cybertorts must continually evolve to address new social and technological dangers, but, as we will show, Section 230 prevents cybertorts from evolving.[68]

1. Extending the Liability Shield to Distributors

At common law, defendants that "publicize another's libel may be treated in one of three ways: as primary publishers (such as book or newspaper publishers); as conduits (such as a telephone company); or as distributors (such as a book store, library, or news dealer)."[69] The common-law rule makes a distributor liable where it has knowledge of the facts and circumstances that are pro-

service provider has an active, even aggressive role in making available content prepared by others.").

[64] *Id.* at 52. ("In some sort of tacit *quid pro quo* arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted."). *Id.*

[65] Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc., 206 F.3d 980 (10th Cir. 2000).

[66] *Id.* at 986.

[67] Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 93 (2003).

[68] *Id.* at 77–86 (explaining term "legal lag" through sociologist William Ogburn's concept of cultural lag in which the various institutions of American society do not change at the same rate, thereby creating a "cultural lag" when one element has not yet accommodated to developments in another); *see* David Sanders & Jesse Dukeminier, Jr., *Medical Advance and Legal Lag: Hemodialysis and Kidney Transplantation*, 15 UCLA L. REV. 357, 371–80 (1968).

[69] Barrett v. Rosenthal, 112 Cal. App. 4th 749, 761 (Cal. Ct. App. 2003).

ducing clearly libelous activity, but takes no action to remove the material.[70] The California Supreme Court noted that "[r]ecognizing 'distributor' liability would have a dramatic impact on Internet service providers."[71]

Distributors (sometimes known as "secondary publishers"), whose ability to control defamatory speech lies somewhere between that of primary publishers and conduits, are subject to an intermediate standard of responsibility and may only be held liable as publishers if they know, or have reason to know, of the defamatory nature of matter they disseminate.[72] The Restatement Second of Torts explains:

> [A] news dealer is not liable for defamatory statements appearing in the newspapers or magazines that he sells if he neither knows nor has reason to know of the defamatory article. The dealer is under no duty to examine the various publications that he offers for sale to ascertain whether they contain any defamatory items. Unless there are special circumstances that should warn the dealer that a particular publication is defamatory, he is under no duty to ascertain its innocent or defamatory character. On the other hand, when a dealer offers for sale a particular paper or magazine that notoriously persists in printing scandalous items, the vendor may do so at the risk that any issue may contain defamatory language.[73]

While the express language of CDA Section 230 applies only to publishers, US courts have stretched Section 230 to encompass distributors. In *Zeran v. America Online, Inc.*,[74] a malicious anonymous poster instructed members of the public to call Kenneth M. Zeran to order merchandise displaying tactless and incendiary slogans celebrating the 1995 bombing of the Alfred P. Murrah Federal Court Building in Oklahoma City.[75] The anonymous post on America Online stated, "Those interested in purchasing the shirts were instructed to call 'Ken' at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats."[76]

An Oklahoma City radio announcer learned of the messages and mentioned "the message's contents on the air, attributed them to 'Ken' at Zeran's phone number, and urged the listening audience to call the number."[77] "After this ra-

---

[70] *See, e.g.*, Lerman v. Chuckleberry Publ'g, Inc., 521 F. Supp. 228, 235 (S.D.N.Y. 1981), reversed on other grounds, Lerman v. Flynt Distrib. Co., Inc., 745 F.2d 123, 142 (2d Cir. 1984) ("[D]istributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.").

[71] Barrett v. Rosenthal, 146 P.3d 510, 514 (Cal. 2006) (agreeing with the *Zeran* court that Congress did not intend to create such an exception to section 230 immunity).

[72] RESTATEMENT (SECOND) OF TORTS § 581(1) (AM. L. INST. 1977).

[73] *Id.* § 581 cmt. d.

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

[75] *Id.* at 329.

[76] *Id.*

[77] *Id.*

dio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents."[78] "Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home."[79] Zeran spoke with representatives of the radio station and AOL, as well as the local police that "surveilled his home to protect his safety."[80] "[A]n Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRXO made an on-air apology, the number of calls to Zeran's residence finally subsided to fifteen per day."[81]

Zeran filed suit against the radio station and filed a separate suit against AOL in an Oklahoma federal district court.[82] The district court transferred Zeran's suit to the Eastern District of Virginia, where the court granted AOL's motion to dismiss, and Zeran filed an appeal to the Fourth Circuit.[83] The court noted, "Zeran seeks to hold AOL liable for defamatory speech initiated by a third party."[84] The court stated that:

> [O]nce [Zeran] notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.[85]

AOL defended on the grounds that CDA Section 230 barred Zeran's action because the liability shield immunized service providers from liability for third-party postings.[86] The Fourth Circuit agreed, ruling that a service provider, such as AOL, was shielded from both publisher and distributor defamation lawsuits despite the fact that Section 230 only addresses publisher liability. The court reasoned that lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish or alter content—are barred by Section 230.[87] Courts interpreting CDA Section 230 have consistently considered critical to applying the statute the

---

[78] *Id*.
[79] *Id*.
[80] *Id*.
[81] *Id*.
[82] *Id*.
[83] *Id*. at 329–30.
[84] *Id*. at 330.
[85] *Id*.
[86] *Id*.
[87] *Id*. ("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. Specifically, § 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.").

concern that lawsuits could threaten the "freedom of speech in the new and burgeoning Internet medium."[88]

The *Zeran* court highlighted the objective of the CDA in shielding websites from liability for third-party content:

> The amount of information communicated via interactive computer services is . . . staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.[89]

The *Zeran* case was the precedent establishing that an online intermediary, such as a website, is under no obligation to disable information posted by third parties. After *Zeran*, the distinction between publishers and distributors on the Internet became non-existent. Websites and other service providers are not liable for the defamatory postings of third parties absent proof that they are content creators. Even more, U.S. courts have also expanded the Section 230 shield to immunize intermediaries for nearly every tort action.

2. Widening the No Liability Shield to Apply to All Intentional Torts

Sixteen years ago, we wrote that courts "have expanded § 230 far beyond Congress's original intent by immunizing ISPs and websites from distributor liability and virtually every other tort action."[90] Courts have expanded this "no liability" zone for Internet intermediaries even further since our *Washington Law Review* article.[91] In *Jones v. Dirty World Entertainment Recordings LLC*, Sarah J. Jones, a Cincinnati Bengals cheerleader and a public school teacher, filed a defamation action against *The Dirty*, an online tabloid, for anonymous postings about her.[92] "The website enables users to anonymously upload comments, photographs, and video, which Richie then selects and publishes along with his own distinct, editorial comments. In short, the website is a user-generated tabloid primarily targeting nonpublic figures."[93] An anonymous visitor to www.TheDirty.com submitted two photographs of Jones and a male companion and the following post:

> THE DIRTY ARMY: Nik, this is Sara J, Cincinnati Bengal Cheerleader. She's been spotted around town lately with the infamous Shayne Graham. She has also

---

[88] *Id.*

[89] *Id.* at 331.

[90] Rustad & Koenig, *supra* note 15, at 342–43.

[91] *See id.*

[92] Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 401, 403 (6th Cir. 2014).

[93] *Id.* at 401.

> slept with every other Bengal Football player. This girl is a teacher too!! You would think with Graham's paycheck he could attract something a little easier on the eyes Nik!"[94]

Richie also added caustic commentary augmenting the post about Sarah Jones: "Everyone in Cincinnati knows this kicker is a Sex Addict. It is no secret . . . he can't even keep relationships because his Red Rocket has freckles that need to be touched constantly.—nik."[95]

Richie, The Dirty's administrator, refused to remove the postings about Sarah Jones, and she filed "tort claims of defamation, libel *per se*, false light, and intentional inflection of emotional distress."[96] "Richie and Dirty World claimed that § 230(c)(1) barred these claims."[97] The district court ruled that Section 230 did not shield these claims. The case was submitted to a second jury, which returned a verdict in favor of Jones for $38,000 in compensatory damages and $300,000 in punitive damages.[98] The issue for the Sixth Circuit was whether the district court improperly denied the defendants' motion for judgment as a matter of law by holding that the CDA bars Sara Jones' claims.[99] The Sixth Circuit adopted a material contribution standard to determine whether a website is liable for the content.[100] The court expressly declined to adopt the definition of "development" set forth by the lower court.[101]

The court ruled that "Dirty World and Richie did not author the statements at issue; however, they did select the statements for publication. [Nevertheless,] Richie and Dirty World cannot be found to have materially contributed to the defamatory content of the statements posted on [the Dirty Website]."[102] The appeals court also rejected an "encouragement" test.[103] The Sixth Circuit found that The Dirty did not require users to post illegal or actionable content as a condition of use.[104] The Sixth Circuit vacated the judgment in favor of Jones and 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.[105]

---

[94] *Id*. at 403.
[95] *Id*.
[96] *Id*. at 402.
[97] *Id*.
[98] *Id*.
[99] *Id*. at 401.
[100] *Id*. at 413.
[101] *Id*.
[102] *Id*. at 415.
[103] *Id*. at 414.
[104] *Id*. at 416.
[105] *Id*. at 417.

In *Ramey v. Darkside Products, Inc.*,[106] Darkside operated an online advertising guide for legal adult entertainment services. The plaintiff, Ramey, was a D.C. nude dancer who contended that she had not consented to the use of her photographs as an advertisement in the guide.[107] The court recounted how Darkside received the photographs:

> In 1999 or 2000, Plaintiff met Crittenden [advertising customer of Darkside] and Darryl Pounds, a Washington Redskins player who was a friend of Crittenden, while she was performing at the Nexus Gold Club. Shortly thereafter, Plaintiff became sexually involved with Pounds and allowed him to take a series of intimate photographs of her in her home. Crittenden somehow obtained two of these photographs and used them in an advertisement for After Hours. Crittenden paid Defendant to publish this advertisement which contained Plaintiff's image on its Eros Guide website.[108]

The court granted summary judgment in favor of a publisher of an online advertising guide for adult entertainment, dismissing claims of the intentional infliction of emotional distress, unjust enrichment, negligence, and fraud. The court concluded that CDA Section 230 barred these actions as Darkside was an interactive computer service rather than a content provider.[109]

In *Bennett v. Google, Inc.*,[110] a sports apparel retailer and its owner brought action against the Internet search engine provider for defamation, tortious interference with a business relationship, and the intentional infliction of emotional distress after Google failed to remove allegedly offensive third-party blog posts. The blog asserted that the luxury sporting goods company failed to pay its employees or contractors and owed many thousands of dollars to the employees and clients. The blog concluded: "I urge you to think twice before giving your patronage to DJ Bennett.com . . . . The website is pretty, but the person running the show is quite contemptible."[111]

---

[106] Ramey v. Darkside Prods., No. 02-730 (GK), 2004 U.S. Dist. LEXIS 10107, at *5, *7–8 (D.D.C. May 17, 2004) ("Plaintiff discovered that Crittenden's advertisement was on the Eros Guide website. Plaintiff claims that she never authorized Crittenden to use her image in his advertisement. She also claims that she asked him several times to remove his advertisement from Defendant's Eros Guide website. Plaintiff did not ask Defendant to remove Crittenden's advertisement from its website or otherwise communicate with Defendant regarding the advertisement prior to filing this action.").

[107] Plaintiff discovered that Crittenden's advertisement was on the Eros Guide website. Plaintiff claims that she never authorized Crittenden to use her image in his advertisement. She also claims that she asked him several times to remove his advertisement from Defendant's Eros Guide website. Plaintiff did not ask Defendant to remove Crittenden's advertisement from its website or otherwise communicate with Defendant regarding the advertisement prior to filing this action. *Id.* at *9 (internal citations omitted).

[108] *Id.* at *8–9.

[109] *Id.* at *1, *20 ("Accordingly, because Defendant did no more than select and make minor alterations to Crittenden's advertisement, it cannot, as a matter of law, be considered the content provider of the advertisement for purposes of § 230.").

[110] Bennett v. Google, LLC, 882 F.3d 1163, 1164 (D.C. Cir. 2018).

[111] *Id.* at 1165.

Bennett sought to hold Google liable for hosting the blog, but the court ruled that Google was shielded by CDA Section 230.[112] The D.C. Circuit noted that the blog critical of the sports apparel business was created by Pierson and Google, but Google neither edited the posts nor dictated what Pierson should write. "Because Google's choice was limited to a 'yes' or 'no' decision whether to remove the post, its action constituted 'the very essence of publishing.'"[113] The federal court dismissed all the sports stores' causes of action on Section 230 grounds, as the global search engine was not liable for a third-party's blog post hosted on its service.[114]

In *Gaston v. Facebook, Inc.*,[115] an Oregon federal court held that CDA Section 230 precluded a defamatory conspiracy claim, dismissing these claims against an Internet who's who: Google, Facebook, and Lexis/Nexis.[116] In *Gaston*, the content was solely created or supplied by a third-party, not the defendants.[117] Websites and other intermediaries are shielded by CDA Section 230 as long as the content was created by third parties. CDA immunity exists only when the plaintiff's claims are based on content provided by another information content provider. If a defendant is an "information content provider" for the content at issue, then the defendant is not entitled to CDA immunity. These cases represent the ever-expanding CDA Section 230 liability shield to diverse online intermediaries. The next Section illustrates how the liability shield is expanding to every conceivable tort cause of action.

3. Spreading Section 230 Immunity to Negligence Claims

Most tort lawsuits in the bricks-and-mortar world seek damages for negligence rather than for intentional torts.[118] To succeed in a traditional negligence case, the plaintiff must demonstrate: (1) the defendant owes them a duty of care; (2) the defendant breached that duty; (3) there is a causal connection between the breach of the duty of care and (4) the damages created by the breach, such as enabling a cybercriminal to invade the privacy of millions of customers.[119] "The foreseeability aspect of [a] breach [of a duty of care] relates to defendant's knowledge of the dangerous condition, whether actual (defendant

---

[112] *Id.* at 1167.
[113] *Id.* at 1168.
[114] *Id.*
[115] Gaston v. Facebook, Inc., No. 3:12-cv-0063-ST, 2021 WL 629868 (D. Or. Feb. 2, 2012).
[116] *Id.* at *1.
[117] *Id.* at *1, *6.
[118] Joe Palazzolo, *We Won't See You in Court: The Era of Tort Lawsuits Is Waning*, WALL ST. J. (July 24, 2017, 5:09 PM), https://www.wsj.com/articles/we-wont-see-you-in-court-the-era-of-tort-lawsuits-is-waning-1500930572 [https://perma.cc/VFH3-P6LB].
[119] Cedeño Nieves v. Aerostar Airport Holdings LLC, 251 F. Supp. 3d 360, 366 (D. P.R. 2017) (stating prima facie case for negligence).

knew) or constructive (defendant should have known)."[120] "Courts should recognize a modified duty of care on the part of software licensors to incorporate reasonable security into their products and services."[121] Nevertheless, negligence has been foreclosed in Internet-related cases because of CDA Section 230's liability shield that immunizes a broad range of Internet intermediaries.

In the first three decades of the software industry, few plaintiffs recovered under a theory of negligence because of the difficulty of proving duty and breach. Negligence requires first that the publisher owe a duty of care, and software licensors or publishers use contract law to disclaim their duty. In a typical software license agreement, the licensor reallocates the computer security risk to the customer and takes no responsibility for either the direct or consequential damages of a breach of a website or other security intrusion. To date, courts invariably extend CDA Section 230 to Internet-related negligence claims. For example, in *Green v. America Online (AOL)*,[122] the Third Circuit held that § 230(c)(1) immunity applied to a plaintiff's claim that AOL "negligent[ly] fail[ed] to properly police its network for [tortious] content transmitted by its users."[123]

In *Doe v. MySpace, Inc.*,[124] the Fifth Circuit affirmed the dismissal of negligence and gross negligence claims that arose out of a sexual assault of a fourteen year-old girl by an adult she met via MySpace.com.[125] Doe created a profile by lying about her age.[126] This action resulted in her profile being made public, allowing a sexual predator to initiate contact with her and rape her.[127] The court held, "without considering the Does' content-creation argument, that their negligence and gross negligence claims are barred by the CDA, which prohibits claims against Web-based interactive computer services based on their publication of third-party content."[128]

---

[120] *Id.* at 367.

[121] Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1557 (2005).

[122] Green v. Am. Online, 318 F.3d 465 (3rd Cir. 2003) (dismissing cause of action based upon Section 230 for defamatory comments made by third-parties in chatroom).

[123] *Id.* at 470.

[124] Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008).

[125] *Id.* at 422.

[126] *Id.* at 416.

[127] *Id.* ("In the summer of 2005, at age thirteen, Julie Doe ("Julie") lied about her age, represented that she was eighteen years old, and created a profile on MySpace.com. This action allowed her to circumvent all safety features of the Web site and resulted in her profile being made public; nineteen-year-old Pete Solis ("Solis") was able to initiate contact with Julie in April 2006 when she was fourteen. The two communicated offline on several occasions after Julie provided her telephone number. They met in person in May 2006, and, at this meeting, Solis sexually assaulted Julie.").

[128] *Id.* at 422.

In *Doe v. America Online, Inc.*,[129] the Florida Supreme Court held Section 230 shielded AOL because it fell "squarely within this traditional definition of a publisher and, therefore, is clearly protected by § 230's immunity."[130] The court ruled that CDA Section 230's liability shield applied to the "liability based upon negligent failure to control the content of users' publishing of allegedly illegal postings on the Internet that [was] the gravamen of Doe's alleged cause of action."[131] This was the first judicial opinion in which a court stretched the preemptive scope of Section 230 to not only bar defamation claims as a publisher of a third-party's statements but also to bar claims for negligence. The plaintiff in that case contended that America Online failed to employ adequate safeguards to protect children from illegal third-party communication.[132]

The Wisconsin Supreme Court reversed a lower court finding that a website selling firearms was shielded by CDA Section 230 in *Daniel v. Armslist, LLC*.[133] "Daniel's tort action arose from a mass shooting in a Brookfield, Wisconsin spa that killed four people, including Daniel's mother, Zina Daniel Haughton. Daniel alleged that the shooter, Radcliffe Haughton, illegally purchased the firearm after responding to private seller Devin Linn's post on Armslist's firearm advertising website, armslist.com."[134] The husband of Daniel's mother purchased a semiautomatic handgun with a high-capacity magazine using "armslist.com's 'contact' function."[135] One day after he purchased the weapon, the husband killed Daniel's mother and two others, as well as himself. Daniel's negligence complaint spells out several measures that Armslist could have taken to reduce the known risk of selling illegal firearms to dangerous prospective purchasers. The plaintiff contended:

> Armslist could have required buyers to create accounts and provide information such as their name, address, and phone number. In states similar to Wisconsin, where there is online access to an individual's criminal history, Armslist could have required potential buyers to upload their criminal history before their accounts were approved.[136]

Daniel did not dispute that Armslist was an interactive computer service provider, but contended that the design and operation of its website "helped to develop the content of the firearm advertisement."[137] Daniel argued that this facilitation made Armslist an information content provider with respect to the ad-

---

[129] Doe v. Am. Online, Inc., 738 So. 2d 1010 (Fla. 2001).
[130] *Id.* at 1017.
[131] *Id.*
[132] *Id.* at 1015.
[133] Daniel v. Armslist, LLC, 926 N.W. 2d 710 (Wis. 2019).
[134] *Id.* at 714.
[135] *Id.* at 715.
[136] *Id.* at 716.
[137] *Id.* at 718.

vertisement, thereby placing it outside of the CDA's protection.[138] She argued "that her claims [were] not based on Armslist's publication of content at all, but [were] instead based on Armslist's facilitation and encouragement of illegal firearm sales by third parties."[139] Daniel's complaint was that:

> Armslist knew or should have known that its website would put firearms in the hands of dangerous, prohibited purchasers, and that Armslist specifically designed its website to facilitate illegal transactions. The causes of action asserted against Armslist are negligence, negligence per se, negligent infliction of emotional distress, civil conspiracy, aiding and abetting tortious conduct, public nuisance, and wrongful death.[140]

Armslist's defense was "that the CDA immunizes it from liability for the information posted by third parties on armslist.com, and moved to dismiss Daniel's complaint for failure to state a claim upon which relief can be granted."[141] "The circuit court granted Armslist's motion and dismissed the complaint."[142]

The Wisconsin Court of Appeals reversed the dismissal of Daniel's complaint against the website operator to "protect a website operator from liability for its own actions in designing and operating its website."[143] The Wisconsin Supreme Court reversed the decision of the court of appeals, reasoning:

> In this case, all of Daniel's claims against Armslist require the court to treat Armslist as the publisher or speaker of third-party content. Daniel's negligence claim asserts that Armslist had a duty to exercise "reasonable care" in "facilitating" the sale of guns, and had a duty to employ "sufficient questioning and screening" to reduce the risk of foreseeable injury to others. The complaint alleges that Armslist breached this duty by designing armslist.com to "facilitate" illegal gun sales, as well as by failing to implement sufficient safety measures to prevent the unlawful use of its website. Daniel's negligence claim is simply another way of claiming that Armslist is liable for publishing third-party firearm advertisements and for failing to properly screen who may access this content. The complaint alleges that Armslist breached its duty of care by designing a website that could be used to facilitate illegal sales, failing to provide proper legal guidance to users, and failing to adequately screen unlawful content. Restated, it alleges that Armslist provided an online forum for third-party content and failed to adequately monitor that content. The duty Armslist is alleged to have violated derives from its role as a publisher of firearm advertisements. This is precisely the type of claim that is prohibited by § 230(c)(1), no matter how artfully pled.[144]

---

138 *Id*.
139 *Id*.
140 *Id*. at 716.
141 *Id*.
142 *Id*.
143 *Id*.
144 *Id*. at 725–26.

"[C]ourts use the 'material contribution' test to determine whether a website operator is responsible for the 'development' of content."[145] Moreover:

> [C]lose cases . . . must be resolved in favor of immunity, lest we cut the heart out of [S]ection 230 by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties."[146]

The Wisconsin Supreme Court applied the "material contribution" test to determine whether Armslist was liable as a content creator.[147] The court ruled that Armslist was not an information content provider, dismissing all of the plaintiffs' claims that were dependent on treating the operator as the publisher or speaker of third-party content.[148]

A 2002 U.S. Congressional Report notes that ISPs "have successfully defended many lawsuits using [S]ection 230(c). The courts have correctly interpreted [S]ection 230(c), which was aimed at protecting against liability for such claims as negligence."[149] A Texas state appeals court held that CDA Section 230 barred an individual's negligent entrustment, negligent supervision, and negligent undertaking claims against an employer in *Davis v. Motiva Enterprises, LLC*.[150] "Davis alleged that, while employed by Motiva, Fournet used Motiva's technology and facilities to lodge 'an obscene cyber-strike campaign' against her by posting advertisements to Craig's List and posing 'as [Davis] as if she were soliciting for sexual encounters with strangers.'"[151] The case studies in the next Part illustrate some of the worst excesses of CDA Section 230 in shielding ISPs, which were in the best position to prevent or remediate the harm of ongoing cybertorts or crimes.

II. THE DYSFUNCTIONS OF SHIELDING DEPLORABLE CONTENT

Eighteenth century tort law was originally restricted to a narrow set of intentional torts but, in the mid-nineteenth century, evolved to recognize negli-

---

[145] *Id*. at 719.

[146] Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc).

[147] *Daniel*, 926 N.W.2d at 719 ("In order to avoid these two extremes and to remain faithful to the text and purpose of § 230, courts use the 'material contribution' test to determine whether a website operator is responsible for the 'development' of content. '[A] website helps to develop unlawful content, and thus falls within [Section 230(f)(3)], if it contributes materially to the alleged illegality of the conduct.' A material contribution 'does not mean merely taking action that is necessary to the display of allegedly illegal content,' such as providing a forum for third-party posts. 'Rather, it means being responsible for what makes the displayed content allegedly unlawful.'").

[148] *Id*. at 726.

[149] *Fair Hous. Council of San Fernando Valley*, 521 F.3d at 1188.

[150] Davis v. Motiva Enters., LLC., No. 09-14-00434-CV, 2015 WL 1535694 (Tex. App. Apr. 2, 2015).

[151] *Id*. at *1.

gence and strict products liability in railroad and industrial accidents. "As time passed, tort law expanded to permit victims of less serious infringements, such as accidents on the roads, a means of seeking redress in the courts."[152] Torts in the twenty-first century must continually evolve to address new injuries created by technological advances, such as chatrooms, bots, and other Internet innovations.[153]

CDA Section 230 impedes the development of cybertorts because websites and other online intermediaries have no existing duty to take down tortious or criminal content even if they have actual notice. This Part uses cybertort cases to illustrate the injustices that arise from CDA Section 230's website immunity for third-party tortious postings.

Cybertorts, such as reputational injury or the invasions of privacy, stand in sharp contrast to traditional torts where physical injuries and deaths predominate, typically arising out of automobile accidents, slip and fall mishaps, medical malpractice, dangerously defective products, and other personal injury torts. Cybertorts frequently trigger a First Amendment analysis because most actions are information-based torts.[154] These Internet tort cases present courts with difficult issues in balancing state tort causes of action against expression protected by the Constitution.[155]

Many online torts are easily recognizable extensions of long-established torts in the brick-and-mortar world. In the physical world, a defamatory statement is one that is false and that (1) injures another person's reputation; (2) subjects the person to hatred, contempt, or ridicule; or (3) causes others to lose good will or confidence in that person.[156] Defamation in cyberspace differs

---

[152] KEITH N. HYLTON, TORT LAW: A MODERN PERSPECTIVE (2016).

[153] Rustad & Koenig, *supra* note 67, at 77–78, 93 (explaining term "legal lag" through sociologist William Ogburn's concept of cultural lag in which the various institutions of American society do not change at the same rate, thereby creating a "cultural lag" when one element has not yet accommodated to developments in another); *see also* Sanders & Dukeminier, Jr., *supra* note 68, at 395–99.

[154] In Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 447 (E.D. Pa. 1996), the court ruled that a private company did not have a First Amendment right to send massive amounts of unsolicited, commercial emails to Internet subscribers.

[155] MARY MULLEN, THE INTERNET AND PUBLIC POLICY: CYBERTORTS AND ONLINE PROPERTY RIGHTS 3 (2018).

[156] Romaine v. Kallinger, 537 A.2d 284, 287 (N.J. 1988). Courts vary in defining defamation, and often a particular definition or rule is peculiar to a small number of jurisdictions. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 773 (1984). Defamation is "that which tends to injure 'reputation' in the popular sense; to diminish the esteem, respect, goodwill or confidence in which the plaintiff is held, or to excite adverse, derogatory or unpleasant feelings or opinions against him." *Id*. Keeton describes the prima facie case as follows:

> [I]t has always been necessary for the plaintiff to prove as a part of his prima facie case that the defendant (1) published a statement that was (2) defamatory (3) of and concerning the plaintiff. In a typical case of defamation, the publisher (1) realized that the statement made was defamato-

from defamation in the real world only because the false, injurious statements are posted on websites or otherwise take place online. Unlike traditional torts, Internet-related torts seldom involve personal injury or death.

Other cybertorts are unique to the Internet. These Internet torts include actions for the cyberconversion of domain names, denial of service attacks, spyware, cyberstalking, negligent computer security, creating computer viruses, and camfecting, which is "the process by which the camfecter spies on everything in the field of vision of another person's webcam, while operating it without the owner's permission, usually after having infected their PC with a virus which grants access to the device."[157] Cybersmearing is broadly defined as anonymous or pseudo-anonymous defamation on the Internet.[158] Another unique cybertort is "[d]oxing, short for 'dropping documents,' [which] is the practice of disclosing a person's identifying information (e.g., their home address) on the Internet to retaliate against and harass the 'outed' person."[159]

The primary online wrongdoers are theoretically liable for intentional torts but are generally beyond the reach of the law, given that they are frequently anonymous, insolvent, imprisoned, and/or located in foreign venues. Courts are unanimous in holding that intermediaries such as Google, Facebook, or Twitter have no duty to delete fraudulent third-party content, even if it constitutes an ongoing crime or tort.[160] Cybercrime enforcement is theoretically possible, but generally impractical because law enforcement generally lacks the financial, technical, and scientific expertise to investigate cross-border cybercrimes effectively. Prosecutors are too overburdened with crime in the streets to investigate crimes in cyberspace, where jurisdiction is uncertain and discovery is time con-

---

ry, (2) intended to refer to the plaintiff, and (3) intended to communicate it to a third person or persons.

Id. at 802. A business defamation lawsuit occurs when an untrue statement is communicated which "prejudice[s] [the business entity] in the conduct of its business and deter[s] others from dealing with it." A.F.M. Corp. v. Corp. Aircraft Mgmt., 626 F. Supp. 1533, 1551 (D. Mass. 1985); *see e.g*., Amway Corp. v. Proctor & Gamble Co., No. 1:98-CV-726, 2000 U.S. Dist. LEXIS 372, at *15–16 (W.D. Mich. Jan. 6, 2000) (ruling that Amway made prima facie showing that P & G's website was aimed at forum and caused harm to its business reputation).

[157] Alice Sommacal, *Camfecting: What It Is and How We Can Protect Ourselves from It*, UNILAB (May 25, 2018), https://www.unilab.eu/articles/coffee-break/camfecting/ [https://perma.cc/MX9M-LKGE].

[158] *See* Roger M. Rosen & Charles B. Rosenberg, *Suing Anonymous Defendants for Internet Defamation*, THE L.A. LAW., 19 (2001).

[159] Vangheluwe v. Got News, LLC, 365 F.3d 850, 852 (E.D. Mich. 2019).

[160] Internet service providers have no duty to remove or take down content that constitutes an ongoing tort so long as they are not classifiable as a content creator. *See, e.g.,* Doe II v. MySpace Inc., 96 Cal. Rptr. 3d 148, 156 (Cal. Ct. App. 2009) (ruling MySpace had no duty to remove fraudulent profile); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 835 (Cal. Ct. App. 2002) (ruling that CDA Section 230 barred negligence claim arising out of eBay's failure to remove or alter allegedly fraudulent product descriptions).

suming and expensive. The reality is that many reprehensible cybercrimes and torts go unpunished without the deterrence of cybertorts.

Cyberspace provides an ideal legal environment for creating ongoing torts because ISPs and other Internet intermediaries have no duty to disable or remove illegal content constituting ongoing torts, such as defamation, the invasion of privacy, the intentional infliction of emotional distress, negligence, and virtually every other intentional tort. Commercial websites that host deplorable content for profit also enjoy an absolute immunity, even when they host content advocating terrorism, containing humiliating images of ex-lovers, or selling fake medicines. Courts have interpreted CDA Section 230 so broadly that it now shields online intermediaries from all tort liability even if there is clear and convincing evidence that the postings pose an imminent threat of harm to the public.

A. COVID-19 Vaccine Disinformation

The Food and Drug Administration (FDA) states that individuals and companies "are trying to profit from this pandemic by selling unproven and illegally marketed products that make false claims, such as being effective against the coronavirus" when they have not been approved or authorized by the FDA.[161] "The FDA has received multiple reports of people who have needed medical attention, including hospitalization, after self-medicating with ivermectin intended for livestock."[162] The FDA states that ivermectin has not been approved "for use in preventing or treating COVID-19 in humans or animals. The FDA is also aware of people trying to prevent COVID-19 by taking chloroquine phosphate, which is sold to treat parasites in aquarium fish."[163]

As the novel coronavirus spreads across the United States, so does an infodemic of dangerous misinformation threatening public health, which is often spread by social media.[164] Fraudulent and dangerous COVID-19 "cures" are not

---

[161] U.S. Food & Drug Administration, *Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments*, FDA (Feb. 3, 2022), https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments [https://perma.cc/3XCG-K7DG].

[162] *Id.*

[163] *Id.*

[164] "'We're not just fighting an epidemic; we're fighting an infodemic,' said Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO) at a gathering of foreign policy and security experts in Munich, Germany, in mid- February, referring to fake news that 'spreads faster and more easily than this virus.'" "WHO explains that infodemics are an excessive amount of information about a problem, which makes it difficult to identify a solution. They can spread misinformation, disinformation and rumors during a health emergency. Infodemics can hamper an effective public health response and create confusion and distrust among people." The Department of Global Communications, *UN Tackles 'Infodemic' of Misinformation and Cybercrime in COVID-19 Crisis*, UNITED NATIONS (Mar. 31, 2020), https://www.un.org/en/un-coronavirus-communications-team/un-

just "fake news;"[165]—they undermine efforts to confront the COVID-19 pandemic. The UNESCO Director for Policies and Strategies Regarding Communication and Information explained that falsehoods related to all aspects of COVID-19 endanger the public, stating:

> There seems to be barely an area left untouched by disinformation in relation to the COVID-19 crisis, ranging from the origin of the coronavirus, through to unproven prevention and 'cures', and encompassing responses by governments, companies, celebrities and others . . . . Because of the scale of the problem, the World Health Organization (WHO), which is leading the UN's response to the pandemic, has added a "MythBusters" section to its online coronavirus advice pages. It refutes a staggering array of myths, including claims that drinking potent alcoholic drinks, exposure to high temperatures, or conversely, cold weather, can kill the virus . . . . The likely consequence, he says, is complacency, which could fuel more premature deaths. The UNESCO official also pointed to a more harmful example of disinformation: encouraging the taking of medication, approved for other purposes, but not yet clinically proven as being effective against COVID-19.[166]

Congress has identified false information regarding COVID-19 vaccines on Facebook and other social media as a serious issue. Representative Diana DeGette of Colorado sent a letter to Facebook and Twitter's chief executives calling for them to explain how these social networks are addressing the problem of false postings on their service.

> In December [2020], the Food and Drug Administration granted Emergency Use Authorizations for two COVID-19 vaccines found to be safe and effective based on available evidence, and states are now administering these vaccines to targeted populations. As the country enters this next phase in its fight against the virus--the success of which is dependent on hundreds of millions of Americans trusting the science behind these vaccines--the Committee is deeply troubled by news reports of coronavirus vaccine misinformation on your platform. In fact, the proliferation of false and misleading information on platforms is so widespread that the American Medical Association wrote to your company last month urging you to 'guard against disinformation' . . . . It is imperative that Twitter stops the spread of false or misleading information about coronavirus vaccines on its platform. False and misleading information is dangerous, and if

tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19 [https://perma.cc/VZE7-8JQG].

[165] UNESCO defines 'Fake news' as "an oxymoron which lends itself to undermining the credibility of information which does indeed meet the threshold of verifiability and public interest – i.e., real news." JULIE POSETTI ET AL., *Foreword to* UNESCO, JOURNALISM, 'FAKE NEWS' & DISINFORMATION: HANDBOOK FOR JOURNALISM EDUCATION AND TRAINING 7 (2018).

[166] United Nations, *During This Coronavirus Pandemic, 'Fake News' Is Putting Lives at Risk: UNESCO*, UN NEWS (Apr. 13, 2020), https://news.un.org/en/story/2020/04/1061592 [https://perma.cc/XR5R-N5RA].

> relied on by the public to make critical health choices, it could result in the loss of human life.[167]

Instagram labeled a bogus COVID-19 posting on Madonna's Instagram account as false information and "directed users to a page that debunked the video's claims."[168] "PolitiFact published a fact-check warning its audience that, contrary to what was being said on Twitter, drinking chlorine dioxide (or bleach) did not cure coronavirus. In reality, that was dangerous and could even 'generate life-threatening side effects.'"[169] Two weeks after this warning was issued, "the madness of suggesting that someone with coronavirus should drink bleach was still loose on social networks in the United States."[170] "Facebook . . . will remove misinformation about the COVID-19 vaccines from the platform and from Instagram in order to continue combatting false claims about the pandemic."[171] Facebook's updated policy provides:

> Posts will be removed if they include claims that the COVID-19 vaccines will kill or seriously harm people, will cause autism or infertility, will change people's DNA, or will cause irrational side effects like turning a person into a monkey. Other false claims will also be removed, like those that say contracting the disease is safer than getting the vaccine and that receiving the shot is unsafe for certain groups of people. Facebook will take down false statements about how COVID-19 vaccines were made or their efficacy.[172]

CDA Section 230 does not impose a notice-and-takedown duty to disable COVID-19 vaccine disinformation on social networks. While social media entities have no duty to disable this content, the largest site, Facebook, has voluntarily instituted takedown policies.[173] Other social media companies use policies in between the anti-misinformation policies of Facebook and Pinterest.

---

[167] Targeted News Service, *Rep. DeGette Demands Answers on Tech Companies' Efforts to Prevent Vaccine Misinformation Online*, TARGETED NEWS SERV. (Feb. 3, 2021).

[168] Rachel McGrath, *Madonna's Instagram Account Slapped with 'False Information' Warning After Covid-19 Conspiracy Theory Post*, EVENING STANDARD (July 29, 2020), https://www.standard.co.uk/showbiz/celebrity-news/madonna-instagram-coronavirus-conspiracy-theory-a4511606.html [https://perma.cc/HR3G-SCKC].

[169] Cristina Tardáguila, *These Are False Cures and Fake Preventative Measures Against Coronavirus. Help Fact-Checkers Spread the Word*, POYNTER (Feb. 13, 2020), https://www.poynter.org/fact-checking/2020/these-are-false-cures-and-fake-preventative-measures-against-coronavirus-help-fact-checkers-spread-the-word [https://perma.cc/Y4CC-XQ47].

[170] *Id.*

[171] Natasha Dailey, *Facebook Expanded Its Rules on Posting Misinformation and Will Remove All False Claims About COVID Vaccines, Including That They Cause Autism*, BUS. INSIDER: INDIA (Feb. 9, 2021, 2:17 PM), https://www.businessinsider.com/facebook-remove-false-claims-about-covid-vaccines-autism-who-2021-2 [https://perma.cc/2LPX-Z8TJ].

[172] *Id.*

[173] Molly Schuetz, *Facebook Will Take down Misinformation About Covid Vaccines*, BLOOMBERG (Dec. 3, 2020, 6:00 AM), https://www.bloomberg.com/news/articles/2020-12-03/facebook-will-take-down-misinformation-about-covid-vaccines [https://perma.cc/3H5L-GYYV].

"Twitter prohibits tweets that 'advance harmful false or misleading narratives about COVID-19 vaccinations' and has said it removed 8,400 posts" by December 2020.[174] Despite these efforts, scams and dangerous information continues to proliferate on Facebook and other social networks.[175] "An international pressure group that spread false and conspiratorial claims about Covid-19 more than doubled the average number of interactions it got on Facebook in the first six months of 2021 in spite of renewed efforts to curb misinformation on the platform, according to a report."[176]

"The World Doctors Alliance includes prominent members who have falsely claimed Covid-19 is a hoax and that vaccines cause widespread harm."[177] The Center for Disease Control warns that members of the "general public are receiving calls appearing to originate from CDC through caller ID, or they are receiving scammer voice mail messages saying the caller is from the Centers for Disease Control and Prevention (CDC)."[178] "Malicious cyber criminals are also attempting to leverage interest and activity in COVID-19 to launch coronavirus-themed phishing emails" used to send malware enabling them "to takeover healthcare IT systems and steal information."[179]

B. Shielding Content Inciting Terrorist Acts

Observers argue that CDA Section 230 needs to be scaled back because "[a]s technologies advance and the web becomes more prevalent, the seriousness of terrorists' incitement increases and infringes on the public's sense of security and safety. Therefore, it is time to challenge the immunity regime and redefine it."[180] The First Amendment provides no "right to facilitate terrorism by working under the organization's direction or control or by managing, supervising or directing the operation of a terrorist organization."[181] "[C]ivil lia-

---

[174] Daniel Funke, *False COVID-19 Vaccine Claims Persist on Facebook, Despite a Ban. Here's Why*., POYNTER (Mar. 31, 2021), https://www.poynter.org/fact-checking/2021/false-covid-19-vaccine-claims-persist-on-facebook-despite-a-ban-heres-why [https://perma.cc/P7CN-D5XZ].

[175] *See e.g.*, Liz Wegerer, *Top Facebook Scams of 2021 and How to Avoid Them,* VPN OVERVIEW (Nov. 18, 2021), https://vpnoverview.com/privacy/social-media/facebook-scams [https://perma.cc/QDN6-5V8S].

[176] Niamh McIntyre, *Group That Spread False Covid Claims Doubled Facebook Interactions in Six Months: Revelations About World Doctors Alliance Pages Raise Questions About Platform's Efforts to Control Misinformation*, GUARDIAN (Oct. 21, 2021, 6:51 PM), https://www.theguardian.com/technology/2021/oct/21/group-that-spread-false-covid-claims-doubled-facebook-interactions-in-six-months [https://perma.cc/T755-YE27].

[177] *Id*.

[178] Center for Disease Control (CDC), *COVID-19-Related Phone Scams and Phishing Attacks*, CDC (April 3, 2020), https://www.cdc.gov/media/phishing.html [https://perma.cc/UA8G-6NX9].

[179] *Id*.

[180] Michal Lavi, *Do Platforms Kill?*, 43 HARV. J. L. & PUB. POL'Y 477, 554 (2020).

[181] United States v. Taleb-Jedi, 566 F. Supp. 2d 157, 168 (E.D.N.Y. 2008).

bility for funding a foreign terrorist organization does not offend the First Amendment so long as the plaintiffs are able to prove that the defendants knew about the organization's illegal activity, desired to help that activity succeed and engaged in some act of helping."[182]

CDA Section 230 shields website operators who host terrorists even if they have notice of the potential or actual harm enabled by the deplorable posts. ISIS or Hamas have no First Amendment right to organize or advocate homicidal attacks on Facebook, Twitter, or other social networks.[183] "[T]he First Amendment does not preclude restrictions on certain categories of speech having little or no social value, and threats are one such category."[184] "A statement qualifies as a 'true threat,' unprotected by the First Amendment, if it is 'a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.'"[185] A Congressional Research Service report notes that the First Amendment protects speech, not violent conduct:

> As the Supreme Court has observed, while the First Amendment protects the "freedom of speech," it "does not protect violence." But when speech promotes violence, a tension can form between the values of liberty and security. In an oft-quoted passage from a dissenting opinion, Justice Robert Jackson argued that the problems this tension creates are not insurmountable but must be confronted with a dose of pragmatism: a government can temper "liberty with order," but to treat free speech as absolute threatens to "convert the constitutional Bill of Rights into a suicide pact." … Over the past 50 years, the Court has drawn a line between speech that advocates violence in the abstract and speech that facilitates it in a specific way, with the former receiving more robust constitutional protections.[186]

U.S. courts have affirmed the far-reaching CDA Section 230 shield to protect postings by terrorist organizations, even when such organizations pose widespread harm to American society. For example, in *Fields v. Twitter, Inc.*,[187] Fields and another government contractor were shot and killed while employed at a law enforcement-training center in Amman, Jordan.[188] "The

---

[182] Boim v. Quranic Literacy Inst., 291 F.3d 1000, 1028 (7th Cir. 2002).

[183] "With one major exception, the Roberts Court has been quite protective of unpopular (and even revolting) speech under the First Amendment. That exception, however, is a doozy. It involves a statute criminalizing 'material support' for terrorism, and the danger of the law was on stark display this week with reports of a petition to hold Twitter responsible for allowing Hamas to use the service." Gabe Rottman, *Hamas, Twitter and the First Amendment*, ACLU (Nov. 21, 2012, 3:25 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/hamas-twitter-and-first-amendment [https://perma.cc/MJ7U-69V6].

[184] United States v. Parr, 545 F.3d 491, 496–97 (7th Cir. 2008).

[185] *Id.* at 497.

[186] VICTORIA L. KILLION, TERRORISM, CONG. RSCH. SERV., R45713, VIOLENT EXTREMISM, AND THE INTERNET: FREE SPEECH CONSIDERATIONS 1 (2019).

[187] Fields v. Twitter, Inc., 217 F. Supp. 3d 1116 (N.D. Cal. 2016), *aff'd*, Fields v. Twitter, Inc., 881 F.3d 739 (9th Cir. 2018).

[188] *Id.* at 1118.

shooter, Anwar Abu Zaid, was a Jordanian police officer who had been studying at the center."[189] "[T]he Islamic State of Iraq and Syria ('ISIS') claimed responsibility for the attack, and according to Israeli intelligence, the gunman belonged to a clandestine ISIS terror cell."[190]

Field and her co-plaintiff "assert[ed] that Twitter's 'provision of material support to ISIS was a proximate cause.'"[191] "Twitter enabled ISIS to acquire the resources needed to carry out numerous terrorist attacks," including the murder that took place on November 9, 2015, "when an ISIS operative in Amman, Jordan shot and killed Lloyd 'Carl' Fields, Jr. and James Damon Creach."[192] "Fields claim[ed] that Twitter 'knowingly permitted the terrorist group ISIS to use its social media network as a tool for spreading extremist propaganda, raising funds, and attracting new recruits,' constituting 'material support.'"

Field's complaint included a large "number of images that were once posted on Twitter by pro-ISIS accounts promoting terrorism, including an image combining the Twitter logo with the ISIS flag."[193] Field contended that ISIS used Twitter to spread propaganda and incite fear by posting graphic photos and videos of its terrorist feats and to raise funds for its terrorist activities.[194] Field's complaint charged further that Twitter "knowingly permitted . . . ISIS to use its social network as a tool for spreading extremist propaganda, raising funds and attracting new recruits," and that this material support has been instrumental to the rise of ISIS and has enabled it to carry out numerous terrorist attacks, including the November 9, 2015, shooting attack in Amman, Jordan, in which Fields and Creach were killed.[195]

Additionally, the plaintiffs asserted that "ISIS use[d] Twitter as a recruitment platform, 'reach[ing] potential recruits by maintaining accounts on Twitter so that individuals across the globe can reach out to [ISIS] directly. After first contact, potential recruits and ISIS recruiters often communicate via Twitter's Direct Messaging capabilities.'"[196] Field and her coplaintiff noted that "[t]hrough its use of Twitter, ISIS has recruited more than 30,000 foreign re-

---

[189] *Id*.

[190] *Id*.

[191] *Id*. at 1119. "Plaintiffs assert that Twitter's 'provision of material support to ISIS was a proximate cause of [their] injur[ies].'" *Id*. They allege that Twitter "had 'knowingly permitted . . . ISIS to use its social network as a tool for spreading extremist propaganda, raising funds and attracting new recruits.'" *Id*. at 1120*; see also*, Pennie v. Twitter, Inc., 281 F. Supp. 3d 874, 881 (N.D. Cal. 2017) ("Defendant's provision of material support to ISIS was a proximate cause of the injury inflicted on Plaintiffs.").

[192] *Fields*, 217 F. Supp. 3d at 1119.

[193] Michelle Roter, *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, 45 HOFSTRA L. REV. 1379, 1395 (2017).

[194] *Id*.

[195] *Fields*, 200 F. Supp. 3d at 1119–20.

[196] *Id*. at 1119.

cruits over the last year."[197] The plaintiff also contended that Twitter took no action to block ISIS's use of Twitter despite having notice of its misuse of the social network.[198]

Fields and her co-plaintiff sought to hold Twitter liable for Abu Zaid's despicable acts and ISIS's terrorism "under 18 U.S.C. § 2333(a), part of the Anti-Terrorism Act (ATA), on the theory that Twitter provided material support to ISIS by allowing ISIS to sign up for [and use] Twitter accounts, and that this material support was a proximate cause of the November 2015 shooting."[199] The federal district court dismissed the complaint because it sought to "hold Twitter liable as a publisher or speaker of ISIS's hateful rhetoric, and that such liability is barred by the CDA."[200] The court granted Twitter's motion to dismiss with leave to amend.[201]

Similarly, in *Klayman v. Zuckerberg*,[202] the court ruled that CDA Section 230 shielded Facebook for hosting a page created by a third party inciting Muslim violence against Jewish people.[203] "Klayman encountered a page on Facebook's social networking website entitled 'Third Palestinian Intifada,' which called for Muslims to rise up and kill the Jewish people."[204] "Facebook subsequently removed the Third Intifada page from its website, but not promptly enough for Klayman. He filed suit against Facebook and its founder, Mark Zuckerberg, alleging that their delay in removing that page and similar pages constituted intentional assault and negligence."[205] The court reasoned that "a website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online."[206]

In *Klayman*, the court ruled that Facebook was entitled to CDA Section 230 immunity for threats posted on its service by the Third Palestinian Intifada.[207] Similarly, in *Pennie v. Twitter, Inc.*,[208] the court held that Twitter was immunized from claims alleging that it had provided material support for Hamas, a foreign terrorist group for content hosted on its service.[209] The court

---

[197] *Id.*
[198] *Id.*
[199] *Id.* at 1118.
[200] *Id.*
[201] *Id.* at 1127.
[202] Klayman v. Zuckerberg, 753 F.3d 1354 (D.C. Cir. 2014).
[203] *Id.* at 1355.
[204] *Id.*
[205] *Id.*
[206] *Id.* at 1358.
[207] *Id.* at 1355, 1358.
[208] Pennie v. Twitter, Inc., 281 F. Supp. 3d 874 (N.D. Cal. 2017).
[209] *Id.* at 876. "[S]eparated into its elements, section 230(c)(1) protects from liability only (a) a provider or user of an interactive computer service (b) that the plaintiff seeks to treat as a publisher or speaker (c) of information provided by another information content provider."

concluded that the CDA immunized social media platforms "from most if not all of Plaintiffs' claims, because Plaintiffs' theory of liability rests largely on the premise that Defendants should be held responsible for content created and posted by users (here, Hamas and its affiliates) of Defendants' interactive computer services."[210] While there is no First Amendment protection for those who "advocat[e] . . . the duty, necessity, or propriety of crime, sabotage, violence, or unlawful methods of terrorism as a means of accomplishing industrial or political reform,"[211] CDA Section 230 provides no takedown requirement for content that incites terrorism.

In sharp contrast to U.S. law, the European Union requires

> online platforms to set up mechanisms to enable them to detect and quickly remove online terrorist content. The Commission published a [C]ommunication on that matter in September 2017 and a [R]ecommendation in March 2018. In its [C]ommunication, the Commission stated that if no clear progress w[ere] made on the removal of illegal content, it would propose legislative and therefore binding measures to tackle the problem. It was to assess whether additional measures were needed by May 2018.[212]

In 2017, the United Kingdom and France "held a joint press conference to declare the implementation of a 'very concrete' antiterrorist plan. One of the plan's three main objectives is to [reinforce] the obligation of internet platforms to suppress terrorist propaganda contents."[213] Just one day after the joint announcement, "Facebook presented its measures to fight illicit content, which include the use of artificial intelligence systems to detect *ex ante* illicit content and the recruitment of 3,000 moderators. And Google introduced new measures to identify and tackle terrorist content online."[214]

C. Revenge Pornography

Revenge pornography ("revenge porn") is a third category of deplorable content that websites have no duty to disable, even though there is no First Amendment interest, and the postings cause specific harm or pose likely harm

---

Id. at 888 (quoting Fields v. Twitter, 200 F.Supp.3d 964, 969 (N.D. Cal. 2016)). "As far as this Court is aware, every court that has considered the issue has held that the CDA bars claims similar to those presented here, even where the user posting objectionable content to an interactive service is, or is affiliated with, a foreign terrorist organization." *Id.* at 889.

[210] *Id.* at 888.

[211] Brandenburg v. Ohio, 395 U.S. 444, 444 (1969).

[212] Parliamentary Questions, *Online Platforms' Responsibility for Removing Terrorist Content*, EUROPEAN PARLIAMENT (May 24, 2018), https://www.europarl.europa.eu/doceo/document/E-8-2018-002833_EN.html [https://perma.cc/V8V6-TGXG].

[213] Jones Day Insights, *Online Terrorist Propaganda: France and UK Put Internet Giants in the Cross-Hairs*, JONES DAY (July 2017), https://www.jonesday.com/en/insights/2017/07/online-terrorist-propaganda-france-and-uk-put-internet-giants-in-the-cross-hairs [https://perma.cc/E92S-WLDU].

[214] *Id.*

to specific victims. "Nonconsensual pornography" may be defined generally as "distribution of sexually graphic images of individuals without their consent."[215] Revenge porn is the tort that keeps on causing intense emotional pain. The Vermont Supreme Court stated that "[t]he nonconsensual dissemination of such intimate images—to a victim's employer, coworkers, family members, friends, or even strangers—can cause 'public degradation, social isolation, and professional humiliation for the victims.'"[216] Forty-eight states, plus the District of Columbia and Guam, have enacted legislation to address revenge porn.[217]

CDA Section 230 has historically sheltered websites from the consequences of hosting revenge pornography.[218] Despite the fact that revenge porn is a crime in most states, "[t]he CDA essentially leaves internet service providers (ISPs) and host sites largely free to host nonconsensual pornography with impunity."[219] At present, websites have no obligation to remove content that constitutes an ongoing tort or crime, thus leaving the victims of these postings without a remedy. "The absence of a bona fide takedown remedy in the DMCA and the immunity provided to ISPs by the current iteration of Section 30 of the Communications Decency Act permit the offending images to remain online in perpetuity. This causes ongoing harm to the victims of nonconsensual pornography."[220]

In *GoDaddy.com v. Toups*,[221] Hollie Toups, the victim of revenge porn, filed an action against Texxxan.com and its web-host, GoDaddy.com, for intentional infliction of emotional distress, violation of the Texas Penal Code, and gross negligence.[222] The trial court denied the dismissal, but the Court of Appeals of Texas reversed the order, "[a]llowing plaintiffs' [sic] to assert any cause of action against GoDaddy for publishing content created by a third par-

---

[215] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014).

[216] State v. VanBuren, 214 A.3d 791, 795 (Vt. 2019). "The images may haunt victims throughout their lives." *Id*. (describing lasting effects of having one's nude photos posted online and stating that "this type of cyber crime can leave a lasting digital stain, one that is nearly impossible to fully erase").

[217] *48 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER CIV. RTS. INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws [https://perma.cc/VB2N-S2KU].

[218] Meghan Fay, *The Naked Truth: Insufficient Coverage for Revenge Porn Victims at State Law and the Proposed Federal Legislation to Adequately Redress Them*, 59 B.C. L. REV. 1839, 1852–53, (2018) ("Section 230, in essence, bars victims from suing revenge porn websites and provides no recourse for the removal of the explicit content.").

[219] Jessica A. Magaldi et al., *Revenge Porn: The Name Doesn't Do Nonconsensual Pornography Justice and the Remedies Don't Offer the Victims Enough Justice*, 98 OR. L. REV. 197, 199 (2020).

[220] *Id*. at 209.

[221] GoDaddy.com, LLC v. Toups, 429 S.W.3d 752 (Tex. Ct. App. 2014).

[222] *Id*. at 753.

ty, or for refusing to remove content created by a third party would be squarely inconsistent with [S]ection 230."[223]

The gist of the claim against GoDaddy was that it negligently failed to remove the revenge pornography after it received notice. The court ruled that GoDaddy had no takedown duty, even if it had knowledge of illegal activity, because Section 230 foreclosed victim's causes of action.[224] The court noted its concern that website owners have no duty to remove false and defamatory posts placed on the site by third parties, but ruled that the website owner had no liability for failing to remove defamatory posts.[225] The court observed that "[p]laintiffs fail to cite to any authority that supports their position that only constitutionally protected content gives rise to immunity under [S]ection 230."[226] The court's decision reflects a unanimous view of courts that websites have no duty to take down objectionable content even if it constitutes an ongoing tort with no First Amendment protections.

The court's statement that Section 230 extends to all content, not just constitutionally protected expression, illustrates how expansively the courts have interpreted the statutory shield. After a hearing, the trial court denied GoDaddy's motion to dismiss.[227] The Texas appeals court reversed this finding, ruling that CDA Section 230 imposes no takedown duty, which foreclosed all causes of action against the service provider.[228] The court reasoned that:

> Because GoDaddy acted only as an interactive computer service provider and was not an information content provider with regard to the material published on the websites, plaintiffs cannot maintain claims against GoDaddy that treat it as a publisher of that material. Moreover, plaintiffs cannot circumvent the statute by couching their claims as state law intentional torts.[229]

---

[223] Amanda L. Cecil, *Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography*, 71 WASH. & LEE L. REV. 2513, 2517 (2014) (quoting *GoDaddy.com*, 429 S.W.3d at 758).

[224] *GoDaddy.com*, 429 S.W.3d at 756 ("We noted our concern 'that section 230 does not provide a right to request a website's owner to remove false and defamatory posts placed on a website by third parties, and does not provide the injured person with a remedy in the event the website's owner then fails to promptly remove defamatory posts[.]' . . . We did not hold, as plaintiffs contend, that plaintiffs' state law claims were outside the scope of section 230's immunity provision.").

[225] *Id*.

[226] *Id*. at 759.

[227] *Id*. at 753.

[228] *Id*. at 762.

[229] *Id*. at 759.

D. Child Pornography

Child pornography is both a crime and tort because it "debases the most defenseless of our citizens."[230] "Both the State and Federal Governments have sought to suppress it for many years, only to find it proliferating through the new medium of the Internet."[231] "Children's engagement with pornography comes from three sources: (1) commercial pornography, (2) social media, and (3) search engines."[232] Child pornography has "so little free speech value that it was 'a category of material outside the protection of the First Amendment.'"[233] CDA Section 230, enacted "to protect children on the Internet, actually absolves Internet service providers ('ISPs') of responsibility for the criminal distribution of child pornography on websites."[234] Broadening the CDA Section 230 liability shield to safeguard websites hosting advertisements for child pornography is an insidious consequence of courts' expansive interpretation of what was once a limited liability shield for defamation as publisher claims.

A Florida appeals court freed AOL of any responsibility for trafficking of children that occurs on its service. In *Doe v. America Online, Inc.*,[235] Jane Doe, a mother, filed a six-count complaint against Richard Lee Russell and AOL to recover for emotional injuries suffered by her son, John Doe.[236] Doe "claimed that in early 1994, Russell lured John Doe (then eleven years old) and two other minor males to engage in sexual activity with each other and with Russell."[237] The *Doe* court indicated further that "Russell photographed and videotaped these acts and utilized AOL's 'chat rooms' to market the photographs and videotapes, and to later sell a videotape to a man in Arizona[.]" The mother filed suit against AOL and one of its users, alleging that user was offering for sale obscene material involving the mother's son.[238]

Count One of Doe's complaints stated:

> [T]hat AOL violated section 847.011(1)(a), Florida Statutes (1995), by knowingly allowing and permitting Russell "to sell, distribute, transmit or offer to sell, distribute or transmit photographs and videotape containing the images of the minor Plaintiff, JOHN DOE, which were unlawful and obscene." In count two, she alleged that AOL violated section 847.0135(2), Florida Statutes, the

---

230 United States v. Williams, 553 U.S. 285, 307 (2008).

231 *Id.*

232 Byrin Romney, *Screens, Teens, and Porn Scenes: Legislative Approaches to Protecting Youth from Exposure to Pornography*, 45 VT. L. REV. 43, 105 (2020).

233 Devon Ishii Peterson, *Child Pornography on the Internet: The Effect of Section 230 of the Communications Decency Act of 1996 on Tort Recovery for Victims Against Internet Service Providers*, 24 U. HAW. L. REV. 763, 792 (2002) (quoting New York v. Ferber, 458 U.S. 747, 763 (1982)).

234 *Id.* at 764–65.

235 Doe v. Am. Online, Inc., 718 So. 2d 385 (Fla. Dist. Ct. App. 1998).

236 *Id.* at 386.

237 *Id.*

238 *Id.*

> Computer Pornography and Child Exploitation Prevention Act of 1986, by allowing Russell to distribute an advertisement offering "a visual depiction of sexual conduct involving [John Doe]" and by allowing Russell to sell child pornography, thus aiding in the sale and distribution of child pornography. In count three, she claimed that section 847.0135, Florida Statutes, is specifically designed to protect a certain class of persons, and its violation constitutes negligence per se. In her fourth count, Doe asserted a claim for negligence because AOL knew, or should have known, that Russell and others like him used the service to market and distribute child pornographic materials, that it should have used reasonable care in its operation, that it breached its duty, and that the damages to John Doe were reasonably foreseeable as a result of AOL's breach. The two final counts were directed at Russell.[239]

The trial court granted AOL's motion to dismiss Doe's complaint, concluding that the immunities provided by Section 230 of the CDA applied to Doe's claims.[240] "The trial court stated that '[m]aking AOL liable for Russell's chat room communications would treat AOL as the "publisher or speaker" of those communications.'"[241] "The court also concluded, '[b]ecause Section 230 bars all of Doe's claims against AOL, the Court neither reaches nor decides whether AOL's state law grounds for dismissal also bars these claims.'"[242]

The Florida Appeals court held that CDA Section 230 applied even though the mother sought to hold the provider liable as a distributor of child pornography, rather than as a publisher or speaker, and that it preempted Florida statutory and common law.[243] The original purpose of CDA Section 230 was to protect children, but this case reveals that enforcement of CDA Section 230 does the opposite by refusing to hold ISPs accountable for hosting or promoting child pornography on their services as illustrated by an Ohio lawsuit:

> [T]he plaintiff sued the U Got Posted operators after her ex-boyfriend posted sexually explicit photos of her when she was sixteen years old and listed her full name and city of residence. She asserted civil child pornography claims (which were likely immunized under CDA § 230) and violation of Ohio's statutory and common law right of publicity law (which may not have been).[244]

E. Hosting Sexually Predatory Content

There is clearly no First Amendment interest in the advertising and sale of illicit, non-consensual videos of persons undressing posted to the Internet. Just as with terrorist content posted by ISIS or Hamas and unconsented pornographic postings, online harassment is not protectable free expression. Still, courts

---

[239] *Id*.
[240] *Id*. at 387.
[241] *Id*.
[242] *Id*.
[243] *Id*. at 388–89.
[244] Andrew Gilden, *Sex, Death, and Intellectual Property*, 32 HARV. J.L. & TECH. 67, 85 (2018).

have been reluctant to recognize new duties such as the negligent failure to warn.

In *Doe v. MySpace, Inc.*,[245] the Fifth Circuit affirmed that Section 230 of the CDA barred claims alleging that MySpace negligently failed to keep minors off its website or to take measures to keep predators from communicating with minors.[246] The court also rejected the plaintiff's argument that MySpace was classifiable as a content creator. The court found that this argument was not presented in the lower court and thus barred.[247] The court held,

> without considering the Does' content-creation argument, that their negligence and gross negligence claims are barred by the CDA, which prohibits claims against Web-based interactive computer services based on their publication of third-party content. 47 U.S.C. § 230(c)(1), (e)(3). Because we affirm the district court based upon the application of § 230(c)(1), there is no need to apply § 230(c)(2), or to assess the viability of the Does' claims under Texas common law in the absence of the CDA.[248]

In *Beckman v. Match.com*,[249] a victim of a sexual assault and knife attack sued the online dating service for negligence in allowing a predator to contact victims through their services. The "plaintiff argue[d] that Match.com failed 'to protect her from individuals trolling the website to further criminal activity' by 'exposing Plaintiff to a serial murderer who used the website as a vessel to facilitate attacks on unsuspecting women,' and 'by exposing Plaintiff to a serial killer who used Defendant's service'" to brutally attack her.[250] The court held that the fatal flaw in plaintiff's attempt to focus on Match.com's failure to warn or negligent misrepresentation "is that all of Match.com's conduct must trace back to the publication of third-party user content or profiles. Match.com is a website that publishes dating profiles."[251]

The court decided that the plaintiff's cause of action was based entirely on "third-party content published by Match.com on its website."[252] The court declared that Section 230 of the CDA precluded a lawsuit for enabling a sexual predator "to post a profile on its website that plaintiff ultimately saw and responded to," thus leading to the predator assaulting her.[253] Negligent warning cases are a difficult battle for plaintiffs because of CDA Section 230 and the court's disinclination to recognize new duties.

---

[245] Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008).
[246] *Id.* at 413.
[247] *Id.* at 422.
[248] *Id.*
[249] Beckman v. Match.com, No. 2:13-CV-97 JCM NJK, 2013 WL 2355512 (D. Nev. May 29, 2013).
[250] *Id.* at *4.
[251] *Id.* at *5.
[252] *Id.*
[253] *Id.* at *3 (citation omitted).

In the linked cases of *John Does v. Franco Productions*[254] and *Doe v. GTE Corp.*,[255] CDA Section 230 prohibited legal redress for the injured victims. *John Does* "was a class action brought on behalf of a group of Illinois State University athletes who were videotaped without their consent in 'various stages of undress by hidden cameras in restrooms, locker rooms, or showers.'"[256] The Illinois college student athletes learned of the existence of the secret films of them from a newspaper story about the adult services website:[257]

> [T]he defendants used hidden cameras to film college athletes in locker rooms, restrooms, and wrestling meets. The secret videotapes were advertised as "hot young dudes" and sold on the Internet. The tapes carried names like "Straight Off the Mat" and "Voyeur Time" and depicted hundreds of young athletes in various degrees of nudity.[258]

A federal jury "awarded $506 million against the Internet distributors for compensatory and punitive damages based upon invasion of privacy, unlawful use of the plaintiffs' images for monetary gain, and mail and wire fraud under civil RICO laws."[259] The college students had no means to uncover the pornographers, rendering the award uncollectable.[260]

The Illinois State college athletes also filed suit against the sites that hosted these illegal films that invaded the privacy of college athletes. In *Doe v. GTE Corp.*,[261] the Illinois athletes filed a complaint against three defendants that provided Internet access and web hosting services for the pornographer, Franco Productions.[262] However, the Seventh Circuit ruled that the Illinois State college athletes had no cause of action against the ISPs that had profited from hosting the adult services websites because of Section 230.[263] The imposition of

---

[254] John Does v. Franco Prods., No. 99 C 7885, 2000 U.S. Dist. LEXIS 8645 (N.D. Ill. June 21, 2000).

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

[256] Michael L. Rustad & Thomas H. Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOK. L. REV. 1, 100–01 (2002) (citation omitted).

[257] *Franco Prods.*, 2000 U.S. Dist. LEXIS 8645, at *2.

[258] Rustad & Koenig, *supra* note 67, at 111 (explaining *Franco* case).

[259] *Id.*

[260] *See id.*

[261] Doe v. GTE Corp., 347 F.3d 655, 656 (7th Cir. 2003).

[262] The federal district court described the case as involving "intercollegiate athletes who, without their knowledge or consent, were videotaped in various stages of undress by hidden cameras in restrooms, locker rooms, or showers." *Franco Prods.*, 2000 U.S. Dist. LEXIS 8645, at *1–2. "The resulting videotapes were sold by various means, including web sites hosted by Genuity.net and TIAC.Net that included still images of the Plaintiffs taken from the videotapes." *Id.*

[263] The district court dismissed all claims against the providers, citing 47 U.S.C. § 230(c) (2000). *GTE Corp.*, 347 F.3d at 656. "After the judgment became final with the resolution or dismissal of all claims against all other defendants—the defaulting defendants were ordered to pay more than $500 million. . . ." *Id.* at 656–57 (citation omitted). The $500 million judgment is uncollectable because the adult services defendants vanished. *See* Rustad &

distributor liability would give legal recourse for these athletes, and many other victims of online misconduct, by requiring ISPs to remove illegal or objectionable material.

The Illinois State athletes were not even able to obtain discovery to determine how extensively GTE and the other web hosts participated in "designing or creating or maintaining the web site, ranging anywhere from completely creating, writing, organizing and originally editing content before it is posted and changing, updating, adding or deleting content thereafter, to providing the template or architecture of the web site."[264] Section 230 precludes a plaintiff from discovering what the service provider knew about prior similar incidents or whether it had a contract or other close connection to the anonymous defendant. "Many of the primary defendants in cybertorts are spiteful individuals who use anonymous or pseudonymous identities to perpetrate their wrongdoing."[265] CDA Section 230's no duty rule for online intermediaries makes it difficult to hold the primary wrongdoer accountable.

These cases demonstrate how U.S. courts have enlarged Section 230 immunity to shield predatory content that does not have any First Amendment expression. The First Amendment does not apply to wrongdoers who surreptitiously film college athletes in various stages of undress. The primary wrongdoers are liable for intentional torts such as the invasions of privacy, false light, and public disclosure of private facts, as well as the intentional infliction of emotional distress. Website host liability can be predicated on gross negligence for designing a website enabling the ongoing tort of the invasion of privacy for these college athletes.

F. Systematic Campaign of Online Harassment

CDA Section 230 also shields methodical sexual harassment and ongoing torts by users of their services. In *Herrick v. Grindr LLC*, Section 230 closed out a tort plaintiff's claims against Grindr, an Internet-based dating application.[266] Matthew Herrick filed suit against Grindr, asserting diverse "tort and products liability claims—based in part on Grindr's failure to warn users of its 'inherently dangerous product' and to implement standard security measures"[267] after the tort victim's ex-boyfriend created a phony Grindr profile to impersonate him.[268] Herrick's ex-boyfriend characterized the plaintiff as HIV positive but still seeking unprotected sex, even "group sex" with other men, and

Koenig, *supra* note 67, at 111 ("The federal court's default judgment against the primary defendants was uncollectible because they fled to an offshore haven.").

[264] *Franco Prods.*, 2000 U.S. Dist. LEXIS 8645, at *7.

[265] Rustad & Koenig, *supra* note 67, at 123 (explaining rarity of cybertort cases in U.S. courts).

[266] Herrick v. Grindr LLC, 765 F. App'x 586, 588–89 (2d Cir. 2019).

[267] Gilden, *supra* note 241, at 86 (citation omitted).

[268] *Herrick*, 765 F. App'x at 590.

stated that "Herrick would try to turn the men away but that his resistance would just be part of the fantasy."[269]

Matthew Herrick's attorney described his client's ordeal and Grindr's failure to delete the fictious profile that impersonated the plaintiff:

> The impersonating profile sent men for fisting, orgies, and aggressive sex. They were told that if he resisted, that was part of the fantasy. They should just play along. It seemed clear to me that Gutierrez was endeavoring to do more than harass and frighten Matthew. He appeared to be trying to recruit unwitting accomplices to perpetrate sexual assaults.
>
> Like many of my clients, before coming to see me Matthew had tried everything he could to take care of the problem on his own. He filed more than a dozen complaints with his local police precinct . . . .
>
> By the time Matthew came to me for help, the Manhattan district attorney opened an investigation and he'd gotten a family court "stay away" order, but neither was stopping the traffic of strangers coming to his home and work for sex. He also did everything he could to get the imposter profiles taken down.[270]

Herrick provided evidence that stalkers lurked outside his apartment, knocked forcefully on his door, refused to leave, and confronted him at his place of employment. Herrick's attorney described his client's nightmare and his frustration with Grindr's failure to remove the impersonating profile:

> "I emailed and called and begged them to do something," Matthew told me, the frustration rising in his voice. His family and friends also contacted Grindr about the fake profiles—in all, about 50 separate complaints were made to the company, either by Matthew or on his behalf. The only response the company ever sent was an automatically generated email: "Thank you for your report."
>
> All in all, more than 1,400 men, as many as 23 in a day, arrived in person at Matthew's home and job over the course of 10 months.[271]

Herrick contacted Grindr to report the impersonating profiles, but Grindr responded only with an automated form and took no action to disable the false profiles. Herrick attempted to circumvent the CDA Section 230 liability shield by asserting a wide variety of claims, but the appeals court held Section 230 applied, as the application was "a provider or user of an interactive computer service," and the claims were "based on information provided by another information content provider" (the ex-boyfriend).[272] Herrick's attorney contended that his client's case was proof that CDA Section 230 creates disincentives to expeditiously disable deplorable content:

---

[269] Petition for a Writ of Certiorari at 9, 17a, Herrick v. Grindr LLC, 140 S. Ct. 221 (2019) (No. 19-192); Gilden, *supra* note 241, at 86.

[270] Carrie Goldberg, *Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must Be Fixed*, LAWFARE (Aug. 14, 2019, 8:00 AM), https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed [https://perma.cc/W9SZ-ZM4V].

[271] *Id*.

[272] *Herrick*, 765 F. App'x at 589–90.

> The question is whether the immunity provided to platforms by Section 230 of the Communications Decency Act has any meaningful limits at all. As discussion of Section 230 has become more frequent and mainstream in the last several months, with solemn events—like 8chan apparently hosting the suspected murderer's racist screed in the El Paso shooting and Facebook being painfully slow to remove the live-streamed Christchurch massacre—forcing the U.S. to rethink liability for third-party platforms, it is important that this conversation not be conducted in fuzzy abstracts. Rather, everyone involved in the discussion must look at the stories of real individuals who have been deeply wounded, their lives upended, because of platforms turning a blind eye or willfully ignoring injuries their products facilitate. In all cases involving a Section 230 immunity defense, there are two stories—the story of the individual and the story of the litigation.[273]

G. A "Failure to Warn" Crack in the CDA Section 230 Shield

In a rare exception to the one impervious Section 230 shield, the Ninth Circuit reversed a CDA Section 230 dismissal of a negligent failure to warn cause of action in *Jane Doe No. 14 v. Internet Brands Inc*.[274] In *Internet Brands*, the plaintiff, who was an aspiring model, posted information about herself on the Model Mayhem website.[275] "Model Mayhem is a networking website, found at modelmayhem.com, for people in the modeling industry."[276] The plaintiff "allege[d] that two rapists used the website to lure her to a fake audition, where they drugged her, raped her, and recorded her for a pornographic video."[277] The rapists did not post their own profiles, but preyed upon profiles on Model Mayhem posted by models, contacted potential victims with fake identities posing as talent scouts, and lured the victims to south Florida for modeling auditions.[278]

Jane Doe contended "that Internet Brands knew about the activities of [the rapists] but failed to warn Model Mayhem users that they were at risk of being victimized" and "that this failure to warn caused her to be a victim of the rape scheme."[279] The court ruled that Section 230 of the CDA does not apply because Jane Doe did "not seek to hold Internet Brands liable as a 'publisher or speaker' of content someone posted on the Model Mayhem website, or for Internet Brands' failure to remove content posted on the website."[280]

---

[273] Goldberg, *supra* note 267.

[274] Doe No. 14 v. Int. Brands, Inc., 767 F.3d 894, 900 (9th Cir. 2014), reh'g granted, *opinion withdrawn*, 778 F.3d 1095 (9th Cir. 2015), and *opinion withdrawn and superseded sub nom.* Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016).

[275] *Id.* at 895.

[276] *Id.*

[277] *Id.*

[278] *Id.* at 895–96.

[279] *Id.* at 896.

[280] *Id.* at 897.

Internet Brands purchased the Model Mayhem website from the original developers.[281] "Shortly after the purchase, [it] learned of how [the rapists] were using the website."[282] "In August 2010, Internet Brands sued the [developers] for failing to disclose the potential for civil suits arising from the activities of [the rapists]."[283] "By that time, according to Jane Doe, Internet Brands knew that [the rapists] had used Model Mayhem to lure multiple women to the Miami area to rape them."[284]

The court refused to bar Jane Doe's failure to warn claim, reasoning that it would stretch CDA Section 230 beyond its statutory purpose.[285] The court distinguished Internet Brands acting as a publisher or speaker of user content from a failure to warn claim.[286] "That does not mean the failure to warn claim seeks to hold Internet Brands liable as the 'publisher or speaker' of user content" because "[p]ublishing activity is a but-for cause of just about everything Model Mayhem is involved in."[287]

> Barring Jane Doe's failure to warn claim would stretch the CDA beyond its narrow language and its purpose. To be sure, Internet Brands acted as the "publisher or speaker" of user content by hosting Jane Doe's user profile on the Model Mayhem website, and that action could be described as a "but-for" cause of her injuries.[288]

The court concluded that "[t]he CDA does not bar Jane Doe's failure to warn claim," but did not make any conclusion about "the viability of the failure to warn allegations on the merits."[289] *Internet Brands* is "best read as holding that the CDA does not immunize an [interactive computer service] from a failure to warn claim when the alleged duty to warn arises from something other than user-generated content."[290]

H. Liability of Platforms for Hosting the Sale of Dangerously Defective Products

Products liability is a field of tort law that ensures "that the costs of injuries resulting from defective products are borne by the manufacturers that put such products on the market rather than by the injured persons who are powerless to

---

[281] *Id*. at 896.
[282] *Id*.
[283] *Id*.
[284] *Id*.
[285] *See id*. at 898.
[286] *See id*.
[287] *Id*. at 899.
[288] *Id*.
[289] *Id*. at 900.
[290] In re Facebook, Inc., 625 S.W.3d 80, 95 (Tex. 2021) (quoting Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 592 (S.D.N.Y. 2018)).

protect themselves."[291] Products liability maintains that manufacturers, distributors, suppliers, retailers, and anyone in the chain of distribution are liable for compensating consumers injured by a dangerously designed product, the failure to warn of known defects, and manufacturing defects.[292]

In the Internet-based economy, many substandard software cases will usually have a number of defendants (e.g., product manufacturer, hardware vendor, software licensor, and mobile network operator) involved in the creation of the technology and/or provision of the various components and services required for operation of modern products such as autonomous vehicles.[293] The Illinois Supreme Court describes the policy justification for extending strict liability to such parties:

> [T]he loss caused by unsafe products should be borne by those who create the risk of harm by participating in the manufacture, marketing and distribution of unsafe products; who derive economic benefit from placing them in the stream of commerce, and who are in a position to eliminate the unsafe character of the product and prevent the loss.[294]

The case for the courts' recognition of products liability for Internet platforms like Amazon.com is that they play an important role in advertising and distribution. It is a fundamental law and economics principle to impose liability on least cost avoiders.[295] The manufacturer is in a superior position to know when its software-driven product is suitably designed and safely made for its intended purpose. Every party in the chain of distribution chain should be held accountable. Imposing strict liability on every party in the distribution including Internet platforms encourages safety in design and production and adequate warnings of known product dangers. The increase in the purchase price of individual units should be acceptable to the user because "it results in added assurance of protection."[296]

---

[291] Jackson v. Johns-Manville Sales Corp., 727 F.2d 506, 525 (5th Cir. 1984), *on reh'g*, 750 F.2d 1314 (5th Cir. 1985) (quoting State Stove Mfg. Co. v. Hodges, 189 So. 2d 113, 120 (Miss. 1966)) (discussing policy objectives of strict liability in reallocating the cost of injury to the responsible manufacturer).

[292] *See Products Liability*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[293] *See* Araz Taeihagh & Hazel Si Min Lim, *Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks*, TRANSP. REVS. 1, 8–9 (2018).

[294] Garber v. Amazon.com, Inc., 380 F. Supp. 3d 766, 779 (E.D. Ill. 2019); *see also* Air & Liquid Sys. Corp. v. DeVries, 139 S. Ct. 986, 997 (2019) (Gorsuch, J., dissenting) ("The manufacturer of a product is in the best position to understand and warn users about its risks; in the language of law and economics, those who make products are generally least-cost avoiders of their risks. By placing the duty . . . on a product's manufacturer, we force it to internalize the full cost of any injuries caused. . . .").

[295] Nat'l Union Fire Ins. of Pittsburgh v. Riggs Nat'l. Bank of Wash. D.C., 5 F.3d 554, 557 (D.C. Cir. 1993) (Silberman, J., concurring) ("Placing liability with the least-cost avoider increases the incentive for that party to adopt preventive measures" that will "have the greatest marginal effect on preventing the loss.").

[296] Fasolas v. Bobcat of N.Y., Inc., 128 N.E.3d 627, 632 (N.Y. 2019) (citation omitted).

In contrast, CDA Section 230 protects Internet platforms from liability even though these platforms play an increasingly important role in Internet-related promotion, sale, and distribution. The Third Circuit acknowledged the substantial role played in products liability actions in the information age in its decision holding Amazon liable for its role as a seller.[297] The Third Circuit in *Oberdorf v. Amazon.com, Inc*.[298] concluded that Amazon was a 'seller' for purposes of Section 402A of the Second Restatement of Torts and thus subject to the Pennsylvania strict products liability law.[299]

In *Oberdorf*,[300] Heather Oberdorf, a consumer, purchased a dog collar from "The Furry Gang," a third-party vendor through Amazon:[301]

> [Oberdorf] returned home from work, put a retractable leash on her dog, and took the dog for a walk. Unexpectedly, the dog lunged, causing the D-ring on the collar to break and the leash to recoil back and hit [her] face and eyeglasses. As a result, [she] is permanently blind in her left eye.[302]

Oberdorf filed claims for strict products liability, negligence, breach of warranty, misrepresentation, and loss of consortium against Amazon in the federal court for the Middle District of Pennsylvania.[303]Oberdorf's products liability lawsuit asserted multiple claims including:

> [T]wo separate theories of strict product liability: (1) failure to provide adequate warnings regarding the use of the dog collar, and (2) defective design of the dog collar. She also asserts a variety of negligence theories, namely that Amazon was negligent in (1) distributing, inspecting, marketing, selling, and testing of the dog collar in an unreasonable manner; (2) allowing the dog collar to enter the stream of commerce in a dangerous condition; (3) failing to conduct a proper hazard analysis; (4) failing to follow the guidelines of the "safety hierarchy"; and (5) failing to provide the product with features, elements, precautions, or warnings that would have made it safer.[304]

The U.S. district court decided that Section 230 of the Communications Decency Act barred these claims.[305] The Third Circuit reversed, disagreeing with the lower court's finding that Amazon was not a seller.[306] "Amazon relies on this limitation as its defense, claiming that it is not a 'seller' because it merely provides an online marketplace for products sold by third-party vendors. We

---

[297] *See* Oberdorf v. Amazon.com Inc., 930 F.3d 136, 136–37, 153 (3d Cir. 2019), *reh'g en banc granted*, *opinion vacated*, 936 F.3d 182, 182–83 (3d Cir. 2019) (imposing strict liability on Amazon as a seller of a defective dog collar).

[298] *Id*. at 136.

[299] *Id*. at 153.

[300] *Id*. at 136.

[301] *Id*. at 142.

[302] *Id*. at 140.

[303] *Id*. at 142.

[304] *Id*. at 142–43.

[305] *Id*. at 143.

[306] *Id*. at 153–54.

disagree."[307] The appeals court applied a four-factor test determining Amazon was a seller:

> (1) Whether the actor is the "only member of the marketing chain available to the injured plaintiff for redress";
> (2) Whether "imposition of strict liability upon the [actor] serves as an incentive to safety";
> (3) Whether the actor is "in a better position than the consumer to prevent the circulation of defective products"; and
> (4) Whether "[t]he [actor] can distribute the cost of compensating for injuries resulting from defects by charging for it in his business, i.e., by adjustment of the rental terms."[308]

The Third Circuit concluded that the first factor weighed greatly in favor of a finding that Amazon was classifiable as a seller:

> Amazon contends that, just as every item offered at an auction house can be traced to a seller who may be amenable to suit, every item on Amazon's website can be traced to a third-party vendor. However, Amazon fails to account for the fact that under the Agreement, third-party vendors can communicate with the customer only through Amazon. This enables third-party vendors to conceal themselves from the customer, leaving customers injured by defective products with no direct recourse to the third-party vendor. There are numerous cases in which neither Amazon nor the party injured by a defective product, sold by Amazon.com, were able to locate the product's third-party vendor or manufacturer. In this case, Amazon's Vice President of Marketing Business admitted that Amazon generally takes no precautions to ensure that third-party vendors are in good standing under the laws of the country in which their business is registered. In addition, Amazon had no vetting process in place to ensure, for example, that third-party vendors were amenable to legal process. After Oberdorf was injured by the defective collar, neither she nor Amazon was able to locate The Furry Gang. As a result, Amazon now stands as the only member of the marketing chain available to the injured plaintiff for redress.[309]

The Third Circuit also found that extending strict liability to Amazon would create greater inducements for safety, rejecting Amazon's argument "that it does not have a relationship with the designers or manufacturers of products offered by third-party vendors."[310] The federal appeals court acknowledged, "Amazon does not have direct influence over the design and manufacture of third-party products," but stated "Amazon exerts substantial control over third-party vendors."[311] Amazon's role was more extensive than a sales agent that "in exchange for a commission merely accepted orders and arranged for product shipments. Amazon not only accepts orders and arranges for product shipments, but it also exerts substantial market control over product sales

---

[307] *Id*. at 143.
[308] *Id*. at 144.
[309] *Id*. at 145.
[310] *Id*. at 146.
[311] *Id*.

by restricting product pricing, customer service, and communications with customers."[312]

The court remarked that the third-party vendors enter into an agreement with Amazon, giving the online auction site control over many of their activities with the ultimate penalty of terminating their account.[313] The federal appeals court decided, "[t]herefore, Amazon is fully capable, in its sole discretion, of removing unsafe products from its website. Imposing strict liability upon Amazon would be an incentive to do so. The court also found that the second factor favored recognizing strict liability on Amazon. The second factor favors imposing strict liability on Amazon"[314] The court also found the third factor in favor of Amazon as a seller because it was "'in a better position than the consumer to prevent the circulation of defective products.'"[315] The court found Amazon to be:

> [U]niquely positioned to receive reports of defective products, which in turn can lead to such products being removed from circulation. Amazon's website, which Amazon in its sole discretion has the right to manage, serves as the public-facing forum for products listed by third-party vendors. In its contract with third-party vendors, Amazon already retains the ability to collect customer feedback: "We may use mechanisms that rate, or allow shoppers to rate, Your Products and your performance as a seller and Amazon may make these ratings and feedback publicly available." Third-party vendors, on the other hand, are ill-equipped to fulfill this function, because Amazon specifically curtails the channels that third-party vendors may use to communicate with customers: "[Y]ou may only use tools and methods that we designate to communicate with Amazon site users regarding Your Transactions . . . ." The third factor also weighs in favor of imposing strict liability on Amazon.[316]

The federal appeals court determined that the fourth factor also weighed heavily in favor of imposing strict liability on Amazon as a seller because it was positioned to "distribute the cost of compensating for injuries resulting from defects."[317] The Third Circuit reasoned that Amazon's indemnification agreement with the vendors revealed Amazon's role as being in the best position to distribute loss. The following clause of Amazon's agreement stated:

> You release us and agree to indemnify, defend, and hold harmless us, our Affiliates, and our and their respective officers, directors, employees, representatives, and agents against any claim, loss, damage, settlement, cost, expense, or other liability (including, without limitation, attorneys' fees) . . . .[318]

As the Third circuit noted:

---

312 *Id*. at 149.
313 *Id*. at 146.
314 *Id*.
315 *Id*. at 146–47.
316 *Id*.
317 *Id*. at 147.
318 *Id*.

> Moreover, Amazon can adjust the commission-based fees that it charges to third-party vendors based on the risk that the third-party vendor presents.
> Amazon's customers are particularly vulnerable in situations like the present case. Neither the Oberdorfs nor Amazon has been able to locate the third-party vendor, The Furry Gang. Conversely, had there been an incentive for Amazon to keep track of its third-party vendors, it might have done so.
> The fourth factor also weighs in favor of imposing strict liability on Amazon.[319]

The court concluded that Amazon was in the best position to distribute the cost of compensating customers for injuries caused by defects. Indemnification by vendors is more than a theoretical possibility (as it was for the auctioneer in *Musser*) because Amazon has indemnification agreements with its vendors. Amazon may also adjust the commission-based fees it charges vendors to account for the risk a product presents.[320] The federal appeals court ruled that Oberdorf could pursue strict products liability against Amazon, stating:

> For the above reasons, we hold that (1) Amazon is a "seller" for purposes of § 402A of the Second Restatement of Torts and thus subject to the Pennsylvania strict products liability law, and (2) Oberdorf's claims against Amazon are not barred by § 230 of the CDA except as they rely upon a "failure to warn" theory of liability. We will therefore affirm the dismissal under the CDA of the failure to warn claims. We will vacate the remainder of the judgment of the District Court and remand this matter for further proceedings consistent with this opinion.[321]

The Third Circuit noted that prior courts tended to concentrate on the nature of the duty claimed to have been violated.[322] Claims are precluded under the CDA, those decisions held, "whenever the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a publisher or speaker."[323] The CDA's immunity shield does not preclude a products liability claim, however, "just because it relates to publishing of information on the Internet."[324] The Third Circuit concluded that the strict liability claim was cognizable stating:

> [T]o the extent that [the plaintiff'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 [the plaintiff] is alleging that Amazon failed to provide or to edit adequate warnings regarding the use of the dog collar, we conclude that that activity falls within the publisher's editorial function. That is, Amazon failed to add necessary information to content of the website. For that reason, these failure to warn claims are barred by the CDA.[325]

---

[319] *Id*. at 147.
[320] *Id*.
[321] *Id*. at 153–54.
[322] *Id*. at 149.
[323] *Id*. at 152 (internal quotation marks omitted) (quoting Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1102 (9th Cir. 2009)).
[324] *Id*. at 152–53 (citations omitted).
[325] *Id*. at 153.

The court allowed Oberdorf's strict products liability action to go forward as it was connected to Amazon's role as a seller.[326] Some commentators have expressed alarm over the Third Circuit's decision, concluding that Amazon was a seller not entitled to CDA Section 230 immunity, while others praise the decision:

> The response to the opinion has been mixed, to say the least. Eric Goldman, for instance, has asked "are we at the end of online marketplaces?," suggesting that they "might in the future look like a quaint artifact of the early 21st century." Kate Klonick, on the other hand, calls the opinion "a brilliant way of both holding tech responsible for harms they perpetuate & making sure we preserve free speech online."[327]

A commentator acknowledges that the Third Circuit opinion offers an alternative way of circumventing CDA Section 230's liability shield:

> The Third Circuit's opinion offers a modest way that Section 230 could be changed—and, I would say, improved—to address some of the real harms that it enables without undermining the important purposes that it serves. To wit, Section 230's immunity could be attenuated by an obligation to facilitate the identification of users on that platform, subject to legal process, in proportion to the size and resources available to the platform, the technological feasibility of such identification, the foreseeability of the platform being used to facilitate harmful speech or conduct, and the expected importance (as defined from a First Amendment perspective) of speech on that platform.
>
> In other words, if there are readily available ways to establish some form of identify for users—for instance, by email addresses on widely-used platforms, social media accounts, logs of IP addresses—and there is reason to expect that users of the platform could be subject to suit—for instance, because they're engaged in commercial activities or the purpose of the platform is to provide a forum for speech that is likely to legally actionable—then the platform needs to be reasonably able to provide reasonable information about speakers subject to legal action in order to avail itself of any Section 230 defense. Stated otherwise, platforms need to be able to reasonably comply with so-called unmasking subpoenas issued in the civil context to the extent such compliance is feasible for the platform's size, sophistication, resources, etc.
>
> An obligation such as this would have been at best meaningless and at worst devastating at the time Section 230 was adopted. But 25 years later, the Internet is a very different place. Most users have online accounts—email addresses, social media profiles, &c—that can serve as some form of online identification.
>
> More important, we now have evidence of a growing range of harmful conduct and speech that can occur online, and of platforms that use Section 230 as a shield to protect those engaging in such speech or conduct from litigation. Such

---

[326] *Id*. at 153–54.

[327] Gus Hurwitz, *The Third Circuit's* Oberdorf v. Amazon *Opinion Offers a Good Approach to Reining in the Worst Abuses of Section 230*, TRUTH ON THE MKT.: SCHOLARLY COMMENT. ON L., ECON., & MORE (July 15, 2019), https://truthonthemarket.com/2019/07/15/the-third-circuits-oberdorf-v-amazon-opinion-offers-a-good-approach-to-reining-in-the-worst-abuses-of-section-230 [https://perma.cc/9M5C-XJDP].

> speakers are clear bad actors who are clearly abusing Section 230 facilitate bad conduct. They should not be able to do so.[328]

A New Jersey federal court also allowed products liability claims to go forward against Amazon, despite the CDA Section 230 liability shield. In *Papataros v. Amazon.com, Inc.*,[329] Papataros filed a products liability lawsuit for injuries allegedly caused by a defective scooter that she purchased from Coolreall on the interactive website Amazon.com.[330] "On the listing page for the scooter, between the 'in stock' link and the 'add to cart' link, the website stated, 'Sold by Coolreall and Fulfilled by Amazon.'"[331] After her purchase, Amazon sent her "an e-mail confirmation from Amazon that read '[t]hank you for shopping with us.'"[332] Amazon enters into agreements with third-party sellers and requires indemnification for any claims.[333]

The maker and distributor of the scooter did not respond to Papataros' products liability complaint, while Amazon filed a motion for summary judgment, contending it was exempt from liability under Section 230 of the Communications Decency Act (CDA), 47 U.S.C. § 230(c)(1).[334] The court relied upon the *Oberdorf* decision in dismissing the failure-to-warn claims, while preserving Papataros' strict liability claim.[335] The *Papataros* court stated, "[t]o the extent that Papataros has brought claims against Amazon for failure to provide or edit adequate warnings on its website, those claims are barred by the CDA. Papataros's strict liability claims under the NJPLA, however, are not barred by the CDA."[336] The court found that the express and implied warranty claims were not foreclosed by CDA Section 230.[337]

The court also ruled that Section 230 did not shield Amazon from liability in *State Farm Fire and Casualty Company v. Amazon.com, Inc*.[338] In *State Farm*, Cain purchased a bathtub faucet adapter from a third-party seller on Amazon.com that malfunctioned, flooding his home, which was insured by State Farm.[339] State Farm paid to repair Cain's home, and filed suit against "Amazon.com, Inc. for strict product liability under Wis. Stat. § 895.047."[340]

---

328 *Id*.

329 Papataros v. Amazon.com, Inc., Civ. No. 17-9836 (KM) (MAH), 2019 WL 4011502 (D. N.J. Aug. 26, 2019).

330 *Id*. at *1.

331 *Id*.

332 *Id*.

333 *Id*. at *2.

334 *Id*. at *1.

335 *Id*.

336 *Id*. at *18.

337 *See id*.

338 State Farm Fire & Cas. Co. v. Amazon.com, Inc., 390 F. Supp. 3d 964, 964 (W.D. Wis. 2019).

339 *Id*. at 966.

340 *Id*.

"The question before the court is whether Amazon can be held liable under Wisconsin product liability law for a product sold by a third party through Amazon.com."[341]

The court declined to enter summary judgment in favor of Amazon, ruling "(1) that it is not a 'seller' within the meaning of § 895.047; and (2) that it cannot be held liable for third-party content on its website because § 230(c)(1) of the Communications Decency Act prohibits treating it as a 'publisher.'"[342] The court reasoned further that:

> Amazon does not merely provide a marketplace where third-parties sell to Amazon customers. Amazon was so deeply involved in the transaction with Cain that Wisconsin law would treat Amazon as an entity that would be strictly liable for the faucet adapter's defects, if, as in this case, the manufacturer cannot be sued in Wisconsin. And the Communications Decency Act does not immunize Amazon because State Farm does not seek to impose liability on Amazon merely because it posted some third-party content.[343]

The court framed the issue as whether Amazon is "a peripheral entity like an auctioneer or is it an integral part of the chain of distribution[.]"[344] The court ruled that:

> The undisputed facts show that Amazon is an integral part of the chain of distribution, an entity well-positioned to allocate the risks of defective products to the participants in the chain. Amazon provided the only conduit between XMJ, the Chinese seller, and the American marketplace. Without Amazon, XMJ products would not be available at all in Wisconsin. Amazon did not directly set the price for the faucet adapter, but it set the substantial fees that it would retain for itself, so it was positioned to insure against the risk of defective products. As part of the FBA agreement, Amazon required XMJ to register each product, and Amazon reserved the right to refuse to sell any of them. So, Amazon was in a position to halt the flow of any defective goods of which it became aware. And Amazon took steps to protect itself by requiring XMJ to indemnify Amazon. Amazon also implicitly represented that the adapter was safe by listing it for sale among its own products, and it expressly guaranteed timely delivery in good condition. And, under Amazon's A to Z guarantee, Amazon agreed to process returns and refunds if XMJ did not respond. Amazon took on all the roles of a traditional—and very powerful—reseller/distributor. The only thing Amazon did not do was take ownership of XMJ's goods.[345]

Advances in artificial intelligence, robotics, 3D printing, the Internet of Things, and other information technologies inevitably will create future products liability cases, making the Amazon ruling an important precedent. Every substantive field of law is being reworked in response to the Internet, so it is not surprising that CDA Section 230, a twenty-five-year-old statute, needs to be

---

[341] *Id*.
[342] *Id*.
[343] *Id*. at 966.
[344] *Id*. at 972.
[345] *Id*.

updated to address the dysfunctions of courts stretching a narrow provision applicable to publisher's liability to all torts and all online intermediaries.

Finally, in an increasingly cross-border legal environment, tortfeasors can defame, invade privacy, and misappropriate trade secrets at the click of a mouse in hundreds of jurisdictions simultaneously. Therefore, harmonization of Internet law between the United States and the European Union is highly desirable. Part III contains our proposal to extend notice-and-takedown from copyright infringement to cybertorts, which would harmonize U.S. and European online intermediary law.

III. PROPOSAL TO AMEND CDA SECTION 230 TO RECOGNIZE A CYBERTORT PLAINTIFF'S RIGHT OF NOTICE-AND-TAKEDOWN

Greater than twenty proposals to reduce or eliminate Section 230 were under congressional consideration in 2020,[346] and more CDA Section 230 reform proposals were being developed.[347] The Democrats and Republicans both call for changing CDA Section 230.[348] Section 230 was a major issue during the 2020 United States presidential election, where both Joseph Biden and Donald Trump called for changing CDA Section 230. Progressives "accuse tech com-

---

[346] For example, on October 20, 2020: Congresswoman Anna G. Eshoo (CA-18) and Congressman Tom Malinowski (NJ-7) introduced the *Protecting Americans from Dangerous Algorithms Act*, legislation to hold large social media platforms accountable for their algorithmic amplification of harmful, radicalizing content that leads to offline violence. The bill narrowly amends Section 230 of the Communications Decency Act to remove liability immunity for a platform if its algorithm is used to amplify or recommend content directly relevant to a case involving interference with civil rights (42 U.S.C. § 1985); neglect to prevent interference with civil rights (42 U.S.C. § 1986); and in cases involving acts of international terrorism (18 U.S.C. § 2333). 42 U.S.C. §§ 1985 and 1986 are Reconstruction-era statutes originally designed to reach Ku Klux Klan conspirators and are central to a recent suit alleging Facebook facilitated militia violence in Kenosha, WI. 18 U.S.C. § 2333 is implicated in several lawsuits, including an earlier suit against Facebook, alleging its algorithm connected terrorists with one another and enabled physical violence against Americans. The bill applies only to platform companies with 50 million or more users.

Press Release, Congresswoman Anna G. Eshoo, Reps. Eshoo and Malinowski Introduce Bill to Hold Tech Platforms Liable for Algorithmic Promotion of Extremism (Oct. 20, 2020), https://eshoo.house.gov/media/press-releases/reps-eshoo-and-malinowski-introduce-bill-hold-tech-platforms-liable-algorithmic [https://perma.cc/2SWK-6JU5].

[347] *The Telecommunications Act's "Good Samaritan" Protection: Section 230*, DISRUPTIVE COMPETITION PROJECT, https://www.project-disco.org/section-230 [https://perma.cc/WG7T-XP7T].

[348] "Republicans and Democrats both want to repeal Section 230, but they want to replace it in diametrically opposed ways," said Mark Lemley, a Stanford Law School professor. "Democrats want more content moderation targeting hate speech and misinformation. Republicans want to apply the First Amendment to social media sites even if they are private actors." Bryan Mena & Duncan Agnew, *Republicans and Democrats Both Want to Repeal Part of a Digital Content Law, but Experts Say That Will Be Extremely Tough*, TEX. TRIB. (Jan. 21, 2021, 6:00 PM), https://www.texastribune.org/2021/01/21/section-230-internet-social-media [https://perma.cc/VRV4-UP8E].

panies of using Section 230's immunity to ignore the collateral damage of their users' bad behavior, such as racist or sexist messages in addition to disinformation and provocation spread by Trump on Twitter during most of his time in office."[349]

Joseph Biden, who was then a Presidential candidate, contended that: "[Section 230] should be revoked because [Facebook] is not merely an internet company. It is propagating falsehoods they know to be false, and we should be setting standards not unlike the Europeans are doing relative to privacy."[350] "Calls for reform have taken on new urgency as social media sites battle a flood of troubling content, including disinformation about the coronavirus vaccines, the outcome of the US presidential election and the deadly attack on the US Capitol."[351]

Republican leaders charge that CDA Section 230 is contrary to the public interest because "companies are using Section 230 as a cover to let them moderate content however they want, and are exercising anti-conservative bias in what they choose to take down."[352] Donald Trump castigated the leading American social media websites for anti-conservative "viewpoint bias."[353] President Trump established a panel to reform Section 230, arguing that leftists controlled "Facebook, Instagram, Twitter and Google."[354] In May of 2020, Trump issued an Executive Order limiting CDA Section 230's scope, contending that these websites should lose their legal immunity because of their pattern of disfavoring conservative viewpoints and deleting accounts without warning.[355]

Donald Trump's Executive Order, entered into during the last year of his Presidential term, directed the Federal Communications Commission to "clari-

---

[349] Felix Gillette & Laurence Arnold, *Why 'Section 230' Is Nub of Fights over Online Speech*, BLOOMBERG (Feb. 2, 2021, 2:49 PM), https://www.bloomberg.com/news/articles/2021-02-02/why-section-230-is-nub-of-fights-over-online-speech-quicktake [https://perma.cc/4CRV-PVLV].

[350] I. Bonifacic, *Joe Biden Says Facebook Spreads 'Falsehoods They Know to Be False.'*, ENGAGET (Jan. 17, 2021), https://www.engadget.com/2020-01-17-joe-biden-section-230-repeal-interview.html [https://perma.cc/S7ZS-KMUN].

[351] Marguerite Reardon, *Section 230: How It Shields Facebook and Why Congress Wants Changes*, C/NET (Oct. 6, 2021, 5:00 AM), https://www.cnet.com/news/section-230-how-it-shields-facebook-and-why-congress-wants-changes [https://perma.cc/Y23E-XQPD].

[352] Angela Chen, *What Is Section 230 and Why Does Donald Trump Want to Change It?*, MIT TECH. REV. (Aug. 13, 2019), https://www.technologyreview.com/2019/08/13/610/section-230-law-moderation-social-media-content-bias [https://perma.cc/5HPE-AFWR].

[353] Cristiano Lima, *How a Widening Political Rift over Online Liability Is Splitting Washington*, POLITICO, (July 9, 2019, 2:07 PM), https://www.politico.com/story/2019/07/09/online-industry-immunity-section-230-1552241 [https://perma.cc/3AHV-B38K].

[354] John D. McKinnon & Alex Leary, *Trump Considers Forming Panel to Review Complaints of Online Bias*, WALL ST. J. (May 23, 2020, 2:00 PM), https://www.wsj.com/articles/trump-considers-forming-panel-to-review-complaints-of-online-bias-11590238800 [https://perma.cc/SBQ5-5PMD].

[355] Exec. Order No. 13, 925, 85 Fed. Reg 106 (May 28, 2020).

fy" the law in a number of ways, proposing that editing content could lead to a platform forfeiting its protections under Section 230, as well as looking at whether it uses "deceptive acts or practices" to moderate, or if those practices are "inconsistent with [its] terms of service."[356] "On May 14, 2021, President Biden issued an executive order revoking, among other things, his predecessor's action (Executive Order 13295 of May 28, 2020) that directed the executive branch to clarify certain provisions under Section 230 of the Communications Decency Act."[357] Republicans' calls for revoking CDA Section 230 continued in 2021. Senator Lindsey Graham's bill, for example, would "repeal Section 230 on January 1, 2023, unless Congress acts sooner."[358]

Our proposal in this Part of the Article reforms CDA Section 230 rather than revoking it. Congress should update CDA Section 230 to address its excesses. Specifically, Congress should impose a nondelegable duty on online intermediaries to remove content constituting ongoing cybertorts or crimes once the ISP or other intermediary acquires actual notice of illegal content devoid of any First Amendment interest (CDA Section 230 notice-and-takedown). This reform proposal targets the current no duty rule that websites have no obligation to disable illegal content. As demonstrated in Parts I and II, the courts' expansion of CDA Section 230 has created, what is in effect, a "no liability zone" for all online intermediaries that leaves Internet users with no meaningful remedies for most cybertorts. Primary wrongdoers commit cybertorts anonymously, generally placing themselves beyond the reach of the law. Internet intermediaries such as ISPs are in the best position to avoid or mitigate the damage caused by content constituting cybertorts or crimes on their services.

Torts are increasingly committed on Twitter, blogs, social media sites, e-mail transmissions, and website postings. "For better or worse, wireless [I]nternet access, smart phones, tablet computers, social networking services like Facebook, and stream-of-consciousness communications via Twitter give an omnipresence to speech that makes any effort to trace First Amendment boundaries along the physical boundaries . . . a recipe for serious problems in our public schools."[359] Our notice-and-takedown (NTD) proposal will reverse the current CDA presumption that online intermediaries are shielded from liability for third-party torts by adapting provisions of the Digital Millennium Act's procedure with handling infringing content and the European Union's

---

[356] *Id*.

[357] Jeffrey D. Neuburger, *Biden Revokes Prior Administration's Executive Order on CDA Section 230*, 11 NAT'L L. REV. (May 17, 2021), https://www.natlawreview.com/article/president-revokes-prior-administration-s-executive-order-cda-section-230 [https://perma.cc/HX2P-LLNV].

[358] Press Release, Lindsey Graham, Graham Introduces Bill to Incentivize Section 230 Reform (Dec. 15, 2020), https://www.lgraham.senate.gov/public/index.cfm/2020/12/graham-introduces-bill-to-incentivize-section-230-reform [https://perma.cc/88WX-59T8].

[359] Layshock v. Hermitage Sch. Dist., 650 F.3d 205, 220–21 (3d Cir. 2011) (Jordan, J., concurring).

Digital Services Act governing online intermediary duties to remove illegal online content.

The current U.S. approach to Internet intermediary law is in sharp contrast to the DMCA and to the European Union's Digital Services Act (DSA), which imposes a duty on Internet platforms to disable or remove posted content constituting torts or crimes.[360] The DSA updates the EU's e-Commerce Directive's Internet intermediary rules.[361] The rise of the Internet creates the need for a global notice-and-takedown standard for content constituting ongoing cybertorts or crimes.

A. Digital Millennium Copyright Act's Notice-and-Takedown

"'The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty,'. . . and to update domestic copyright law for the digital age."[362] Two major provisions of the Act limited the liability for Internet service providers of copyright infringement in certain instances and created an exception to liability for making a copy of a computer program for computer maintenance and repair.[363] The "safe harbor" provision of the Digital Millennium Copyright Act limits the liability of online service providers for copyright infringement that occurs "by reason of the storage at the direction of

---

[360] Section 230 federal immunity for service providers is far broader than that offered in European countries. The United Kingdom, for example, adapts the traditional innocent disseminator defense to the on-line environment. It does not provide the carte blanche protection from liability that s. 230 of the American [CDA] does. An ISP, which by virtue of s. 1(3) is not an author, editor, or publisher; that takes reasonable care, having regard to the factors listed in s. 1(5); and does not know or have reason to believe that what he did caused or contributed to the publication of a defamatory statement, will be protected from liability for defamation. Michael Deturbide, *Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses*, 3 J. INFO. L. & TECH., 2000, at pt. 6.1.

[361] The EU Commission is amending, not replacing, the e-Commerce Directive to align with the need to update the Internet intermediary rules to account for new developments such as smart contracts; The resolution on 'Digital Services Act; adapting commercial and civil law rules for commercial entities operating online' calls for more fairness, transparency, and accountability for digital services' content moderation processes, ensuring that fundamental rights are respected, and guaranteeing independent recourse to judicial redress. The resolution also includes the request for a detailed 'notice-and-action' mechanism addressing illegal content, comprehensive rules about online advertising, including targeted advertising, and enabling the development and use of smart contracts.

Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM (2020) 825 final (Dec. 15, 2020), https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN [https://perma.cc/NV2M-STQ8].

[362] Viacom Int'l., Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012).

[363] Amy P. Bunk, *Validity, Construction, and Application of Digital Millennium Copyright Act* (Pub. L. No. 105–304, 112 Stat. 2860 (1998)), 179 A.L.R. Fed. 319 (2002).

a user of material that resides on a system or network controlled or operated by or for the service provider."[364] The DMCA

> requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[365]

A University of California Berkeley study summarized the DMCA's system of notice-and-takedown:

> The Digital Millennium Copyright Act (DMCA), passed by Congress in 1998, enshrined a compromise between copyright holders and online service providers (OSPs) on issues of copyright infringement. Its core feature was section 512, which established a safe harbor mechanism enabling copyright holders to send brief "takedown" requests to OSPs that were to be expeditiously honored and allowing the targets of these notices to contest requests using a "counter-notice" procedure. Since then, the law and procedure has guided copyright protection on the Internet and has been substantially adopted by several other countries.[366]

The DMCA gave copyright owners a remedy against those who did not themselves infringe a copyright but instead circumvented technological controls[367] and thereby enabled others to infringe "by creating both 'circumvention liability for digital trespass under [17 U.S.C.] § 1201(a)(1),' and 'trafficking liability under [17 U.S.C.] § 1201(a)(2) for facilitating such circumvention.'"[368] "The DMCA 'targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools),' even though it 'does not concern itself with the *use* of those materials after circumvention has occurred.'"[369] Just as the DMCA imposed liability on infringing enablers, our proposal makes websites and providers secondarily liable for failing to disable content constituting ongoing cybertorts or cybercrimes.

The DMCA's notice-and-takedown rules are found in the Online Copyright Infringement Liability Limitation Act (OCILLA Title II of the DMCA, separately titled the "Online Copyright Infringement Liability Limitation Act" (OCILLA)). The OCILLA

> was designed to "clarify[y] the liability faced by service providers who transmit potentially infringing material over their networks." But "[r]ather than embarking upon a wholesale clarification" of various copyright doctrines, Congress

---

364 17 U.S.C. § 512(c).

365 Universal City Studios, Inc. v. Corley, 273 F.3d 429, 440 (2d Cir. 2001).

366 Jennifer M. Urban, et al., *Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice*, 64 J. COPYRIGHT SOC'Y U.S.A. 371, 373 (2017).

367 *See Universal City Studios, Inc.*, 273 F.3d at 440.

368 United States v. Reichert, 747 F.3d 445, 448 (6th Cir. 2014).

369 *Id.*

> elected "to leave current law in its evolving state and, instead, to create a series of 'safe harbors[ ]' for certain common activities of service providers."[370]

The Second Circuit described how OCILLA established safe harbors giving service providers a way to limit their liability for copyright infringement for content posted on its services:

> OCILLA established a series of four 'safe harbors' that allow qualifying service providers to limit their liability for claims of copyright infringement based on (a) 'transitory digital network communications,' (b) 'system caching,' (c) 'information residing on systems or networks at [the] direction of users,' and (d) 'information location tools.' . . . To qualify for protection under any of the safe harbors, a party must meet a set of threshold criteria. First, the party must in fact be a "service provider," defined, in pertinent part, as "a provider of online services or network access, or the operator of facilities therefor.". . . A party that qualifies as a service provider must also satisfy certain "conditions of eligibility," including the adoption and reasonable implementation of a "repeat infringer" policy that "provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network.". . . In addition, a qualifying service provider must accommodate "standard technical measures" that are "used by copyright owners to identify or protect copyrighted works."[371]

The DMCA adapted copyright law to the Internet by developing new property rights where there had been none. The DMCA safeguards against excessive copyright liability by shielding Internet service providers from secondary copyright liability—assuming that they have a registered copyright agent and enforce a policy of removing infringing materials.[372] Section 512(c)(1)(B) states that defendants will be divested of their statutory shield from secondary liability if they "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity."[373]

Internet intermediaries have a safe harbor from secondary liability for copyright infringement so long as they observe the DMCA notice-and-takedown (NTD) rules. Amazon.com, for example, posts its "Notice and Procedure for Making Claims of Copyright Infringement" prominently in its user agreement.[374] The DMCA prohibits any person from circumventing a technological measure that controls access to a work protected under Title 17 Copyrights.[375] Under 17 U.S.C. § 512(c)(1)(A):

---

[370] Viacom Int'l, Inc. v. YouTube Inc., 676 F.3d 19, 27 (2d Cir. 2012) (citing S.Rep. No. 105–190 at 2 (1998)).

[371] *Id*. at 27.

[372] 17 U.S.C. § 512(d).

[373] 17 U.S.C. § 512(c)(1)(B).

[374] *Conditions of Use*, AMAZON (Last updated May 3, 2021). https://www.amazon.com/gp/help/customer/display.html?nodeId=GLSBYFE9MGKKQXM [https://perma.cc/4QLT-ANYM].

[375] 17 U.S.C. § 1201(a)(1)(A).

> [A] service provider can receive safe harbor protection only if it "(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;" "(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or" "(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material."[376]

To qualify for the storage exemption safe harbor for information residing on systems or networks, the Online Service Provider (OSP) must designate an agent to receive notice from copyright owners when there is a complaint of infringement.[377] The OSP must also post the agent's name on its website and register the agent with the Library of Congress' Copyright Office and provide the following required information:

> (A) the name, address, phone number, and electronic mail address of the agent[,] [and]
> (B) other contact information which the Register of Copyrights may deem appropriate.
> The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory.[378]

1. Safe Harbor for Internet Platforms

The DMCA established a "safe harbor," protecting the service provider from monetary, injunctive, or other equitable relief for infringement of copyright in the course of service such as YouTube's. "Congress also imported the 'red flag' test of § 512(c)(1)(A)(ii)," which divests service providers of their safe harbor immunity if they "fail[] to take action with regard to infringing material when it is 'aware of facts or circumstances from which infringing activity is apparent.'"[379] Service providers can lose the protection of the DMCA safe harbors if they have actual or apparent, also called "red flag," knowledge of infringing content.[380] "The copyright owner must show knowledge, actual or red flag, for [content] that infringed its copyright and are the subject of its claim. And for red flag knowledge, infringement must be apparent, not merely suspicious."[381]

---

[376] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1020 (9th Cir. 2013).

[377] 17 U.S.C. § 512(c)(2) (describing designated agent as condition for limitation on liability for copyright infringement).

[378] *Id*.

[379] Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 763 (9th Cir. 2007) (citing 17 U.S.C. § 512(c)(1)(A)(ii)).

[380] 17 U.S.C. § 512(c)(1)(A). 17 U.S.C. § 512(d)(1).

[381] Ventura Content, Ltd. v. Motherless, Inc. 885 F.3d 597, 610 (9th Cir. 2018).

The DMCA makes its safe harbor for Internet intermediary immunity contingent upon whether that party qualifies as a "service provider," as defined in the statute, adopts and reasonably implements a "repeat infringers" policy, and accommodates 'standard technical measures' used by copyright owners to protect their works.[382] If these requirements are satisfied, then the safe harbor additionally requires showings as to the service provider's lack of knowledge of infringement, its receipt of no direct financial benefit from the infringing activity, its compliance with DMCA takedown requests, and the designation of an agent for such requests.[383] The DMCA's safe harbor mechanism gives websites a mechanism for challenging deficient complaints:

> [The DMCA's] core feature was section 512, which established a safe harbor mechanism enabling copyright holders to send brief takedown requests to OSPs that were to be expeditiously honored, and allowing the targets of these notices to contest requests using a "counter-notice" procedure. Since then, the law and procedure has guided copyright protection on the Internet and has been substantially adopted by several other countries.[384]

Section 512 of the DMCA places the burden of notifying service providers of infringements upon the copyright owner or its agent. Websites must appoint an agent who will respond to takedown requests and designate contact information conspicuously on its websites. Notifications of claimed infringements must be in writing, with specified contents. Subject to certain provisions, noncompliant notifications shall not be considered in determining whether a service provider has actual or constructive knowledge.[385] Our NTD regime combines DMCA Section 512 procedures followed by 111 countries for addressing infringing content belonging to copyright owners with European Union rules for removing illegal content.[386]

This reform proposal would align U.S. NTD rules with the European Union community's e-Commerce Directive and the Digital Services Act.[387] "The E-Commerce Directive requires member states to acknowledge electronic contracts, establishes the liability of Internet intermediaries, provides for online dispute resolution, and harmonizes e-commerce rules."[388] The European Union's (EU) Digital Services Act updates the e-Commerce Directive's Internet intermediary rules for removing illegal content. Our proposed CDA Section

---

382 17 U.S.C. § 512(k)(1)(B) & (i)(1)(A–B).

383 *Id*. § 512(c)(1–2).

384 Urban, *supra* note 366, at 1.

385 Viacom Int'l, Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 115 (S.D.N.Y., 2013).

386 WORLD INTELLECTUAL PROPERTY ORGANIZATION, WIPO–ADMINISTERED TREATIES, *Contracting Parties WIPO Copyright Treaty (Total Contracting Parties: 110*), https://wipolex.wipo.int/en/treaties/ShowResults?search_what=C&treaty_id=16 [https://perma.cc/23NE-PX2S] (describing the WIPO Copyright Treaty obligations fulfilled by the DMCA and followed in 109 countries, including nearly every U.S. trading partner).

387 Rustad & Koenig, *supra* note 15, at 392.

388 *Id*.

230 NTD regime combines provisions of the DMCA's Section 512 with the EU's proposed DSA online intermediary rules, which will be explained in the next Part.

B. The EU's Notice & Takedown Regime

1. European Union's Cross-Border Takedown Regime

"The European Commission" (EC) "draws up and submits to the Council and Parliament any legislative proposals (for regulations or directives) needed to implement the treaties."[389] Additionally, "the Commission presents new European-wide legislation to the European Council and to the elected European Parliament, both of which are key EU legal institutions."[390] The EC "has approved Internet regulations such as the E-Commerce Directive, E-Signatures Directive, Distance Selling Directive, Data Protection Directive, Database Protection Directive, and the Copyright Directive."[391] The EC has powers of initiative, implementation, management, and control, which allows it to formulate harmonized regulations for the twenty-seven EU member states.

The DMCA relies solely upon private enforcement of takedown for infringing content, while the EU model is predicated upon public regulation supplemented by private enforcement. The advantage of the EU approach is that a consumer in any of the twenty-seven countries has recourse when a website posts injurious illegal content. The EC contends that e-Commerce will increase only if consumers are convinced that they have a minimal adequate remedy when entering cross-border sales and services.[392]

2. The e-Commerce Directive's Online Intermediary Rules

The EC enacted the e-Commerce Directive to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.[393] This EU Directive established rules such as the transparency and information requirements for online service providers, commercial communications, electronic contracts, and

---

[389] European Commission, *Fact Sheet on the European Union* (2021), https://www.europarl.europa.eu/factsheets/en/sheet/25/the-european-commission [https://perma.cc/VXJ2-KK4N].

[390] MICHAEL L. RUSTAD, 3 COMPUTER CONTRACTS § 14.02.

[391] Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law for Europe and America*, 5 J. HIGH TECH. L. 13, 24 (2005).

[392] *See generally Proposal for a Directive of the European Parliament and of the Council on Consumer Rights*, COM (2008) 614 final (Aug. 10, 2008) (outlining goals for consumer protection in cross-border e-commerce transactions).

[393] *Proposal for a Regulation of the European Parliament and of the Council, on a Single Market For Digital Services (Digital Services Act) and Amending Directive* 2000/31/EC, at 1–4, COM (2020) 825 final (Dec. 15, 2020), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN [https://perma.cc/WFV2-3HFU].

limitations of liability of intermediary service providers.[394] The Electronic Commerce Directive of 2000 gave EU consumers who were the victims of illegal content the right to order websites to remove it.[395]

The e-Commerce Directive's statutory purpose is "to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States."[396] The Directive creates a legal framework ensuring "the free movement of information . . . services."[397] The Directive also covers topics such as the liability of intermediary service providers, unsolicited commercial e-mail, and the prohibi-

---

[394] Articles 10 through 21 of the e-Commerce Directive set forth the liability limitations for intermediary service providers and applicable take-down and put-back regimes for illegal material distributed through their facilities. *Id*. European ISPs are immunized for caching, hosting, and perfunctory tasks related to efficient transmission of digital data. *Id*. The e-Commerce Directive does not impose liability on the ISP if it does not modify information transmitted by third parties, unless the ISP acquires actual or constructive notice of illegal content and fails to take prompt remedial steps. *Id*. Article 15(1) makes it clear that Member States may not impose a duty on providers to investigate questionable e-mails or website posters. *Id*. Article 15(2), however, permits Member States to enact legislation requiring providers to notify law enforcement when they discover illegal activities on their services. *Id*. One of the complexities of the e-Commerce Directive's constructive notice provision is its insufficient guidance as to what circumstances and requirements place ISPs on notice. Article 17 of the Brussels Regulations provides that a consumer cannot waive her right to sue a supplier in her local court. Commission Regulation 1215/2012 of Dec. 12, 2012, Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, art. 17, 2012 O.J. (L 351). A supplier, which includes U.S. software companies, directing their activities to the consumer's home state is automatically subject to jurisdiction because he has directed activities to that state as defined in Article 15. Commission Regulation 1215/2012 of Dec. 12, 2012, Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, art. 15, 2012 O.J. (L 351). Finally, a consumer may enforce a judgment in any Member State upon completion of the formalities set forth in Article 53. Commission Regulation 1215/2012 of Dec. 12, 2012, Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, art. 53, 2012 O.J. (L 351).

[395] The EU regulatory framework on content moderation is increasingly complex and has been differentiated over the years according to the category of the online platform and the type of content reflecting a risk-based approach. The e-Commerce Directive of 2000 contains the baseline regime applicable to all categories of platforms and all types of content. The Directive provides the following rules: (i) the 'country of origin' principle, which is the cornerstone of the Digital Single Market; (ii) an exemption of liability for hosting platforms which remain passive and neutral, and which remove the illegal content online as soon as they are made aware of it; (iii) the prohibition of general monitoring measures to protect fundamental rights; and (iv) the promotion of self- and co-regulation as well as alternative dispute resolution mechanisms. Alexandre De Streel et al., *European Parliament Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform* 15 (2020),
https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf [https://perma.cc/BJD5-HJNL].

[396] Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1, 8 (EC).

[397] *Id*.

tion of Internet-related surveillance.[398] The foremost difference between the EU's and the United States' approach is dissimilar assumptions about the role of government in regulating markets. Public regulation of the Internet is the predominant approach of Europe versus the United States' minimal regulation approach. The United States has no equivalent to the e-Commerce Directive for regulating digital services. Prior to the DSA, the EU notice-and-takedown duty was limited to service providers because social media companies, blogs, and chatrooms had not yet been created in 2000. The e-Commerce Directive has a narrow sphere of application:

> 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that
>
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
>
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information;
>
> 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider;
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.[399]

Article 14 of the e-Commerce Directive imposes a duty on Internet platforms, such as Facebook, to takedown illegal content once they acquire "actual knowledge of illegal activity or information."[400] An Internet platform is liable if they do not "expeditiously . . . remove or disable access to the information" if they have either actual knowledge or awareness of the illegality.[401] Article 14 also requires Internet websites to takedown illegal content if they are ordered to do so by courts or administrative authorities.[402]

The e-Commerce Directive did not require Internet platforms to monitor their services for illegal content. Article 15, entitled "no general obligation to monitor," provides:

> Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. Member States may establish obliga-

---

398 *Id*.

399 *Id*.

400 *Id*.

401 *Id*. art. 14(1)(a–b).

402 *Id*. art. 14(3).

> tions for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.[403]

The e-Commerce Directive does not hold services providers responsible for the content they host as long as (1) the acts in question are neutral intermediary acts of a mere technical, automatic, and passive capacity; (2) they are not informed of its illegal character, and (3) they act promptly to remove or disable access to the material when informed of it.[404] In addition, Article 15 prevents EU Member States from requiring service providers to monitor content for potentially illegal activities.[405] The EC summarized the online intermediary liability rules of the e-Commerce Directive as follows:

> The Directive exempts intermediaries from liability for the content they manage if they fulfil certain conditions. Service providers hosting illegal need to remove it or disable access to it as fast as possible once they are aware of the illegal nature of it. The liability exemption only covers services who play a neutral, merely technical and passive role towards the hosted content. Member States cannot force any general content monitoring obligation on intermediaries.[406]

The e-Commerce Directive's purpose was to advance a unified body of consumer protection, providing certainty for consumers and predictability for the business community.[407] European consumers in the single market must be provided with guaranteed minimal protection under national law.[408] The chief deficiency of the Directive's intermediary rules is that it consists of general principles without specific notice-and-takedown rules as opposed to the DMCA's detailed Internet intermediary rules for infringing content.

The European approach, in contrast, enacted a "one size fits all" notice-and-takedown procedure applicable to all illegal content. The e-Commerce Directive's online intermediary rules, modernized by the DSA's detailed procedures, will bring the Directive's notice-and-takedown rules up to date. This reform of the Directive's online liability standards addresses new threats posed by large gatekeepers such as Facebook, search engines such as Google, and video-sharing services such as YouTube:

> Since the adoption of Directive 2000/31/EC (the "e-Commerce Directive"), new and innovative information society (digital) services have emerged, changing the daily lives of Union citizens and shaping and transforming how they communicate, connect, consume and do business. Those services have contributed deeply

---

[403] *Id*. art. 15.

[404] *Id*. art. 14.

[405] *Id*. art. 15.

[406] European Comm'n, *e-Commerce Directive*, SHAPING EUROPE'S DIGITAL FUTURE, https://ec.europa.eu/digital-single-market/en/e-commerce-directive [https://perma.cc/C2N9-NUSE].

[407] *Id*. at 2.

[408] *Id*. at 1.

> to societal and economic transformations in the Union and across the world. At the same time, the use of those services has also become the source of new risks and challenges, both for society as a whole and individuals using such services. . . . The proposal defines clear responsibilities and accountability for providers of intermediary services, and in particular online platforms, such as social media and marketplaces. By setting out clear due-diligence obligations for certain intermediary services, including notice-and-action procedures for illegal content and the possibility to challenge the platforms' content moderation decisions, the proposal seeks to improve users' safety online across the entire Union and improve the protection of their fundamental rights.[409]

3. Overview of the EC's Digital Services Act & Digital Markets Act

The European Commission's "Digital Services Act and Digital Markets Act aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses."[410] The European Commission enacted these two legislative initiatives to upgrade rules governing digital services in the EU. "They form a single set of new rules applicable across the whole EU to create a safer and more open digital space."[411] The EC notes that these new rules have the following two objectives, (1) "to create a safer digital space in which the fundamental rights of all users of digital services are protected" and (2) "to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally."[412]

The Digital Service Act's updating of the e-Commerce Directive's online intermediary rules enacts "the swiftest and most effective enforcement of rules and protects all EU citizens."[413] The updated DSA extends to every Internet intermediary not just Internet Service Providers.[414] The European Commission

---

[409] Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1, 8 (EC).

[410] European Comm'n, *supra* note 406; *see also* European Comm'n, *The Digital Services Package*, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [https://perma.cc/A6JQ-USUC] (The DSA has been published in the Official Journal as of 27 October 2022 and came into force on 16 November 2022. The DSA will be directly applicable across the EU and will apply fifteen months or from 1 January 2024, whichever comes later, after entry into force.).

[411] *Id*.

[412] *Id*.

[413] Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1, 5 (EC).

[414] *Id*. at 2. The EU Commission describes the providers subject to the Digital Service Act as including: Intermediary services offering network infrastructure such as Internet access providers and domain-name registrars. The services also include

> [h]osting services such as cloud and webhosting services, including also [o]nline platforms bringing together sellers and consumers such as online marketplaces, app stores, collaborative economy platforms and social media platforms. Very large online platforms pose particular risks in the dissemination of illegal content and societal harms. Specific rules are foreseen for platforms reaching more than 10 [percent] of 450 million consumers in Europe.

European Comm'n, *supra* note 13.

proposed the Digital Services Act (DSA) in 2020, and it went into effect in late 2022, thus modernizing the e-Commerce Directive's online intermediary rules covering social media as well as other online platforms.[415] The EC makes it clear that the e-Commerce Directive will continue as the current EU legal framework for digital services even after the DSA goes into effect, because the DSA only displaces the e-Commerce Directive's online intermediary standards:

> This proposed Regulation is without prejudice to the e-Commerce Directive, and builds on the provisions laid down therein, notably on the internal market principle set out in Article 3. The proposed Regulation provides for a cooperation and coordination mechanism for the supervision of the obligations it imposes. With regard to the horizontal framework of the liability exemption for providers of intermediary services, this Regulation deletes Articles 12[–]15 in the e-Commerce Directive and reproduces them in the Regulation, maintaining the liability exemptions of such providers, as interpreted by the Court of Justice of the European Union.[416]

The EC defines "digital services" to "include a large category of online services, from simple websites to internet infrastructure services and online platforms."[417] The EC describes the two statutory provisions, the Digital Services Act and the Digital Markets Act as follows:

> The rules specified in the DSA primarily concern online intermediaries and platforms. For example, online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. The Digital Markets Act includes rules that govern gatekeeper online platforms. Gatekeeper platforms are digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services. Some of these services are also covered in the Digital Services Act, but for different reasons and with different types of provisions.[418]

Many EU countries have rejected French President Macron's proposal that the EU commit "to a tight timeline for an agreement on two key pieces of digital legislation."[419] The European Council "encourages the co-legislators to reach agreement on the Roaming Regulation by the end of the year, and invites them to continue work on the Digital Services Act and Digital Markets Act proposals with a view to reaching an ambitious agreement as soon as possible."[420]

---

[415] *See generally* Council Directive 2000/31, art. 1, 2000 O.J. (L 178) (EC) (updating the e-Commerce Directive and creating a legal framework for online service providers, commercial communications, electronic contracts, and limitations of liability of intermediary service providers).

[416] *Id*. at 5.

[417] European Comm'n, *supra* note 406.

[418] *Id*.

[419] Luca Bertuzzi, *EU Countries Reject Strict Deadline for DSA, DMA*, EURACTIV (Oct. 13, 2021), https://www.euractiv.com/section/digital/news/eu-countries-reject-strict-deadline-for-dsa-dma [https://perma.cc/N4UA-UKZY].

[420] *European Union: European Council Conclusions, 21-22 October 2021*, THAI NEWS SERVICE (Oct. 25, 2021) (available on Westlaw's News File).

4. Key Provisions of the Digital Markets Act (DMA)

"The Digital Markets Act aims to ensure that these platforms behave in a fair way online" by regulating large gatekeepers.[421] The DMA establishes the following objective criteria for determining what qualifies as a large online platform gatekeeper:

> [Company] has a strong economic position, significant impact on the internal market and is active in multiple EU countries
> [Company] has a strong intermediation position, meaning that it links a large user base to many businesses
> [Company] has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time.[422]

The Polish Deputy of Development and Technology describes the DMA's statutory purpose as ensuring "fair relations between the platform and companies using its services, and to guarantee openness and competition in the digital market. It may also contribute to the emergence of alternative platforms that can deliver high-quality innovative products and services at competitive conditions and at affordable prices."[423]

"As the EU debates its Digital Markets Act, calls have grown louder for manufacturers to remove all applications pre-installed on new phones to combat the oligopoly of 'gatekeepers' such as Google, Apple, Facebook, Amazon and Microsoft."[424] Tim Cook, Apple's Chief Executive Officer contends that "[t]he DMA could 'destroy the security of the iPhone and a lot of the privacy initiatives we've developed in the App Store.'"[425]

The EC proposed the DMA in 2020 to apply only to very large Internet gatekeepers.[426] The DMA develops specific rules so that these Internet giants

---

[421] European Comm'n, *supra* note 14; *see also* European Comm'n, *The Digital Markets Act: Ensuring Fair and Open Digital Mark*ets, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en [https://perma.cc/K84Q-QL7C] (stating "The Digital Markets Act (DMA) establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called 'gatekeeper.' This allows the DMA to remain well targeted to the problem that it aims to tackle as regards large, systemic online platforms.").

[422] *Id*.

[423] *Poland, EFNI with the Participation of the MRiT Management on the Condition of the Polish Economy: Digital and Green Transformation Ahead*, MENA REPORT, 2021 WLNR 34826848, (Oct. 24, 2021).

[424] Mathieu Pollet, *Manufactures Urged to Remove Pre-installed Apps on New Phones*, EURACTIV (English) (May. 26, 2021), https://www.euractiv.com/section/digital/news/manufacturers-urged-to-remove-pre-installed-apps-on-new-phones [https://perma.cc/P9FY-GAU9].

[425] Mathieu Pollet, *Apple Continues Pushback on Sideloading and Third-Party App Stores*, EURACTIV (English) (Oct. 13, 2021), https://www.euractiv.com/section/cybersecurity/news/apple-continues-pushback-on-sideloading-and-third-party-app-stores [https://perma.cc/TJN4-8N9Q].

[426] Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1, 2 (EC).

"behave in a fair way online. Together with the Digital Services Act, the Digital Markets Act is one of the centrepieces [sic] of the European digital strategy."[427] DMA's sphere of application is to very large gatekeepers that the Commission determines by the following criteria:

> The DMA establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called "gatekeeper." This allows the DMA to remain well targeted to the problem that it aims to tackle as regards large, systemic online platforms.
> These criteria will be met if a company:
> has a strong economic position, significant impact on the internal market and is active in multiple EU countries
> has a strong intermediation position, meaning that it links a large user base to a large number of businesses
> has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time.[428]

The EC describes the growth of immense gatekeepers since the inception of the Internet:

> Large platforms have emerged benefitting from characteristics of the sector such as strong network effects, often embedded in their own platform ecosystems, and these platforms represent key structuring elements of today's digital economy, intermediating the majority of transactions between end users and business users. Many of these undertakings are also comprehensively tracking and profiling end users. A few large platforms increasingly act as gateways or gatekeepers between business users and end users and enjoy an entrenched and durable position, often as a result of the creation of conglomerate ecosystems around their core platform services, which reinforces existing entry barriers.
> As such, these gatekeepers have a major impact on, have substantial control over the access to, and are entrenched in digital markets, leading to significant dependencies of many business users on these gatekeepers, which leads, in certain cases, to unfair behaviour [sic] vis-à-vis these business users. It also leads to negative effects on the contestability of the core platform services concerned.[429]

For the first time, the European Union has given content creators and plaintiffs procedural guarantees described by the Commission as:

> [T]he right to be heard and of access to the file (Article 30) and the protection of professional secrecy (Article 31). It also provides for the consultation of the Digital Markets Advisory Committee set up by this Regulation before adopting identified individual decisions addressed to gatekeepers (Article 32). Finally, the Regulation provides for a possibility for three or more Member States to request the Commission to open a market investigation pursuant to Article 15 (Article 33).[430]

---

427 European Commission, *supra* note 14.

428 *Id*.

429 Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1, 2 (EC).

430 *Id*. at 7.

The DMA's system of fines reflects deterrence principles that are the functional equivalent of punitive damages. The Commission notes that the fines can be as high as "10 [percent] of the company's total worldwide annual turnover."[431] In addition, periodic penalty payments of up to "5 [percent] of the average daily turnover" may be imposed on gatekeepers.[432]

> In case of systematic infringements of the DMA obligations by gatekeepers, additional remedies may be imposed on the gatekeepers after a market investigation. Such remedies will need to be proportionate to the offence committed. If necessary and as a last resort option, non-financial remedies can be imposed. These can include behavioural and structural remedies, e.g. the divestiture of (parts of) a business.[433]

The DMA system of graduating penalties is designed to achieve specific and general deterrence in order to spur gatekeepers to expeditiously remove illegal content.

5. The Digital Services Act's Regulation on Online Intermediaries

The Digital Services Act (DSA) provides detailed rules governing Internet intermediaries and is therefore more central to liability issues than the DMA. The EU Parliament proposed the updated DSA as a regulation rather than a directive, so, after approval, it will go into effect automatically and uniformly to all EU countries without national legislation.[434]

Until the DSA goes into effect, the e-Commerce Directive's general standards for intermediaries will remain in effect. After the DSA goes into effect, the DSA will replace the Directive's intermediary rules, but the other provisions of the e-Commerce Directive will remain in effect. The DSA provides comprehensive notice-and-takedown rules, while the other provisions of the e-Commerce Directive remain in effect. The EU Monitor explains the updating of the Directive as follows:

> Building on the key principles set out in the e-Commerce Directive, which remain valid today, this proposal seeks to ensure the best conditions for the provision of innovative digital services in the internal market, to contribute to online safety and the protection of fundamental rights, and to set a robust and durable governance structure for the effective supervision of providers of intermediary services. The proposal defines clear responsibilities and accountability for providers of intermediary services, and in particular online platforms, such as social media and marketplaces. By setting out clear due-diligence obligations for certain intermediary services, including notice-and-action procedures for illegal content and the possibility to challenge the platforms' content moderation decisions, the proposal seeks to improve users' safety online across the entire Union

---

[431] European Commission, *supra* note 14.

[432] *Id*.

[433] *Id*.

[434] Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1, 3 (EC).

> and improve the protection of their fundamental rights. Furthermore, an obligation for certain online platforms to receive, store and partially verify and publish information on traders using their services will ensure a safer and more transparent online environment for consumers. Recognising the particular impact of very large online platforms on our economy and society, the proposal sets a higher standard of transparency and accountability on how the providers of such platforms moderate content, on advertising and on algorithmic processes. It sets obligations to assess the risks their systems pose to develop appropriate risk management.[435]

"It is not yet known how this regulation will be implemented. It is conceivable, however, that platform operators will use an upload filter system to prevent the repeated uploading of already deleted posts. 'Notice-and-action' would therefore not amount to a general, but nevertheless a limited monitoring obligation."[436]

The DSA will give EU-wide fundamental rights, protecting all citizens from illegal content.[437] "Regulations are automatically applicable to all EU Member States. Conventions are the equivalent of treaties. When a new Member State joins the European Union, regulations apply automatically, unlike the case with Conventions."[438] The EU Commission argues that DSA will:

> Better protect consumers and their fundamental rights online
> Establish a powerful transparency and a clear accountability framework for online platforms
> Foster innovation, growth, and competitiveness within the single market
> For citizens
> More choice, lower prices
> Less exposure to illegal content
> Better protection of fundamental rights
> For providers of digital services
> Legal certainty, harmonisation of rules
> Easier to start-up and scale-up in Europe
> For business users of digital services
> More choice, lower prices
> Access to EU-wide markets through platforms
> Level-playing field against providers of illegal content
> For society at large
> Greater democratic control and oversight over systemic platforms

---

[435] *Id*. at 4.

[436] Nico Brunotte, *Update 2.0 to the Digital Services Act - Farewell to the "Notice-and-Takedown" Procedure?*, DLA PIPER (June 18, 2020), https://mse.dlapiper.com/post/102g9pn/update-2-0-to-the-digital-services-act-farewell-to-the-notice-and-takedown-pr [https://perma.cc/Q4WX-BL5U].

[437] European Commission, *supra* note 13 ("The European Parliament and Member States will discuss the Commission's proposal according to the ordinary legislative procedure. Once adopted, the new rules will be directly applicable across the EU.").

[438] Michael L. Rustad & Thomas H. Koenig, *Wolves of the World Wide Web: Reforming Social Networks' Contacting Practices*, 49 WAKE FOREST L. REV. 1431, 1502 n.319 (2014).

> Mitigation of systemic risks, such as manipulation or disinformation[439]

"In the view of the European Commission, there should still be no general monitoring obligation, i.e.[,] platforms would not have to proactively check their services for illegal postings as long as they do not receive a corresponding user notification."[440] Private enforcement initiated by tort victims places less of an administrative burden on gatekeepers or platforms, who do not have a duty to police their services for illegal content under the DSA.

6. What Internet Intermediaries Are Covered by the Digital Markets Act

The European Commission has also proposed the Digital Markets Act (DMA), which "will be applicable only to large companies that will be identified as 'gatekeepers' according to objective criteria."[441] Gatekeepers such as Google, Amazon, and Facebook are subjected to more stringent rules than smaller online service providers are because these entities "enjoy, or will foreseeably enjoy, an entrenched and durable position. This can grant them the power to act as private rule-makers and to function as bottlenecks between businesses and consumers."[442] Gatekeeping "companies control at least one so-called 'core platform service' (such as search engines, social networking services, certain messaging services, operating systems and online intermediation services), and have a lasting, large user base in multiple countries in the EU."[443] A platform will be considered a gatekeeper if it meets a series of criteria.

> Specifically, there are three main cumulative criteria that bring a company under the scope of the Digital Markets Act:
> 1. A size that impacts the internal market: this is presumed to be the case if the company achieves an annual turnover in the European Economic Area (EEA) equal to or above € 6.5 billion in the last three financial years, or where its average market capitalisation or equivalent fair market value amounted to at least € 65 billion in the last financial year, and it provides a core platform service in at least three Member States;
> 2. The control of an important gateway for business users towards final consumers: this is presumed to be the case if the company operates a core platform service with more than 45 million monthly active end users established or located in the EU and more than [ten thousand] yearly active business users established in the EU in the last financial year;
> 3. An (expected) entrenched and durable position: this is presumed to be the case if the company met the other two criteria in each of the last three financial years.
> If all these quantitative thresholds are met, the specific company is presumed to be a gatekeeper, unless it submits substantiated arguments to demonstrate the

---

439 *See* European Commission, *supra* note 13.
440 Brunotte, *supra* note 436.
441 European Commission, *supra* note 14.
442 *Id*.
443 *Id*.

> contrary. If not all these thresholds are met, the Commission may evaluate, in the context of a market investigation for designating gatekeepers, the specific situation of a given company and decide to identify it as a gatekeeper on the basis of a qualitative assessment.[444]

The DSA requires all Internet intermediaries to comply with its general obligations, while DMA is only applicable to very large online entities that include:

> Intermediary services offering network infrastructure: Internet access providers, domain name registrars, including also:
> Hosting services such as cloud and webhosting services, including also:
> Online platforms bringing together sellers and consumers such as online marketplaces, app stores, collaborative economy platforms and social media platforms.
> Very large online platforms pose particular risks in the dissemination of illegal content and societal harms. Specific rules are foreseen for platforms reaching more than 10 [percent] of 450 million consumers in Europe.[445]

Online intermediaries offering services to EU countries will be required to "comply with the new rules. Micro and small companies will have obligations proportionate to their ability and size while ensuring they remain accountable."[446] Unlike the "one size fits all" obligation of the current e-Commerce Directive, the DSA imposes greater obligations on Amazon, Facebook, Google, Twitter, and the other large entities.[447]

7. Impact of the DSA on Internet Intermediaries' Legal Obligations

The EU Commission explains that the 2020 DSA "significantly improves the mechanisms for the removal of illegal content and for the effective protection of users' fundamental rights online, including the freedom of speech. [The DSA] also creates a stronger public oversight of online platforms, in particular for platforms that reach more than 10 [percent] of the EU's population."[448] The Commission states that the specific impacts include:

> measures to counter illegal goods, services, or content online, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers"
> new obligations on traceability of business users in online marketplaces, to help identify sellers of illegal goods.
> effective safeguards for users, including the possibility to challenge platforms' content moderation decisions
> transparency measures for online platforms on a variety of issues, including on the algorithms used for recommendations

---

444 *Id*.
445 European Commission, *supra* note 13.
446 *Id*.
447 *Id*.
448 *Id*.

> obligations for very large platforms to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems
> access for researchers to key data of the largest platforms, in order to understand how online risks evolve
> oversight structure to address the complexity of the online space: EU countries will have the primary role, supported by a new European Board for Digital Services; for very large platforms, enhanced supervision, and enforcement by the Commission.[449]

8. The DSA's Sphere of Application

The European Commission describes the DSA's sphere of Application as follows:

> Chapter 1 [of the DSA] sets out general provisions, including the subject matter and scope of the Regulation (Article 1) and the definitions of key terms used in the Regulation (Article 2).
> Chapter II contains provisions on the exemption of liability of providers of intermediary services. More specifically, it includes the conditions under which providers of mere conduit (Article 3), caching (Article 4) and hosting services (Article 5) are exempt from liability for the third-party information they transmit and store. It also provides that the liability exemptions should not be disapplied when providers of intermediary services carry out voluntary own-initiative investigations or comply with the law (Article 6) and it lays down a prohibition of general monitoring or active fact-finding obligations for those providers (Article 7). Finally, it imposes an obligation on providers of intermediary services in respect of orders from national judicial or administrative authorities to act against illegal content (Article 8) and to provide information (Article 9).
> Chapter III sets out the due diligence obligations for a transparent and safe online environment, in five different sections.
> Section 1 lays down obligations applicable to all providers of intermediary services, in particular: the obligation to establish a single point of contact to facilitate direct communication with Member States' authorities, the Commission and the Board (Article 10); the obligation to designate a legal representative in the Union for providers not established in any Member State, but offering their services in the Union (Article 11); the obligation to set out in their terms and conditions any restrictions that they may impose on the use of their services and to act responsibly in applying and enforcing those restrictions (Article 12); and transparency reporting obligations in relation to the removal and the disabling of information considered to be illegal content or contrary to the providers' terms and conditions (Article 13).[450]

The DSA unifies and strengthens Internet intermediary standards as the EU Commission states below:

> The proposal maintains the liability rules for providers of intermediary services set out in the e-Commerce Directive—by now established as a foundation of the

---

[449] *Id.*

[450] Council Directive 2000/31, art. 1, 2000 O.J. (L 178) 1-4 (EC).

> digital economy and instrumental to the protection of fundamental rights online. Those rules have been interpreted by the Court of Justice of the European Union, thus providing valuable clarifications and guidance. Nevertheless, to ensure an effective harmonisation across the Union and avoid legal fragmentation, it is necessary to include those rules in a Regulation. It is also appropriate to clarify some aspects of those rules to eliminate existing disincentives towards voluntary own-investigations undertaken by providers of intermediary services to ensure their users' safety and to clarify their role from the perspective of consumers in certain circumstances. Those clarifications should help smaller, innovative providers scale up and grow by benefitting from greater legal certainty.
>
> A deeper, borderless single market for digital services requires enhanced cooperation among Member States to guarantee effective oversight and enforcement of the new rules set out in the proposed Regulation. The proposal sets clear responsibilities for the Member State supervising the compliance of service providers established in its territory with the obligations set by the proposed Regulation. This ensures the swiftest and most effective enforcement of rules and protects all EU citizens.[451]

Gatekeeper entities having an "establishment in the Union" or targeting a "significant number of users in one or more Member States" must comply with the DSA, no matter where they are headquartered.[452] The DSA's broad sphere of application makes it clear that non-EU companies must comply, in contrast to the Directive, which did not address that issue.[453] U.S. companies have lobbied vigorously against the DSA's intermediary rules, creating tensions with EU legislators. "U.S. officials used the first U.S.-EU Trade and Technology Council meeting in Pittsburgh in September [2021] to raise concerns with proposed EU digital market legislation, including the Digital Services Act. EU officials have said they don't plan to allow the U.S. to weigh in on EU regulatory rulemaking."[454]

The current U.S. approach to online intermediary liability relies upon a market-based approach as opposed to the EU's DSA, which is a thick regulatory measure. At present, the United States has no mechanism to takedown illegal content, only infringing content under the DMCA. Our proposed reform would create a broad takedown duty for content constituting ongoing torts or crimes. We propose a notice-and-takedown procedure that draws upon the notice, takedown, and putback provisions of Section 512 of the DMCA and of the DSA. Our proposal harmonizes U.S. takedown law for infringing and illegal content by adopting the safe harbor provisions of the DMCA. Our proposal

---

[451] *Id*.

[452] These entities direct activities to EU Member States and are thus subject to the DSA. *Id*. ("to offer services in the Union").

[453] *See* Council Directive 2000/31, art. 14, at 13.

[454] *G7 Trade Ministers Tout Digital Trade Principles, Forced Labor Accord*, INSIDE U.S. TRADE'S WORLD TRADE ONLINE (Oct. 22, 2021, 3:37 PM), https://insidetrade.com/daily-news/g7-trade-ministers-tout-digital-trade-principles-forced-labor-accord [https://perma.cc/EEV4-SXQG].

adapts the Internet intermediary rules in the DSA, creating new duties for giant gatekeepers such as Amazon, Facebook, Google, and Twitter.

Our proposal imports the DSA's definition of online platforms as opposed to the narrow definition of Internet Service Providers:

> Online platforms, such as social networks or online marketplaces, should be defined as providers of hosting services that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public, again at their request. However, in order to avoid imposing overly broad obligations, providers of hosting services should not be considered as online platforms where the dissemination to the public is merely a minor and purely ancillary feature of another service and that feature cannot, for objective technical reasons, be used without that other, principal service, and the integration of that feature is not a means to circumvent the applicability of the rules of this Regulation applicable to online platforms.[455]

The DSA definition of platforms includes search engines like Google, live streaming platforms such as YouTube, and giant gatekeeping social networks such as Facebook and Twitter. These large gatekeepers are cross-border institutions, often beyond local law enforcement. Our proposal recognizes the need to make providers of intermediary services liable where they undertake illegal activities such as hosting ongoing torts or crimes.

IV. OUR PROPOSAL TO ADOPT NOTICE & TAKEDOWN FOR ONGOING ONLINE TORTS

A. Who Must Respond to Takedown Notices?

Our CDA Section 230 reform proposal adapts the EC's logic as illustrated in the DMA, which will be applicable only to large companies that will be identified as "gatekeepers" according to objective criteria.[456] Our CDA Section 230 NTD procedures will also only apply to very large Internet gatekeepers. The CDA Section 230 reform will determine who is a gatekeeper by examining quantitative criteria such as their revenue and number of U.S. users, but also apply a case-by-case assessment that parallel the NTD procedures proposed by the DMA.

The CDA Section 230 reform will determine who is a gatekeeper by examining quantitative criteria such as their revenue and number of U.S. users, but also by a case-by-case assessment. As new social media evolve, the qualitative and quantitative measures for determining which entities or platforms will be subject to NTD.

---

[455] *Proposal for a Regulation of the European Parliament and the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive*, COM (2020) 825 final (Dec. 12, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&rid=2 [https://perma.cc/856A-4DWK].

[456] European Commission, *supra* note 14.

B. Who Gives Notice of Infringing, Tortious, or Other Illegal Content?

At present, Section 230 preempts all tort claims so websites have no legal incentive to act with respect to deplorable conduct on their services, even if they have notice of actual or potential harm posed by this content.[457] No other country in the world has a "no duty" provision like CDA Section 230 that shields very large platforms from hosting false information about COVID-19 vaccines, terrorism, revenge pornography, and malicious fake dating profiles. The CDA Section 230 proposal adapts a synthesis of the most efficient provisions of the DMCA's and the DSA's notice-and-takedown provisions. Both the DMCA and the DSA depend largely upon private enforcement for their NTD procedures. Copyright owners, whose content is posted on a service, initiate the DMCA's NTD.[458] The U.S. Copyright Office explains the private enforcement model of NTD for the DMCA as follows:

> In 1998, Congress passed the Digital Millennium Copyright Act (DMCA), which amended U.S. copyright law to address important parts of the relationship between copyright and the internet. The three main updates were: (1) establishing protections for online service providers in certain situations if their users engage in copyright infringement, including by creating the notice-and-takedown system, which allows copyright owners to inform online service providers about infringing material so it can be taken down; (2) encouraging copyright owners to give greater access to their works in digital formats by providing them with legal protections against unauthorized access to their works (for example, hacking passwords or circumventing encryption); and (3) making it unlawful to provide false copyright management information (for example, names of authors and copyright owners, titles of works) or to remove or alter that type of information in certain circumstances.[459]

The CDA Section 230 reform extends DMCA-style NTD from infringing content to ongoing torts. This will create necessary incentives to encourage websites to remove ongoing torts upon receiving written or digital notice as to why the content is considered tortious. The policy underlying tort NTD shares much common ground with the DMCA's reliance on the victims of illegal con-

---

[457] U.S. DEP'T OF JUST., SECTION 230—NURTURING INNOVATION OR FOSTERING UNACCOUNTABILITY? KEY TAKEAWAYS AND RECOMMENDATIONS (2020). Courts have extended CDA Section 230 immunity provision to a remarkable array of scenarios. They include instances where a provider republished content knowing it violated the law; solicited illegal content while ensuring that those responsible could not be identified; altered its user interface to ensure that criminals were not caught; and sold dangerous products. *Id*. In this way, Section 230 has evolved into a super-immunity that, among other things, prevents the best-positioned entities from responding to the most harmful content. This would have seemed absurd to the CDA's drafters. The law's overbroad interpretation means that platforms have no liability-based reason to take down illicit material and that victims have no legal leverage to insist otherwise.

[458] *See generally* 17 U.S.C. § 512 (2019).

[459] *The Digital Millennium Copyright Act*, U.S. COPYRIGHT OFF., https://www.copyright.gov/dmca [https://perma.cc/32W6-VBFA].

tent initiating takedown of illegal content. The CDA Section 230 NTD model places the burden of discovering ongoing torts on the victims of this illegal content, not the gatekeeper or the federal government. Our NTD regime is based upon private enforcement as opposed to thick government regulation, which is consistent with the DMCA and the e-Commerce Directive. In addition, very large gatekeepers must comply with court orders or federal regulatory action to remove ongoing cybertorts posted on the Internet, which is drawn from the DMA.

C. No Duty to Monitor for Ongoing Torts

Our NTD proposal adopts a safe harbor provision protecting Internet platforms from being required to monitor their sites, which is modeled on DMCA Section 512[460] and Article 15 of the e-Commerce Directive,[461] which remains in effect, as it is not superseded by the DSA of 2020.[462] The DMCA places the burden of notifying such service providers of infringements upon the copyright owner or his agent. Section 512 of the DMCA "requires such notifications of claimed infringements to be in writing and with specified contents and directs that deficient notifications shall not be considered in determining whether a service provider has actual or constructive knowledge."[463] Monitoring poses a significant censorship risk if providers respond to the duty to remove ongoing torts by eradicating any questionable material. Our NTD proposal requires notifications of claimed ongoing torts to be in writing, with specifics as to why the posted content violates their rights.

D. What Constitutes Sufficient Notice?

The website or other Internet intermediary must receive written or digital notice from the direct victim of the ongoing tort. CDA Section 230 does not adopt the "red flags" test requiring the large gatekeeper to disable content when there is apparently a tort. Our NTD is aligned with the DMCA's notice requirements. The DMCA safe harbor at issue "requires [either] actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement." [464] The DMCA includes safe-harbor

---

[460] 17 U.S.C. § 512 (2019).

[461] Council Directive 2000/31/EC, art. 15, 2000 O.J. (L 178) 13.

[462] *The Digital Services Act Package*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [https://perma.cc/4E5L-PD8X]; *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*, COM (2020) 825 final (Dec. 15, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&rid=2 [https://perma.cc/2U4E-HWXW].

[463] Viacom Int'l., Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 115 (S.D.N.Y. 2013).

[464] *Id*. at 118 (internal quotation marks omitted).

provisions "that provide protections to internet service providers under certain conditions."[465]

> First, there are three threshold requirements: [T]he party (1) must be a service provider as defined by the statute; (2) must have adopted and reasonably implemented a policy for the termination in appropriate circumstances of users who are repeat infringers; and (3) must not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works.[466]

E. Content of the Takedown Notice

Our proposed CDA NTD procedures require the complainant to specify in writing the reasons why the content is an ongoing tort and to provide the website with contact information. The CDA reform proposal imports the DSA requirement that the plaintiff demonstrates specific and identifiable ongoing torts as a predicate for a gatekeeper removing content. In addition, the cybertort complainant must have specific reasons why content constitutes an ongoing cybertort, which also parallels Section 512 of the DMCA's procedure.[467] Under our proposal, cybertort complaints must also attest a good faith belief that the content is tortious, closely paralleling the DMCA requirements in Section 512. Under our proposed NTD procedures for disabling content constituting ongoing torts or crimes, the complainant must identify the location of the content constituting illegal content with specificity.

G. What Objectionable Content Is Subject to Notice-and-Takedown?

CDA Section 230 notice-and-takedown (NTD)procedures are sector-specific, like the DMCA, versus the e-Commerce Directive, DSA, and DMA that have a broader sphere of application, which encompasses all illegal content. The CDA NTD procedures apply to tortious or criminal content, such as false COVID-19 cures, the incitement of terrorism postings, child pornography, defamation, and other intentional ongoing cybertorts or cybercrimes described in Part II of this Article.

H. Safe Harbor for Internet Platforms

Our CDA Section 230 NTD for ongoing torts adopts a DMCA-style safe harbor for Internet platforms. The DMCA, but not the Directive, requires websites to appoint an agent responding to takedown requests and to designate it conspicuously on its websites.[468] Section 512 of the DMCA "places the burden

---

[465] Myeress v. Buzzfeed, Inc., No. 18-CV-2365 (VSB), 2019 WL 1004184, at *2 (S.D.N.Y. Mar. 1, 2019) (internal quotation marks omitted).

[466] *Id*. (internal quotation marks omitted).

[467] *Id*. at *2–3 (internal quotation marks omitted).

[468] 17 U.S.C. § 512 (2019).

of notifying such service providers of infringements upon the copyright owner or his agent."[469] Notifications of claimed infringements must be in writing with specified contents.[470] An Internet gatekeeper need not respond to deficient notices.[471] Our CDA Section 230 NTD reform adopts a parallel provision to DMCA Section 512, requiring that a tort victim must show knowledge, actual versus apparent or red flag knowledge that content constitutes an ongoing tort.[472] The safe harbor provisions appropriately balance the rights of websites against cybertort victims by guarding against frivolous, excessive, or malicious takedown notices.

I. Why Our CDA Takedown Does Not Silence Speech Torts with Matters of Public Concern

"[T]he First Amendment to the United States Constitution provides special protection to speech on matters of public concern, even if that speech is revolting and upsetting."[473] In rare cases, the First Amendment applies to speech torts such as defamation. In *Higgins v. Ky. Sports Radio, LLC*,[474] the court dismissed tort actions filed by John Higgins, a basketball referee who officiated in the 2017 NCAA Elite Eight Tournament game.[475] Higgins was a well-known NCAA college basketball official who was part of a "three-person officiating crew for the 2017 Elite Eight game between Kentucky and North Carolina."[476] Kentucky fans heatedly blamed their team's loss on his poor officiating, in some cases threatening the referee's life.[477]

ESPN described how Higgins "met with law enforcement for more than two hours Tuesday after Kentucky fans sent death threats, repeatedly called his company's office and home—despite an unlisted number—and posted a barrage of false messages about his business on the company's Facebook page . . . ."[478] John Higgins filed a tort lawsuit against Kentucky Sports Radio and two announcers who relentlessly discussed the officiating in the Elite Eight game, including publicizing their perception that Mr. Higgins was at least partially responsible for Kentucky's loss. "Additionally, the Defendants discussed

---

469 Viacom Int'l., Inc., 940 F. Supp. at 114–15.

470 *Id*. at 115.

471 *Id*.

472 Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 610 (9th Cir. 2018).

473 Higgins v. Ky. Sports Radio, LLC, No. 5:18-cv-043-JMH, 2019 U.S. Dist. LEXIS 45535, at *3 (E.D. Ky. Mar. 20, 2019).

474 *Id*.

475 *Id*. at *1–2.

476 *Id*.

477 Jeff Goodman & Dana O'Neil, *NCAA Referee John Higgins Receiving Death Threats from Kentucky Fans*, ESPN (Mar. 29, 2017), https://www.espn.com/mens-college-basketball/story/_/id/19029689/ncaa-official-john-higgins-receiving-death-threats-kentucky-wildcats-fans-following-loss-north-carolina-tar-heels [https://perma.cc/GW24-FNTW].

478 *Id*.

the Higgins' business and read and posted reviews and comments from angry fans on various media platforms."[479] Higgins contended that the Sports radio fans "indirectly recruited an army of willing and upset fans to attack [him], in retribution for Mr. Higgins's role in officiating the Elite Eight contest."[480] The federal court dismissed Higgin's lawsuit with prejudice, reasoning that:

> [W]hile Plaintiffs' frustration is understandable and their damages are real, in some instances the First Amendment to the United States Constitution provides special protection to speech on matters of public concern, even if that speech is revolting and upsetting. In this instance, after reviewing the entire record and considering the content, form, and context of the allegedly tortious speech, the Court has reached the conclusion that Defendants' speech, broadcast in various forms on radio, television, and the internet, involved matters of public concern. Thus, the speech enjoys special protection and the First Amendment prevents the Plaintiffs from using tort actions to silence and punish the Defendants for engaging in protected speech.[481]

Our CDA Section 230 takedown only applies to speech that does not concern matters of public concern and, therefore, does not conflict with the First Amendment. As the Kentucky court explains, it is improper to use "tort actions to silence and punish" defendants "for engaging in protected speech."[482] Under our proposed reform to CDA Section 230, content creators can order the put back of materials that websites and other platforms remove when the First Amendment protects the content.

J. Remedies for Frivolous Takedown Requests

A content creator may claim compensatory and sometimes punitive damages where deterrence is required because of repeated NTD frivolous demands. Compensatory damages consist of both the actual damages that were a direct result of the frivolous demand (but may not include noneconomic damages such as pain and suffering), and special damages where the content creator proves harm from the frivolous demand. Table One (below) compares and contrasts our proposed CDA Section 230 NTD for ongoing torts compared to the EU's proposed NTD rules for all illegal content and the DMCA, which is the U.S. enactment of the global standard for taking down infringing content. The CDA Section 230 reform is a grand synthesis of the best features of the DSA and DMA and Section 512 of the DMCA.

---

[479] *Higgins*, 2019 U.S. Dist. LEXIS 45535, at *3.
[480] *Id*.
[481] *Id*. at *3–4.
[482] *Id*.

TABLE 1: COMPARING CDA SECTION 230 NTD TO THE DMCA & E-COMMERCE DIRECTIVE[483]

NTD Regimes	Proposed CDA Section 230 NTD for Ongoing Torts	Digital Service Act's (DSA) Rules for Takedown and Removal of all Illegal Content	Digital Millennium Copyright Act's Sector Specific Rules for Taking Down Infringing Content
Who Must Respond to Takedown Notices?	The CDA Section 230 notice-and-takedown (NTD) is restricted to very large gatekeepers defined as those providers that target 50 million U.S. users or more. The CDA NTD also requires a showing	Europe's new rules recognize that the problem with NTD lies with the very largest gatekeepers. Europe requires all Internet websites to have a complaint mechanism but imposes a higher duty on the largest gatekeepers. The EU's Digital Markets Act (DMA)	All online content providers (websites, chatrooms, blogs, etc.) must expeditiously remove infringing copyright content upon notice. "Congress enacted section 512 of the Copyright Act, which (1) enabled copyright owners to have infringing online content removed without the need for litigation, and (2) facilitated

[483] The sources and notes that follow pertain to the information in this Table. European Commission, *supra* note 14; *see List of Largest Internet Companies*, WIKIPEDIA, (last edited Dec. 15, 2021, 9:10 PM), https://en.wikipedia.org/wiki/List_of_largest_Internet_companies [https://perma.cc/46C3-YBPV] (noting Alphabet, Amazon, and Facebook had $85 billion in revenue or greater); *see also Just How Massive Is Google, Anyway*?, COMPUTER SCH., http://www.computerschool.org/computers/google [https://perma.cc/4BBL-L7LV] (noting annual income of $8.3 billion). Most top ranked social networks with more than 100 million users originated in the United States, but services like Chinese social networks WeChat, QQ, or video sharing app Douyin have also garnered mainstream appeal in their respective regions due to local context and content. Douyin's popularity has led to the platform releasing an international version of its network: a little app called TikTok. Statista Research Dep't., *Global Social Networks Ranked by Number of Users 2021*, STATISTA (Nov. 16, 2021), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users [https://perma.cc/887R-FPTM] (Our proposal only applies if social networks, search engines or other platforms target 100 million or more users in the U.S. Thus, Chinese, Japanese and other foreign sites will not be subject to the CDA Section 230 where they do not target at least 100 million U.S. users); European Commission, *supra* note 14 (Gatekeepers have changed over time as evidenced by the rise of Google, Facebook, and Amazon. The EU anticipated updating the definition and obligation of gatekeepers to "keep up with the fast pace of digital markets, the Commission will carry out market investigations."); *The Digital Millennium Copyright Act*, U.S. COPYRIGHT OFFICE, https://www.copyright.gov/dmca [https://perma.cc/RY4L-RADF]; *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*, COM (2020) 825 final (Dec. 15, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&rid=2 [https://perma.cc/ZV7W-NV73]; *see* 17 U.S.C. § 512 (2019); Council Directive 2000/31/EC, art. 15, 2000 O.J. (L 178) 13–15, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN [https://perma.cc/NRM3-D82H]; Myeress v. BuzzFeed Inc., No. 18-CV-2365 (VSB), 2019 WL 1004184, at *2–3 (internal quotations marks omitted); UMG Recordings, Inc. v. Shelter Cap. Partners LLC, 718 F.3d 1006, 1021 (9th Cir. 2013).

	that the platform has a minimum annual revenue of 65 million euros. We adapt the definition of very large gatekeepers in EU's Digital Markets Act (DMA). As currently conceived, CDA NTD only targets immense entities like Alphabet, Amazon, Facebook, and Google. As with the EU's Digital Services Act, small and medium companies need a complaint mechanism, but do not have the detailed, expensive obligations of the very large gatekeepers. Congress will update the definition of very large gatekeepers, with procedures paralleling those of the DMA.	NTD procedures only apply to companies like Google, Facebook, Amazon, and Twitter. The DMA establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called "gatekeeper." This allows the DMA to remain well targeted to the problem that it aims to tackle as regards large, systemic online platforms. "These criteria will be met if a company: has a strong economic position, significant impact on the internal market and is active in multiple EU countries; has a strong intermediation position, meaning that it links a large user base to a large number of businesses; [and] has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time."	the development of the internet industry by providing legal certainty for participating online service providers. Section 512 shields online service providers from monetary liability and limits other forms of liability for copyright infringement—referred to as safe harbors—in exchange for cooperating with copyright owners to expeditiously remove infringing content if the online service providers meet certain conditions."
Who Gives Notice of Infringing, Tortious, or Other Illegal Content?	The direct victim of a posting that constitute an ongoing cybertort, much like the role of the copyright owner in the DMCA initiate NTD. In addition, Internet platforms such as websites must also comply with court orders or regulatory action to remove ongoing	Section 2 of the DSA "lays down obligations, additional to those under Section 1, applicable to providers of hosting services. In particular, that section obliges those providers to put in place mechanisms to allow third parties to notify the presence of alleged illegal content (Article 14). Furthermore, if such a provider decides to remove or disable access to specific information pro-	Copyright owners are the persons or entities giving online service providers notice of infringing content to initiate takedown.

	cybertorts posted on the Internet.	vided by a recipient of the service it imposes the obligation to provide that recipient with [a] statement of reasons" (Article 15)." "Some large online platforms act as 'gatekeepers' in digital markets. The Digital Markets Act aims to ensure that these platforms behave in a fair way online. Together with the Digital Services Act, the Digital Markets Act is one of the centrepieces of the European digital strategy."	
Do very large gatekeepers and other Internet intermediaries have a duty to monitor for illegal activity?	The CDA Section 230 imposes no duty on gatekeepers or any Internet intermediary to monitor for ongoing torts.	Article 15 of the e-Commerce Directive explicitly states that Internet hosts have no duty to monitor. Article 15 of the Directive remains in effect as it is not superseded the Digital Services Act of 2020.	DMCA Section 512 does not impose a duty on service providers to monitor for infringing content.
What Constitutes a Sufficient Notice Requiring Websites and Other Providers to Disable or Takedown Objectionable Content?	The website or other Internet intermediary must receive written or digital notice from the direct victim of the ongoing tort to have a duty to act. The CDA Section 230 does not adopt "red flags" test requiring the large gatekeeper to disable content when there is apparently a tort. Our notice provision is aligned with the DMCA's written notice require-	The DSA requires the complainant to provide service provider with a statement of reasons why content is illegal.	The DMCA safe harbor at issue requires either actual knowledge or awareness of facts and circumstances indicating "specific and identifiable infringements." "The DMCA "includes safe-harbor provisions that provide protections to Internet service providers under certain conditions." "First, there are three threshold requirements: the party "(1) must be a service provider as defined by the statute; (2) must have adopted and reasonably implemented a policy for the termination in appropriate circumstances of users who are repeat infringers; and (3) must not interfere with standard technical

	ments, but also includes digital notice. The CDA reform also adapts the EU's Digital Services Act requirement in requiring specific and identifiable ongoing torts as a predicate for action. In addition, the tort complainant must specific reasons why content constitutes an ongoing cybertort, which parallels Section 512 of the DMCA's procedure.		measures used by copyright owners to identify or protect copyrighted works."
Content of the Takedown Notice?	The CDA notice-and-takedown requires the complainant to specify reasons why the content is an ongoing tort and provides the website with contact information. In addition, the complaint must attest to a good faith belief that the content is tortious closely paralleling the DMCA requirements in Section 512. As the DMCA, the complainant must specify the location of the tortious material with specificity.	The e-Commerce Directive provides no guidance on what must be in a takedown complaint. Article 14 of the DSA replaces "Article 14 of the e-Commerce Directive promulgates extensive guidance on the content of takedown notice. Article 14 (1) of the DSA requires that providers of hosting services, such as websites, establish "mechanisms . . . to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content." Article 14(2) gives specific guidance on the content of takedown notices: "(a) an explanation of the	The copyright owner's complaint of infringing content on a website must declare, under penalty of perjury, that he, or she, is authorized to represent the copyright holder, and that he, or she, has a good-faith belief the use is infringing; thus, a notification must do more than identify the infringing item. In addition to the Section 512(c)(3) takedown, the DMCA also recognizes a Section 512(h) takedown. The contents of the request must include: "(A) a copy of a notification described in subsection (c)(3)(A); (B) a proposed subpoena; and (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting

		reasons why the individual or entity considers the information in question to be illegal content; (b) a clear indication of the electronic location of that information, in particular the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content; (c) the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU; (d) a statement confirming the good faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete 4. Where the notice contains the name and an electronic mail address of the individual or entity that submitted it, the provider of hosting services shall promptly send a confirmation of receipt of the notice to that individual or entity."	rights under this title." Subsection (c)(3)(A) provides in the part relevant to the issue before the court that the notice include a "take down" provision: "(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material."
What objectionable content is subject	Ongoing cybertorts posted on a website or	All illegal activity including infringing content, torts, and crimes.	Only infringing content.

to notice-and-takedown?	other Internet platform.		
Does the NTD Recognize a Safe Harbor against liability?	Yes, the NTD for torts adapts the DMCA safe harbor provisions for infringing content.	No, there is no safe harbor under the e-Commerce Directive nor the DSA.	If a services provider or other operator learns of specific infringing material available on the system and fails to purge such material from the system, the operator knows of and contributes to direct infringement. "But 'absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material.'" The DMCA's notice, takedown, and put-back procedures are triggered when a copyright owner, or an assignee, gives written notice to the designated agent of the service provider under § 512(c)(3)(A).
Does the NTD have safeguards against takedown demands to silence free expression?	The CDA Section 230 NTD only applies to cybertorts that are not speech torts applying to matters of public concern.	Neither the DSA nor DMA address whether takedown demands can be challenged on grounds of free expression.	No DMCA provision addresses whether takedown demands may be defended on grounds of free expression. In general, there is no First Amendment right to infringe on the intellectual property rights of creators.
Remedies for Frivolous Takedown Demands	The CDA Section 230 NTD creates a cause of action for remedying frivolous takedown demands backed by the deterrent of punitive damages. The punitive damages remedy will be calibrated by the wealth of	No remedy against frivolous takedown demands.	Not addressed in the DMCA.

	the defendant as well as other aggravating circumstances

CONCLUSION

Internet law must evolve to make actionable harmful conduct by online intermediaries, especially when the conduct is willful, as is the case when websites and other intermediaries host deplorable conduct constituting ongoing cybertorts or cybercrimes. Since the judicially expanded CDA Section 230 liability shield prevents cybertorts from evolving to protect consumers in the online world, Congress must act now to impose a takedown duty on the largest Internet gatekeepers. Like the DMCA's takedown procedures for copyright infringement, our proposed CDA Section 230 modification is a specific sector reform. Our CDA reform adapts specific provisions of the DSA to create a notice-and-takedown regime that balances the interests of tort plaintiffs and content creators.

We also adapt the EU's policy of placing the burden of notice-and-takedown only on the largest Internet entities. These powerful gatekeepers are the source of new risks and challenges, which could not have been foreseen when the CDA was enacted in 1996. Our CDA reform retains the beneficial role of continuing to give all Internet intermediaries a broad liability shield.

Imposing a duty on Internet intermediaries to expeditiously takedown ongoing torts is a democratic measure that gives plaintiffs a direct remedy to remove illegal content as opposed to waiting for regulators to act. A gatekeeper must act expeditiously to remove, or disable access to, the material when it (1) has actual knowledge, (2) is aware of facts or circumstances from which infringing activity is apparent, or (3) has received notification of claimed infringement meeting the requirements of § 512(c)(3). Our CDA Section 230 NTD reform relies upon private, not public, enforcement by arming the direct victims of cybertorts with a takedown remedy. This notice-and-takedown reform will bring common sense to the common law by aligning CDA Section 230 with the DMCA and EU's Digital Services Act.

[THIS PAGE INTENTIONALLY LEFT BLANK]